(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 684 299**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)
H04W 8/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.07.2009 PCT/EP2009/059925**

(87) Fecha y número de publicación internacional: **04.02.2010 WO10012821**

(96) Fecha de presentación y número de la solicitud europea: **31.07.2009 E 09781333 (1)**

(97) Fecha y número de publicación de la concesión europea: **23.05.2018 EP 2321946**

(54) Título: **Método, aparato, sistema y producto de programa informático para soportar P-CSCF heredada para indicar a la S-CSCF que omita autenticación**

(30) Prioridad:

01.08.2008 WO PCT/EP2008/060148

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.10.2018

(73) Titular/es:

NOKIA SIEMENS NETWORKS OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

SHEN, JIADONG

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método, aparato, sistema y producto de programa informático para soportar P-CSCF heredada para indicar a la S-CSCF que omita autenticación

Campo de la invención

La presente invención se refiere a protección de identidad. Más específicamente, la presente invención se refiere a métodos, aparatos, un sistema y un producto de programa informático relacionado para la protección de identidad. Ejemplos de la presente invención pueden ser aplicables a los servicios centralizados (ICS) del subsistema multimedia (IMS) del Protocolo de Internet (IP).

Antecedentes

ICS se ha considerado y se ha introducido en el programa de asociación de la 3ª generación (3GPP) por ejemplo la *release* 8, especificación técnica (TS) 23.292.

ICS puede proporcionar servicios de comunicación de manera que todos los servicios, y el control de servicio, están basados, por ejemplo, en mecanismos y activadores de IMS. ICS posibilita servicios de IMS a usuarios que están conectados, por ejemplo, mediante el servicio centralizado. Cuando un usuario de ICS accede al IMS usando acceso de conmutación de circuitos (CS), es decir mediante un servidor (un servidor de MSC que soporta ICS) del centro de conmutación móvil de ICS (IMSC), puede realizarse autenticación y autorización en el servidor de IMSC y por lo tanto, por ejemplo una función de control de sesión de llamada de servicio (S-CSCF) puede omitir la autenticación de IMS parta un registro de IMS de este tipo.

Al usuario de ICS puede asignarse una denominada identidad de usuario privada de IMS de ICS (IMPI) especial cuando accede al IMS, por ejemplo, mediante el dominio de CS. La S-CSCF puede usar esta IMPI de ICS especial como una indicación para esta situación de que el usuario ya se ha autenticado y autorizado por el servidor de IMSC. Sin embargo, la IMPI de ICS no está protegida frente a abuso. Un usuario malicioso puede usar una IMPI de ICS especial de este tipo para usar el servicio de IMS, por ejemplo, gratis, ya que se omite el proceso de autenticación.

En *releases* de IMS anteriores esto se resolvió por la P-CSCF que comprueba una solicitud de registro recibida desde un usuario y la pasa hacia la S-CSCF que indica si la solicitud de registro puede provenir o no de un usuario malicioso potencial. La S-CSCF puede a continuación desafiar la solicitud de registro si la P-CSCF ha indicado que la solicitud de registro puede provenir desde un usuario malicioso.

El documento US 2008/0039085 describe un método para autenticar el equipo de usuario, el método comprende recibir una solicitud de registro desde el equipo de usuario en una entidad de intermediario de una red confiable, recibir información de localización del equipo de usuario específica de usuario en la entidad de intermediación de la red confiable, generar un encabezamiento de red confiable en la entidad de intermediación, incluyendo el encabezamiento de red confiable la información de localización específica de usuario recibida, reenviar el encabezamiento de red confiable a una entidad de servicio para autenticación, comparar la información de localización específica de usuario a una lista de referencias aprobadas en la entidad de servicio y si la información de localización específica de usuario coincide con una entrada en la lista de referencias aprobadas, autenticar el equipo de usuario para acceso a la red confiable.

El documento del 3GPP: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 8)", borrador 36PP, XP050280757 hace referencia a especificar características de seguridad y un mecanismo para acceso seguro al subsistema de IM (IMS) para el sistema de telecomunicación móvil de la 3G.

El documento del 3GPP; "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) Centralized Services; Stage 2 (Release 8)", 3GPP TS 23.292, XP050361576 hace referencia a especificar los requisitos de arquitectura para entrega de servicios de IMS consistentes a un usuario independientemente del tipo de acceso conectado (por ejemplo acceso de dominio de CS, o IP-CAN).

Sin embargo la situación es diferente en el sistema de ICS, puesto que el IMSC está ahora realizando el registro y deberá evitarse una autenticación adicional por la S-CSCF cuando el usuario ya se ha autenticado y autorizado satisfactoriamente por el IMSC.

En los organismos de normalización (por ejemplo, el 3GPP) se analizó usar el encabezamiento de Información de red de Acceso P (PANI) para indicar desde el IMSC a la S-CSCF que la autenticación puede omitirse. El encabezamiento PANI puede contener información acerca de la red de acceso y un parámetro “proporcionado por la red”. La información acerca de la red de acceso puede informar a la S-CSCF que la autenticación ya se ha realizado.

Una posible desventaja de la solución de encabezamiento de PANI reside en que las *Releases* de P-CSCF más antiguas pueden no soportar el mecanismo “proporcionado por la red”. Por lo tanto, puede existir una posibilidad de que pueda abusarse de este mecanismo por un usuario malicioso. El usuario malicioso puede establecer el parámetro “proporcionado por la red” y una P-CSCF que no tenga conocimiento puede no eliminar el parámetro. Como consecuencia, la S-CSCF puede omitir la autenticación.

Una manera para resolver este problema puede ser la administración apropiada, es decir la S-CSCF puede decidir si aceptar o no la indicación “proporcionada por la red” basándose en una base de datos. Sin embargo, una base de datos de este tipo requiere administración adicional que puede ser no gestionable en escenarios de itinerancia.

Otro enfoque reside en usar una solución basándose en bases de datos únicamente, donde se almacenan todos los servidores de MSC que soportan ICS (IMSC). Adicionalmente, la S-CSCF puede únicamente omitir el proceso de autenticación si el usuario de ICS se registra, por ejemplo, con el IMS mediante un servidor de IMSC de este tipo. Sin embargo, esta alternativa puede provocar un esfuerzo administrativo inaceptable y provocará también un gran problema para la sincronización de las bases de datos.

Una desventaja posible adicional puede residir en que, como un usuario de ICS puede acceder también a su dominio de IMS doméstico mediante un servidor de IMSC visitado en caso de itinerancia, todos los servidores de IMSC en dominios de itinerancia de CS externos tienen también que almacenarse en la base de datos. Esto significa que cada vez que se añade o elimina un servidor de IMSC, las bases de datos en todos los dominios con un acuerdo de itinerancia tienen que actualizarse. Esto provocará esfuerzos administrativos inaceptables y provocará también un gran problema para la sincronización de las bases de datos.

Teniendo en cuenta lo anterior, es un objetivo de los ejemplos de la presente invención superar una o más de las anteriores desventajas. En particular, la presente invención proporciona métodos, aparatos, un sistema y un producto de programa informático relacionado para la protección de identidad.

De acuerdo con un ejemplo de la presente invención, en un primer aspecto, este objetivo se consigue por ejemplo mediante **un método** que comprende:
transmitir, después del registro satisfactorio de un terminal en una entidad de red, un mensaje de registro que comprende información de identidad de terminal e información de indicación de integridad que indica integridad afirmativa de la información de identidad de terminal.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el primer aspecto anterior,

- el método comprende adicionalmente generar el mensaje de registro por la entidad de red;
- el mensaje de registro es uno de un mensaje de registro inicial, un mensaje de repetición de registro y un mensaje de anulación de registro;
- la entidad de red es un centro de conmutación móvil mejorado del servicio centralizado del subsistema multimedia del protocolo de Internet.

De acuerdo con un ejemplo de la presente invención, en un segundo aspecto, este objetivo se consigue por ejemplo mediante **un método** que comprende:
procesar, después de la recepción de un mensaje de registro que comprende información de identidad de terminal e información de indicación de integridad que indica integridad de la información de identidad de terminal, el mensaje de registro recibido basándose en la información de identidad de terminal y la información de indicación de integridad de manera que,

i) si la integridad se indica afirmativa, se omite un procedimiento de autenticación del terminal, o,
ii) si la integridad se indica negativa, el mensaje de registro recibido se rechaza sin aprovisionamiento de información clave relacionada con el registro del terminal.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el segundo aspecto anterior,

- el método comprende adicionalmente recibir el mensaje de registro;
- la información clave se refiere a un registro seguro entre el terminal y una entidad de control de red;
- el procesamiento del elemento i) se realiza si se reconoce un registro satisfactorio del terminal, y el procesamiento del elemento ii) se realiza si se reconoce el mensaje de registro recibido como desprotegido;
- la información de indicación de integridad que indica integridad negativa está constituida por una bandera de integridad protegida que se establece a no.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el primer y segundo aspectos anteriores,

- la información de indicación de integridad que indica integridad afirmativa está constituida por una bandera de integridad protegida que se establece a sí;
- el mensaje de registro es un mensaje de registro de protocolo de iniciación de sesión;
- la información de identidad de terminal está constituida por una identidad privada de multimedia del protocolo de Internet del servicio centralizado del subsistema multimedia del protocolo de Internet especial.

De acuerdo con un ejemplo de la presente invención, en un tercer aspecto, este objetivo se consigue por ejemplo mediante **un aparato** que comprende:
medios para transmitir, después del registro satisfactorio de un terminal en el aparato, un mensaje de registro que comprende información de identidad de terminal e información de indicación de integridad que indica integridad afirmativa de la información de identidad de terminal.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el tercer aspecto anterior,

- el aparato comprende adicionalmente medios para generar el mensaje de registro;
- el mensaje de registro es uno de un mensaje de registro inicial, un mensaje de repetición de registro y un mensaje de anulación de registro;
- el aparato está constituido por un centro de conmutación móvil mejorado del servicio centralizado del subsistema multimedia del protocolo de Internet.

De acuerdo con un ejemplo de la presente invención, en un cuarto aspecto, este objetivo se consigue por ejemplo mediante **un aparato** que comprende:
medios para procesar, después de la recepción de un mensaje de registro que comprende información de identidad de terminal e información de indicación de integridad que indica integridad de la información de identidad de terminal, el mensaje de registro recibido basándose en la información de identidad de terminal y la información de indicación de integridad de manera que,

i) si la integridad se indica afirmativa, se omite un procedimiento de autenticación del terminal, o,
ii) si la integridad se indica negativa, el mensaje de registro recibido se rechaza sin aprovisionamiento de información clave relacionada con el registro del terminal.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el cuarto aspecto anterior,

- la información clave se refiere a un registro seguro entre el terminal y una entidad de control de red;
- el aparato comprende adicionalmente medios para recibir el mensaje de registro;
- los medios para recibir están configurados para recibir el mensaje de registro desde uno de la entidad de control de red y el aparato de acuerdo con el tercer aspecto;
- los medios para procesar están configurados para procesar de acuerdo con el elemento i) si se reconoce un registro satisfactorio del terminal, y están configurados para procesar de acuerdo con el elemento ii) si se reconoce el mensaje de registro recibido como desprotegido;
- la información de indicación de integridad que indica integridad negativa está constituida por una bandera de integridad protegida que se establece a no;
- el aparato está constituido por una función de control de sesión de llamada de servicio.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el tercer y cuarto aspectos anteriores,

- la información de indicación de integridad que indica integridad afirmativa está constituida por una bandera de integridad protegida que se establece a sí;
- el mensaje de registro es un mensaje de registro de protocolo de iniciación de sesión;
- la información de identidad de terminal está constituida por una identidad privada de multimedia del protocolo de Internet del servicio centralizado del subsistema multimedia del protocolo de Internet especial;
- la entidad de control de red está constituida por una función de control de sesión de llamada de intermediario;
- al menos uno o más de los medios para transmitir, medios para generar, medios para procesar, medios para recibir y el aparato se implementan como un conjunto de chips o módulo.

De acuerdo con un ejemplo de la presente invención, en un quinto aspecto, este objetivo se consigue por ejemplo mediante **un aparato** que comprende:
un transmisor configurado para transmitir, después del registro satisfactorio de un terminal en el aparato, un mensaje de registro que comprende información de identidad de terminal e información de indicación de integridad que indica integridad afirmativa de la información de identidad de terminal.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el quinto aspecto anterior,

- el aparato comprende adicionalmente un generador configurado para generar el mensaje de registro;
- el mensaje de registro es uno de un mensaje de registro inicial, un mensaje de repetición de registro y un mensaje de anulación de registro;
- el aparato está constituido por un centro de conmutación móvil mejorado del servicio centralizado del subsistema multimedia del protocolo de Internet.

De acuerdo con un ejemplo de la presente invención, en un sexto aspecto, este objetivo se consigue por ejemplo mediante **un aparato** que comprende:
un procesador configurado para procesar, después de la recepción de un mensaje de registro que comprende información de identidad de terminal e información de indicación de integridad que indica integridad de la información de identidad de terminal, el mensaje de registro recibido basándose en la información de identidad de terminal y la información de indicación de integridad de manera que,

i) si la integridad se indica afirmativa, se omite un procedimiento de autenticación del terminal, o,
ii) si la integridad se indica negativa, el mensaje de registro recibido se rechaza sin aprovisionamiento de información clave relacionada con el registro del terminal.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el sexto aspecto anterior,

- la información clave se refiere a un registro seguro entre el terminal y una entidad de control de red;
- el aparato comprende adicionalmente un receptor configurado para recibir el mensaje de registro;
- el receptor está configurado para recibir el mensaje de registro desde uno de la entidad de control de red y el aparato de acuerdo con el quinto aspecto;
- el procesador está configurado para procesar de acuerdo con el elemento

  i) si se reconoce un registro satisfactorio del terminal, y está configurado para procesar de acuerdo con el elemento
  ii) si se reconoce el mensaje de registro recibido como desprotegido;

- la información de indicación de integridad que indica integridad negativa está constituida por una bandera de integridad protegida que se establece a no;
- el aparato está constituido por una función de control de sesión de llamada de servicio.

De acuerdo con perfeccionamientos adicionales del ejemplo de la presente invención como se definen bajo el quinto y sexto aspectos anteriores,

- la información de indicación de integridad que indica integridad afirmativa está constituida por una bandera de integridad protegida que se establece a sí;
- el mensaje de registro es un mensaje de registro de protocolo de iniciación de sesión;
- la información de identidad de terminal está constituida por una identidad privada de multimedia del protocolo de Internet del servicio centralizado del subsistema multimedia del protocolo de Internet especial;
- la entidad de control de red está constituida por una función de control de sesión de llamada de intermediario;
- al menos uno o más de un transmisor, un generador, un procesador, un receptor y el aparato se implementan como un conjunto de chips o módulo.

De acuerdo con un ejemplo de la presente invención, en un séptimo aspecto, este objetivo se consigue por ejemplo mediante **un sistema** que comprende:

un terminal;
un aparato de acuerdo con uno cualquiera del tercer y quinto aspectos anteriores; y
un aparato de acuerdo con uno cualquiera del cuarto y sexto aspectos anteriores.

De acuerdo con un ejemplo de la presente invención, en un octavo aspecto, este objetivo se consigue por ejemplo mediante **un producto de programa informático** que comprende medios de código para realizar etapas de método de un método de acuerdo con uno cualquiera del primer y segundo aspectos anteriores, cuando se ejecuta en un medio o módulo de procesamiento.

De acuerdo con un ejemplo de la presente invención, en un noveno aspecto, este objetivo se consigue por ejemplo mediante **un programa informático** que comprende medios de código para realizar un método que comprende:
transmitir, después del registro satisfactorio de un terminal en una entidad de red, un mensaje de registro que comprende información de identidad de terminal e información de indicación de integridad que indica integridad afirmativa de la información de identidad de terminal.

De acuerdo con un ejemplo de la presente invención, en un décimo aspecto, este objetivo se consigue por ejemplo mediante **un programa informático** que comprende medios de código para realizar un método que comprende:

procesar, después de la recepción de un mensaje de registro que comprende información de identidad de terminal e información de indicación de integridad que indica integridad de la información de identidad de terminal, el mensaje de registro recibido basándose en la información de identidad de terminal y la información de indicación de integridad de manera que,

i) si la integridad se indica afirmativa, se omite un procedimiento de autenticación del terminal, o,
ii) si la integridad se indica negativa, el mensaje de registro recibido se rechaza sin aprovisionamiento de información clave relacionada con el registro del terminal.

A este respecto, ha de señalarse que los ejemplos de la presente invención posibilitan uno o más de lo siguiente:

- posibilitar que la S-CSCF verifique si el emisor de una solicitud de registro es o no un IMSC, asegurando que, por medio del concepto únicamente el IMSC pueda enviar una solicitud de integridad protegida de este tipo, y que mediante una P-CSCF únicamente la solicitud REGISTER desprotegida para usuarios de ICS pueda alcanzar una S-CSCF;
- basándose en el elemento anterior, la S-CSCF puede omitir la autorización y autenticación si la solicitud de registro se recibe desde un IMSC.
- Proporcionar una solución para el problema analizado en los organismos de normalización (por ejemplo, el 3GPP);
- Aliviar esfuerzos administrativos y evitar problemas relacionados con la sincronización de las bases de datos;
- Posibilitar que el servidor de IMSC genere una solicitud de registro, que además incluye, por ejemplo, la IMPI de ICS especial.

Breve descripción de los dibujos

Se describen ejemplos de la presente invención en el presente documento a continuación con referencia a los dibujos adjuntos, en los que:

La Figura 1 muestra métodos para protección de identidad de acuerdo con un ejemplo de la presente invención en caso de aceptación de la solicitud de registro;

La Figura 2 muestra los métodos para protección de identidad de acuerdo con un ejemplo de la presente invención en caso de rechazo de la solicitud de registro; y

La Figura 3 muestra aparatos (por ejemplo IMSC 2021 y S-CSCF 2023) para protección de identidad de acuerdo con un ejemplo de la presente invención.

Descripción detallada de la presente invención

Se describen ejemplos de la presente invención en el presente documento a continuación a modo de ejemplo con referencia a los dibujos adjuntos.

Se ha de observar que para esta descripción, las expresiones “IMSC, SIP REGISTER, IMPI de ICS especial, bandera de integridad protegida, bandera de integridad protegida='sí' y bandera de integridad protegida='no'” son ejemplos de “entidad de red, mensaje de registro, información de identidad de terminal, información de indicación de integridad, integridad afirmativa e integridad negativa”, respectivamente, sin restringir las expresiones anteriormente nombradas a los detalles técnicos o de implementación especiales impuestos a las primeras expresiones nombradas.

La Figura 1 muestra métodos para protección de identidad de acuerdo con un ejemplo de la presente invención en caso de aceptación de la solicitud de registro, mientras que la Figura 2 muestra métodos en caso de rechazo de la solicitud de registro. La señalización entre elementos se indica en dirección horizontal, mientras que los aspectos de tiempo entre la señalización pueden reflejarse en la disposición vertical de la secuencia de señalización así como en los números de secuencias. Se ha de observar que los aspectos de tiempo indicados en las Figuras 1 y 2 no restringen necesariamente una cualquiera de las etapas de métodos mostradas a la secuencia de etapas señalada. Esto se aplica en particular a etapas de método que son funcionalmente disjuntas entre sí. En las Figuras 1 y 2, para facilidad de descripción, se representan medios o porciones que pueden proporcionar funcionalidades principales con bloques funcionales o flechas de línea continua y/o una fuente normal, mientras que se representan medios o porciones que pueden proporcionar funciones opcionales con bloques funcionales o flechas de línea discontinua y/o una fuente en cursiva.

Como se muestra en la Figura 1, un sistema de comunicación 200 puede comprender un terminal o equipo de usuario (UE) 201 y una red 202. La red 202 puede comprender a su vez un servidor de MSC o IMSC 2021 (denominado como “IMSC” en lo sucesivo), un servidor de abonado doméstico/registro de localización doméstico (HSS/HLR) 2022 opcional y una S-CSCF 2023.

Como medidas preparatorias opcionales, en las etapas opcionales S0-1 a S0-3, por ejemplo el UE 201 puede realizar registro (o conexión) al IMSC 2021. Adicionalmente, en la etapa opcional S1-0a, por ejemplo el IMSC 2021 puede realizar la decisión sobre el registro de IMS recibido desde el UE 201, y en la etapa opcional S1-0b, por ejemplo el IMSC 2021 puede realizar descubrimiento de una dirección de IMS relacionada con el UE 201.

En la etapa opcional S1-1, por ejemplo el IMSC 2021 puede realizar la generación de un mensaje de registro que comprende información de identidad de terminal (por ejemplo la IMPI de ICS especial) e información de indicación de integridad (por ejemplo, bandera de integridad protegida) que indica integridad afirmativa de la información de identidad de terminal (por ejemplo bandera="sí").

En la etapa S1-2, por ejemplo el IMSC 2021 puede realizar transmisión, después del registro satisfactorio (véanse las etapas opcionales S0-1 a S0-3) de un terminal (por ejemplo el UE 201) en una entidad de red (por ejemplo el mismo IMSC 2021), el mensaje de registro (por ejemplo SIP REGISTER).

Como para los perfeccionamientos adicionales del método anterior relacionado con el IMSC 2021, el mensaje de registro puede ser un mensaje de registro inicial, un mensaje de repetición de registro o un mensaje de anulación de registro. Adicionalmente, la entidad de red puede ser el centro de conmutación móvil mejorado del servicio centralizado del subsistema multimedia del protocolo de Internet.

Adicionalmente, en una etapa opcional S2-1, por ejemplo la S-CSCF 2023 puede realizar la recepción del mensaje de registro transmitido en la etapa S1-2.

A continuación, en la etapa S2-2, por ejemplo la S-CSCF 2023 puede realizar procesamiento, después de la recepción del mensaje de registro (por ejemplo SIP REGISTER) que comprende la información de identidad de terminal (por ejemplo la IMPI de ICS especial) e información de indicación de integridad (por ejemplo bandera de integridad protegida) que indica integridad de la información de identidad de terminal, el mensaje de registro recibido basándose en la información de identidad de terminal y la información de indicación de integridad de manera que,

i) si la integridad se indica afirmativa, se omite un procedimiento de autenticación del terminal (por ejemplo UE 201), o,
ii) si la integridad se indica negativa (por ejemplo bandera="no"), el mensaje de registro recibido se rechaza sin aprovisionamiento de información clave relacionada con el registro del terminal (no mostrado en la Figura 1).

Finalmente, en la etapa opcional S0-4, por ejemplo la red 202 puede realizar la finalización de la señalización de registro.

Como para los perfeccionamientos adicionales del método anterior relacionado con la S-CSCF 2023, la información clave puede referirse a un registro seguro entre el terminal y una entidad de control de red (por ejemplo una P-CSCF 2024 mostrada en la Figura 2). Adicionalmente, el procesamiento del elemento i) puede realizarse si se reconoce un registro satisfactorio del terminal, y el procesamiento del elemento ii) puede realizarse si se reconoce el mensaje de registro recibido como desprotegido. Además, la información de indicación de integridad que indica integridad negativa puede estar constituida por una bandera de integridad protegida que se establece a no (no mostrado en la Figura 1).

Como para perfeccionamientos adicionales de los métodos anteriores relacionados tanto con el IMSC 2021 como la S-CSCF 2023, la información de indicación de integridad que indica integridad afirmativa puede estar constituida por una bandera de integridad protegida que se establece a sí. Adicionalmente, el mensaje de registro puede ser un mensaje de registro de protocolo de iniciación de sesión (SIP). Además, la información de identidad de terminal puede estar constituida por una identidad privada multimedia del protocolo de Internet (IMPI) del servicio centralizado (ICS) del subsistema multimedia (IMS) del protocolo de Internet (IP) especial.

Como se ha mencionado anteriormente, la Figura 2 muestra aquellos métodos en caso de rechazo de la solicitud de registro. Como se muestra en la Figura 2, en la etapa opcional S0-1, un UE malicioso 201 puede intentar transmitir por ejemplo una solicitud de SIP REGISTER fraudulenta que comprende su IMPI de ICS especial y la bandera de integridad protegida establecida a "sí".

En la etapa opcional S0-2, por ejemplo la P-CSCF 2024 puede realizar la recepción de la solicitud de SIP REGISTER fraudulenta. En una etapa opcional S0-3, por ejemplo la P-CSCF 2024 puede realizar procesamiento de manera que si no existe asociación de seguridad (SA) para la IMPI de ICS especial recibida en la P-CSCF 2024, entonces la solicitud REGISTER puede determinarse que se recibe fuera de cualquier SA o con una SA no unida a la IMPI de ICS especial. En ese caso, la P-CSCF 2024 puede establecer la integridad protegida a "no" o puede eliminar este parámetro.

Además, en una etapa opcional S0-4, por ejemplo la P-CSCF 2024 puede realizar transmisión de la solicitud de SIP REGISTER que tiene la IMPI de ICS especial del UE 201 malicioso y la bandera de integridad protegida establecida a "no". Esta solicitud de SIP REGISTER puede recibirse por la S-CSCF 2021 en la etapa opcional anteriormente

descrita S2-1.

A continuación, en la etapa S2-2, por ejemplo la S-CSCF 2023 puede realizar procesamiento de acuerdo con el elemento ii) como se ha descrito anteriormente.

Finalmente, en una etapa opcional S0-5, por ejemplo la red 202 puede realizar el rechazo de la solicitud REGISTER hacia el UE malicioso 201.

La Figura 3 muestra aparatos (por ejemplo IMSC 2021 y S-CSCF 2023) para protección de identidad de acuerdo con un ejemplo de la presente invención. En la Figura 3, para facilidad de descripción, se representan medios o porciones que pueden proporcionar funcionalidades principales con bloques funcionales o flechas de línea continua y una fuente normal, mientras que se representan los medios o porciones que pueden proporcionar funciones opcionales con bloques funcionales o flechas de línea discontinua y una fuente en cursiva.

El IMSC 2021 puede comprender una CPU (o funcionalidad de núcleo CF) 20211, una memoria 20212, un transmisor (o medios para transmitir) 20213, un receptor opcional (o medios para recibir) 20214 y un generador opcional (o medios para generar) 20215.

A su vez, la S-CSCF 2023 puede comprender una CPU (o funcionalidad de núcleo CF) 20231 que puede servir también como un procesador (o medios para procesar), una memoria 20232, un transmisor opcional (o medios para transmitir) 20233 y un receptor opcional (o medios para recibir) 20234.

Finalmente, la P-CSCF opcional 2024 puede tener una estructura sustancialmente similar a la de la S-CSCF 2023.

Como se indica por la extensión de línea discontinua del bloque funcional de la CPU 20211, los medios para generar 20215 del IMSC 2021 pueden ser una funcionalidad que se ejecuta en la CPU 20211 del IMSC 2021 o pueden ser, como alternativa una entidad o medios funcionales separados.

Las CPU 20x1 (en las que x = 21 y 23) pueden configurarse respectivamente para procesar diversas entradas de datos y para controlar las funciones de las memorias 20x2, los medios para transmitir 202x3 y los medios para recibir 20x4 (y los medios para generar 20215 del IMSC 20221). Las memorias 20x2 pueden servir, por ejemplo para almacenar medios de código para llevar a cabo, por ejemplo, los métodos de acuerdo con un ejemplo de la presente invención, cuando se ejecutan por ejemplo en las CPU 20x1. Se ha de observar que los medios para transmitir 20x3 y los medios para recibir 20x4 pueden proporcionarse, como alternativa, como respectivos transceptores integrales. Se ha de observar adicionalmente que los transmisores/receptores pueden implementarse i) como transmisores/receptores físicos para realizar funciones de transceptor por ejemplo mediante una interfaz aérea (por ejemplo, en caso de transmitir entre el UE 201 y el IMSC 2021), ii) como entidades de encaminamiento, por ejemplo, para transmitir/recibir paquetes de datos, por ejemplo en una red (por ejemplo entre el IMSC 2021 o la P-CSCF 2024 y la S-CSCF 2023 cuando se disponen como entidades de red separadas) de PS (conmutación de circuitos), iii) como funcionalidades para escribir/leer información en/desde un área de memoria dada (por ejemplo en caso de CPU o memorias compartidas/comunes por ejemplo del IMSC 2021 o la P-CSCF 2024 y la S-CSCF 2023 cuando se disponen como una entidad de red integral (no mostrado)), o iv) como cualquier combinación adecuada de i) a iii).

Como medidas preparatorias opcionales, por ejemplo el UE 201 (no mostrado) puede realizar registro (o conexión) al IMSC 2021. Adicionalmente, por ejemplo el IMSC 2021 puede realizar decisión sobre el registro de IMS recibido desde el UE 201, y por ejemplo el IMSC 2021 puede realizar descubrimiento de una dirección de IMS relacionada con el UE 201 (por ejemplo la IMPI de ICS especial).

Opcionalmente, por ejemplo los medios para generación 20215 del IMSC 2021 pueden realizar generación de un mensaje de registro que comprende información de identidad de terminal (por ejemplo la IMPI de ICS especial) e información de indicación de integridad (por ejemplo bandera de integridad protegida) que indica integridad afirmativa de la información de identidad de terminal (por ejemplo bandera=“sí”).

A continuación, por ejemplo los medios para transmitir 20213 del IMSC 2021 pueden realizar transmisión, después del registro satisfactorio de un terminal (por ejemplo UE 201) en una entidad de red (por ejemplo el mismo IMSC 2021), el mensaje de registro (por ejemplo SIP REGISTER).

Como alternativa, por ejemplo la P-CSCF 2024 puede realizar recepción de la solicitud de SIP REGISTER fraudulenta, y puede realizar procesamiento de manera que si no existe asociación de seguridad (SA) para la IMPI de ICS especial recibida en la P-CSCF 2024, a continuación la solicitud REGISTER puede determinarse que se recibe fuera de cualquier SA o con una SA no unida a la IMPI de ICS especial. En ese caso, la P-CSCF 2024 puede establecer la integridad protegida a “no” o puede eliminar este parámetro, y puede realizar la transmisión de la solicitud de SIP REGISTER que tiene la IMPI de ICS especial del UE malicioso 201 y la bandera de integridad protegida establecida “no”.

En cuanto a perfeccionamientos adicionales relacionados con el IMSC 2021, el mensaje de registro puede ser un mensaje de registro inicial, un mensaje de repetición de registro o un mensaje de anulación de registro. Adicionalmente, la entidad de red puede ser el centro de conmutación móvil mejorado del servicio centralizado del subsistema multimedia del protocolo de Internet.

Opcionalmente, por ejemplo los medios para recibir 20234 de la S-CSCF 2023 pueden realizar la recepción del mensaje de solicitud de registro (que comprende por ejemplo integridad protegida = “sí”) transmitido por los medios para transmitir 20213 del IMSC 2021 o el mensaje de solicitud de registro (que comprende por ejemplo integridad protegida = “no”) transmitido por la P-CSCF 2024.

A continuación, por ejemplo los medios para procesar 20231 de la S-CSCF 2023 pueden realizar procesamiento, después de la recepción del mensaje de registro (por ejemplo SIP REGISTER) que comprende la información de identidad de terminal (por ejemplo la IMPI de ICS especial) e información de indicación de integridad (por ejemplo bandera de integridad protegida) que indica integridad de la información de identidad de terminal, el mensaje de registro recibido basándose en la información de identidad de terminal y la información de indicación de integridad de manera que,

i) si la integridad se indica afirmativa, se omite un procedimiento de autenticación del terminal (por ejemplo UE 201), o,
ii) si la integridad se indica negativa (por ejemplo bandera=“no”), el mensaje de registro recibido se rechaza sin aprovisionamiento de información clave relacionada con el registro del terminal.

Como para perfeccionamientos adicionales relacionados con la S-CSCF 2023, la información clave puede hacer referencia a un registro seguro entre el terminal y una entidad de control de red (por ejemplo una P-CSCF 2024 mostrada en la Figura 2). Adicionalmente, los medios para procesar pueden configurarse para procesar de acuerdo con el elemento i) si se reconoce un registro satisfactorio del terminal, y de acuerdo con el elemento ii) si se reconoce el mensaje de registro recibido como desprotegido. Además, la información de indicación de integridad que indica integridad negativa puede estar constituida por una bandera de integridad protegida que se establece a no.

Como para perfeccionamientos adicionales relacionados con tanto el IMSC 20221 como la S-CSCF 2023, la información de indicación de integridad que indica integridad afirmativa puede estar constituida por una bandera de integridad protegida que se establece a sí. Adicionalmente, el mensaje de registro puede ser un mensaje de registro de protocolo de iniciación de sesión (SIP). Además, la información de identidad de terminal puede estar constituida por una identidad privada multimedia del protocolo de Internet (IMPI) del servicio centralizado (ICS) del subsistema multimedia (IMS) del protocolo de Internet (IP) especial.

Adicionalmente, al menos uno de, o más medios para transmitir 20213, medios para generar 20215, medios para procesar 20231, medios para recibir 20234 y/o el IMSC 2021 y/o la S-CSCF 2023, o las respectivas funcionalidades llevadas a cabo, pueden implementarse como un conjunto de chips o módulo.

Finalmente, la presente invención también se refiere a un sistema que puede comprender un terminal o equipo de usuario, el IMSC 2021 anteriormente descrito y la S-CSCF 2023 anteriormente descrita.

Sin estar restringido a los detalles que siguen en esta sección, la realización de la presente invención puede resumirse como sigue:
Como el usuario de ICS ya se ha autenticado satisfactoriamente en el dominio de CS, su comunicación de IMS mediante el dominio de CS/servidor de IMSC está protegida. Por lo tanto, puede usarse un parámetro que indica “protección de integridad” satisfactoria para indicar desde el servidor de MSC a la S-CSCF que puede omitirse la autenticación en el IMS. Se propone usar el parámetro en el encabezamiento de autorización. Un parámetro adecuado puede ser el denominado parámetro de “integridad protegida”.

Cuando un usuario de ICS accede al IMS por ejemplo mediante un servidor de IMSC, el servidor de IMSC deberá usar la IMPI de ICS especial para registrar el usuario de ICS con IMS (como se especifica por ejemplo en el documento del 3GPP TS 23.292). Y en la solicitud REGISTER, el parámetro de “integridad protegida” en el encabezamiento de autorización puede establecerse a “sí”. La justificación reside en que el usuario ya está autenticado en el IMSC. Cuando la S-CSCF recibe la solicitud REGISTER y reconoce la IMPI especial y el parámetro “integridad protegida” se establece a “sí”, puede omitirse el procedimiento de autenticación para la solicitud REGISTER. Y la S-CSCF puede siempre rechazar una solicitud REGISTER con la IMPI de ICS especial, donde el parámetro de “integridad protegida” no se establece a “sí”. La S-CSCF nunca deberá proporcionar claves en el rechazo para permitir que el UE y la P-CSCF establezcan una SA para la IMPI de ICS especial.

Puesto que se introdujo el parámetro de “integridad protegida”, todas las P-CSCF deben asegurar que cuando el parámetro de “integridad protegida” para una solicitud REGISTER se establece a “sí”, esta solicitud REGISTER se recibe mediante una Asociación de Seguridad (SA) para la IMPI de ICS contenida en la solicitud REGISTER. Por lo tanto, se asegura que no ocurra el uso incorrecto del parámetro de integridad protegida por un usuario malicioso. Ya que la S-CSCF nunca puede proporcionar las claves al UE y a la P-CSCF para establecer una SA para una IMPI de

ICS especial, la S-CSCF puede únicamente recibir un REGISTER para una IMPI de ICS especial desde un IMSC, donde el parámetro “integridad protegida” se establece a “sí”. De esta manera, la S-CSCF puede omitir de manera segura la autenticación para una solicitud REGISTER de este tipo.

En otras palabras, cuando un atacante abusa de la IMPI de ICS para registrarse con el IMS, no puede establecerse la SA entre una P-CSCF y el UE, ya que no se proporcionan claves por la S-CSCF para esa IMPI de ICS. Por lo tanto, ninguna P-CSCF puede establecer el parámetro “integridad protegida” a “sí” para una solicitud REGISTER de este tipo. Y la S-CSCF puede rechazar una solicitud REGISTER de este tipo.

En aún otras palabras, se propone en la S-CSCF permitir el rechazo de la solicitud por la S-CSCF sin el aprovisionamiento de ninguna clave si se reconoce la IMPI de ICS y la bandera de integridad se establece a “no”, y para omitir autenticación adicional cuando la bandera se establece a “sí” y se reconoce la IMPI de ICS especial.

Aún además, por ejemplo una S-CSCF de la *Release* 5 puede desafiar la solicitud de REGISTER desprotegida, donde pueden proporcionarse claves para proteger la siguiente solicitud REGISTER. Y, el UE puede a continuación insertar una respuesta al desafío en una solicitud REGISTER protegida. La S-CSCF puede únicamente rechazar de manera final la solicitud REGISTER protegida, si la respuesta desde el UE es incorrecta. Hay también otros manejos excepcionales para la solicitud REGISTER protegida. Pero para una solicitud REGISTER desprotegida, la S-CSCF de la *Release* 5 puede aún intentar desafiar la solicitud, que es parte del procedimiento de autenticación.

Adicionalmente, el rechazo depende de la definición de rechazo: por ejemplo una S-CSCF de la *Release* 5 puede rechazar una solicitud REGISTER desprotegida con un desafío (por ejemplo código de respuesta 401 No autorizado). Un UE puede a continuación responder al desafío, por ejemplo, en la siguiente solicitud REGISTER. Una S-CSCF que soporta usuarios de ICS puede rechazar una solicitud REGISTER desprotegida sin desafío alguno o claves (por ejemplo código de respuesta 403 Prohibido). Ambas pueden observarse como rechazo si un rechazo es una respuesta negativa. Una S-CSCF que soporta ICS puede usar un rechazo especial. Y, este rechazo especial puede no proporcionar clave alguna para proteger la comunicación entre el UE y la P-CSCF.

[Ejemplos adicionales]

Para el fin de la presente invención como se ha descrito en el presente documento anteriormente, debería observarse que

- una tecnología de acceso puede ser cualquier tecnología por medio de la cual un equipo de usuario puede acceder a una red de acceso (o estación base, respectivamente). Puede usarse cualquier tecnología actual o futura, tal como WiMAX (Interoperabilidad Mundial para Acceso por Microondas) o WLAN (Red de Acceso Local Inalámbrica), BlueTooth, Infrarrojos y similares; aunque las tecnologías anteriores son en su mayoría tecnologías de acceso inalámbrico, por ejemplo en diferentes espectros de radio, la tecnología de acceso en el sentido de la presente invención puede implicar también tecnologías alámbricas, por ejemplo tecnologías de acceso basadas en IP como redes de cable o de línea fija.
- una red puede ser cualquier dispositivo, unidad o medios mediante los cuales una entidad de estación u otro equipo de usuario puede conectar y/o utilizar servicios ofrecidos por la red de acceso; tales servicios incluyen, entre otros, datos y/o comunicación (audio-) visual, descarga de datos etc.;
- en general, la presente invención puede ser aplicable en aquellos entornos de red/equipo de usuario que se basan en un esquema de transmisión basado en paquetes de datos de acuerdo con el que se transmiten datos en paquetes de datos y que están, por ejemplo, basados en el protocolo de internet IP. La presente invención, sin embargo, no está limitada a los mismos, es aplicable también cualquier otra versión de IP o IP móvil (MIP) presente o futura, o más en general, un protocolo que siga principios similares como (M)IPv4/6;
- un equipo de usuario puede ser cualquier dispositivo, unidad o medio mediante el cual un usuario de sistema puede experimentar servicios desde una red de acceso;
- las etapas de método es probable que se implementen como porciones de código de software y que se ejecuten usando un procesador en un elemento de red o terminal (como ejemplos de dispositivos, aparatos y/o módulos de los mismos, o como ejemplos de entidades que incluyen aparatos y/o módulos de los mismos), se encuentra el código de software independiente y puede especificarse usando cualquier lenguaje de programación conocido o desarrollado futuro siempre que se conserve la funcionalidad definida por las etapas de método;
- en general, cualquier etapa de método es adecuada para implementarse como software o por hardware sin cambiar la idea de la invención en términos de la funcionalidad implementada;
- etapas de método y/o dispositivos, unidades o medios es probable que se implementen como componentes de hardware en el IMSC y/o la S-CSCF, o cualquier módulo o módulos de los mismos, son independientes de hardware y pueden implementarse usando cualquier tecnología de hardware conocida o desarrollada futura o cualquier híbrido de estas, tales como MOS (Semiconductor de Metal Óxido), CMOS (MOS Complementario), BiMOS (MOS Bipolar), BiCMOS (CMOS Bipolar), ECL (Lógica de Emisores Acoplados), TTL (Lógica de Transistor-Transistor), etc., usando por ejemplo componentes de ASIC (CI Circuito Integrado) Específico de la Aplicación)), componentes de FPGA (Campos de Matrices de Puertas Programables), componentes de CPLD (Dispositivos de Lógica Programable Complejos) o componentes de DSP (Procesador de Señales Digitales); además, cualesquiera etapas de método y/o dispositivos, unidades o medios es probable que se implementen

como componentes de software que pueden, como alternativa, basarse en cualquier arquitectura de seguridad apta, por ejemplo de autenticación, autorización, codificación y/o protección de tráfico;

- dispositivos, unidades o medios (por ejemplo IMSC y/o S-CSCF, o uno cualquiera de sus respectivos medios) pueden implementarse como dispositivos, unidades o medios individuales, pero esto no excluye que se implementen en una forma distribuida a través de todo el sistema, siempre que se conserve la funcionalidad del dispositivo, unidad o medio;
- un aparato puede representarse por un chip de semiconductores, un conjunto de chips, o un módulo (hardware) que comprende tal chip o conjunto de chips; este, sin embargo, no excluye la posibilidad de que una funcionalidad de un aparato o módulo, en lugar de implementarse por hardware, pueda implementarse como software en un módulo (software) tal como un programa informático o un producto de programa informático que comprende porciones de código de software ejecutables para ejecución/que se ejecutan en un procesador;
- un dispositivo puede considerarse como un aparato o como un conjunto de más de un aparato, ya sea funcionalmente en cooperación entre sí o funcionalmente de manera independiente entre sí pero en un mismo alojamiento de dispositivo, por ejemplo.

Aunque la presente invención se ha descrito en el presente documento anteriormente con referencia a realizaciones particulares de la misma, la presente invención no está limitada a la misma y pueden hacerse diversas modificaciones a la misma.

Para facilidad de aclaración, la siguiente tabla proporciona un estudio de las abreviaturas usadas en la descripción anterior. Se ha de observar que una “s” que sigue una abreviatura representa el plural de esta abreviatura, por ejemplo, “los UE” representa “equipos de usuario”.

3GPP	proyecto común de tecnologías inalámbricas de la 3ª generación
TR/TS	informe técnico/especificación técnica
UE	equipo de usuario
CS	conmutación de circuitos
PS	conmutación de paquetes
IP	protocolo de Internet
IMS	subsistema multimedia de IP
ICS	servicio centralizado de IMS
IMPI	identidad de usuario privada de IMS
MSC	centro de conmutación móvil
IMSC	MSC mejorado de ICS
SA	asociación de seguridad
CSCF	función de control de sesión de llamada
PANI	información de red de acceso P
P-CSCF	CSCF de intermediario
S-CSCF	CSCF de servicio

REIVINDICACIONES

1. Un método, que comprende:
transmitir, después del registro satisfactorio de un terminal en una primera entidad de red (2021), un mensaje de registro mediante la primera entidad de red (2021) a una segunda entidad de red (2023), en donde la primera entidad de red (2021) es un centro de conmutación móvil de servicios centralizados del subsistema multimedia del protocolo de Internet,
caracterizado por que el mensaje de registro comprende información de identidad de terminal e información de indicación de integridad y en el que la información de indicación de integridad indica el registro satisfactorio del terminal mediante la primera entidad de red (2021).

2. El método de acuerdo con la reivindicación 1, que comprende adicionalmente generar el mensaje de registro mediante la primera entidad de red.

3. El método de acuerdo con las reivindicaciones 1 o 2, en el que el mensaje de registro es uno de un mensaje de registro inicial, un mensaje de repetición de registro y un mensaje de anulación de registro.

4. Un método, que comprende:
procesar, mediante una primera entidad de red (2023), después de la recepción de un mensaje de registro desde una segunda entidad de red (2021), caracterizado por comprender el mensaje de registro información de identidad de terminal e información de indicación de integridad, basándose el mensaje de registro recibido en la información de identidad de terminal y la información de indicación de integridad de manera que, si la indicación de integridad indica un registro satisfactorio del terminal mediante la segunda entidad de red (2021), se omite un procedimiento de autenticación del terminal, en donde la segunda entidad de red (2021) es un centro de conmutación móvil de servicios centralizados del subsistema multimedia del protocolo de Internet.

5. El método de acuerdo con la reivindicación 4, que comprende adicionalmente recibir el mensaje de registro.

6. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el que el mensaje de registro es un mensaje de registro de protocolo de iniciación de sesión.

7. Un aparato (2021), que comprende:
medios para transmitir, después del registro satisfactorio de un terminal en el aparato, un mensaje de registro a una primera entidad de red (2023), en donde el aparato (2021) es un centro de conmutación móvil de servicios centralizados del subsistema multimedia del protocolo de Internet,
caracterizado por que el mensaje de registro comprende información de identidad de terminal e información de indicación de integridad y en el cual la información de indicación de integridad indica el registro satisfactorio del terminal mediante el aparato (2021).

8. El aparato de acuerdo con la reivindicación 7, que comprende adicionalmente medios para generar el mensaje de registro.

9. El aparato de acuerdo con las reivindicaciones 7 u 8, en el que el mensaje de registro es uno de un mensaje de registro inicial, un mensaje de repetición de registro y un mensaje de anulación de registro.

10. Un aparato (2023), que comprende:
medios para procesar, después de la recepción de un mensaje de registro desde una primera entidad de red (2021), caracterizado por comprender el mensaje de registro información de identidad de terminal e información de indicación de integridad, basándose el mensaje de registro recibido en la información de identidad de terminal y la información de indicación de integridad de manera que, si la indicación de integridad indica un registro satisfactorio del terminal mediante la primera entidad de red (2021), se omite un procedimiento de autenticación del terminal (201), en donde la primera entidad de red (2021) es un centro de conmutación móvil de servicios centralizados del subsistema multimedia del protocolo de Internet.

11. El aparato (2023) de acuerdo con la reivindicación 10, que comprende adicionalmente medios para recibir el mensaje de registro.

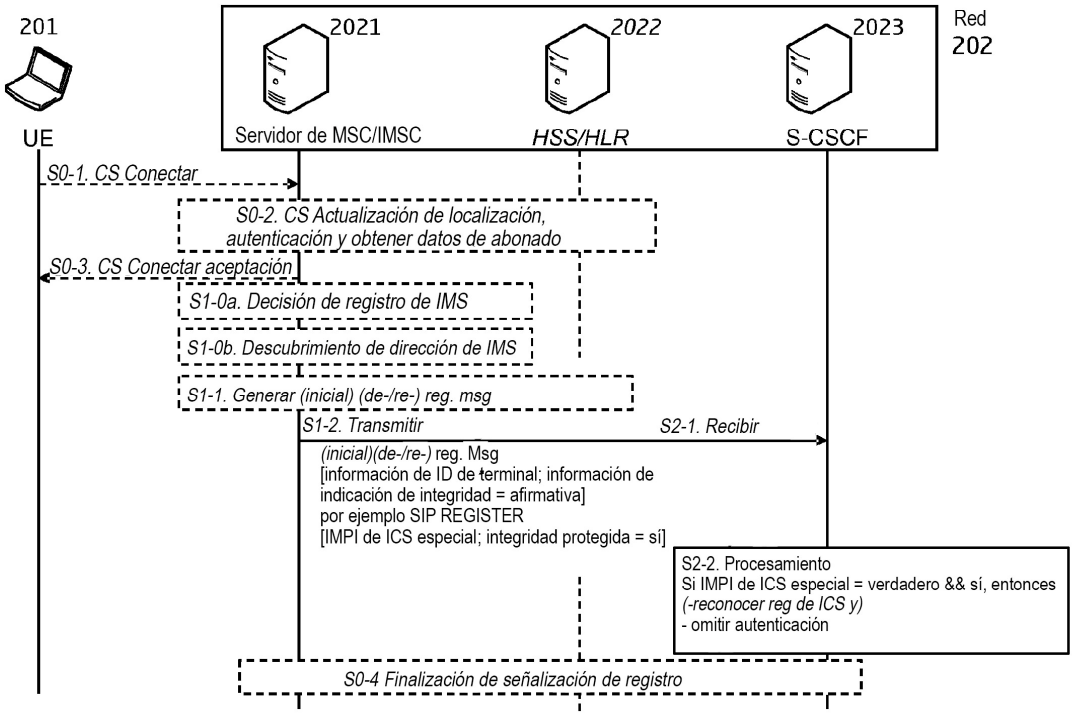
12. El aparato (2023) de acuerdo con una cualquiera de las reivindicaciones 7 a 11, en el que el mensaje de registro es un mensaje de registro de protocolo de iniciación de sesión.

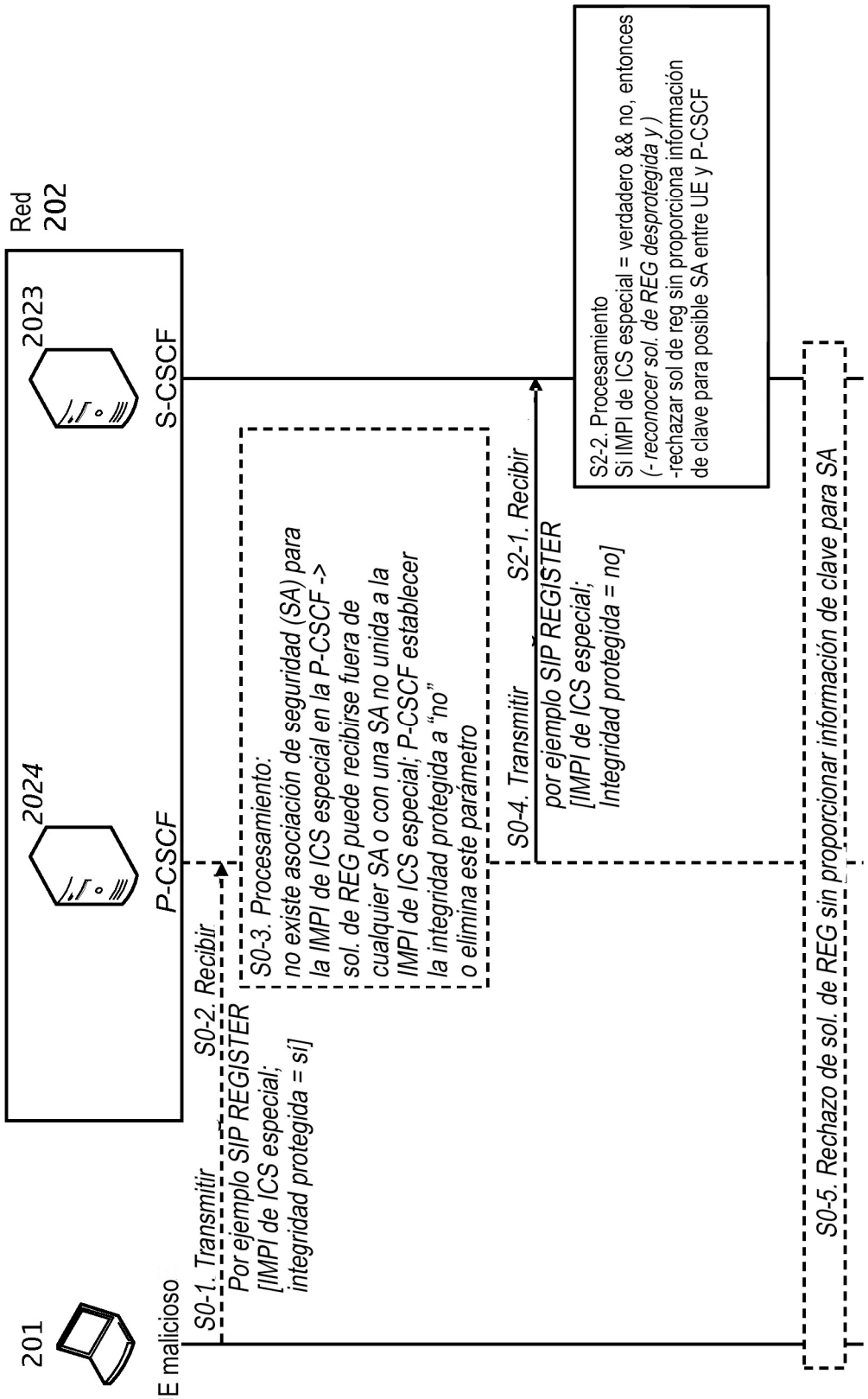
13. El aparato de acuerdo con una cualquiera de la reivindicación 10, la reivindicación 11 y la reivindicación 12 dependiendo de las reivindicaciones 10 u 11, en donde el aparato está constituido por una función de control de sesión de llamada de servicio.

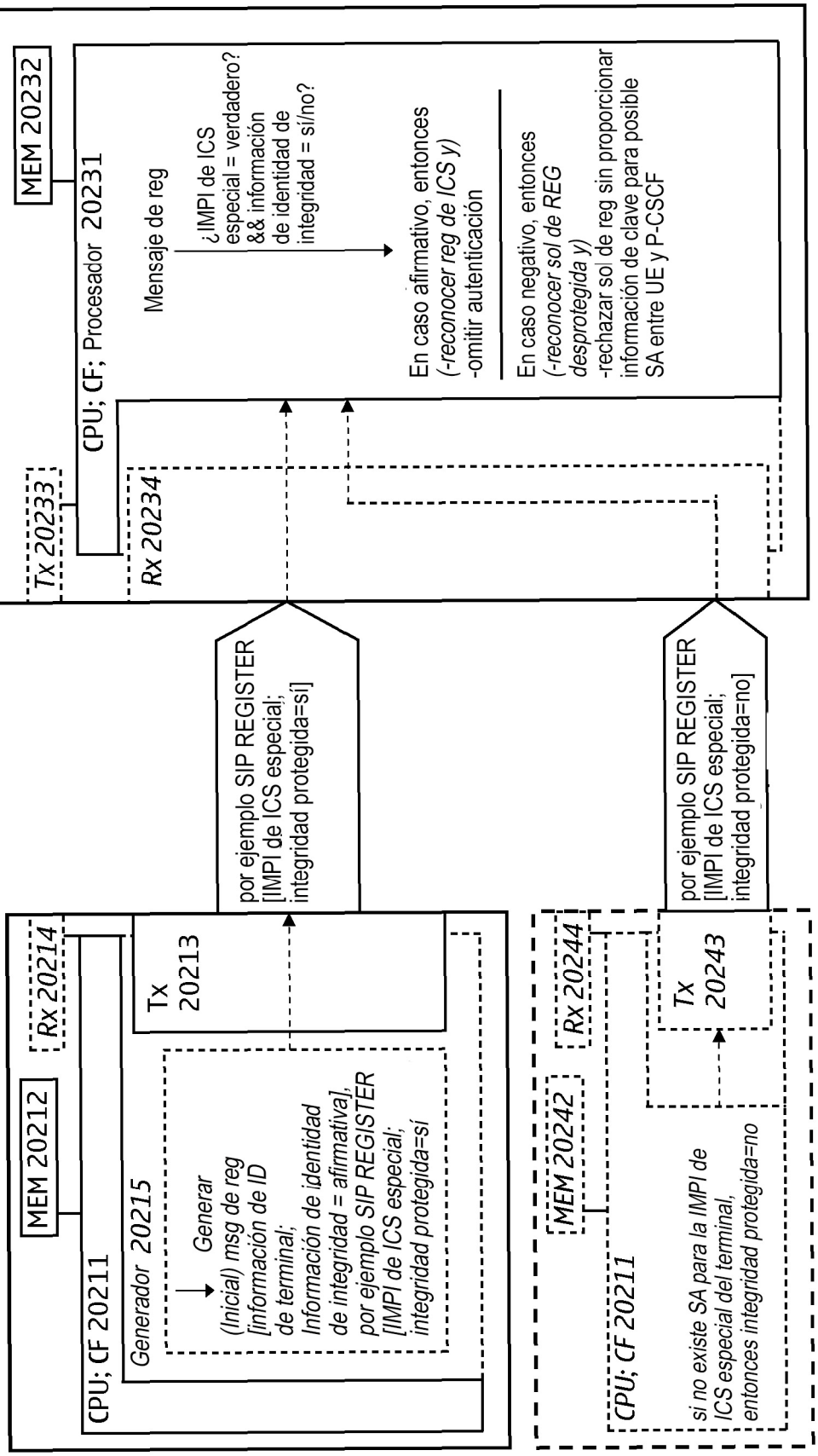
14. Un sistema, que comprende:

un terminal (201);
un aparato (2021) de acuerdo con una cualquiera de la reivindicación 7, la reivindicación 9 o la reivindicación 12 dependiendo de las reivindicaciones 7 a 9; y
un aparato (2023) de acuerdo con una cualquiera de la reivindicación 10, la reivindicación 11, la reivindicación 12 dependiendo de las reivindicaciones 10 u 11, o la reivindicación 13.

15. Un producto de programa informático que comprende medios de código para realizar etapas de método de un método de acuerdo con una cualquiera de las reivindicaciones 1 a 6, cuando se ejecuta en un medio o un módulo de procesamiento.


201
UE
2021
Servidor de MSC/IMSC
2022
HSS/HLR
2023
S-CSCF
Red
202
S0-1. CS Conectar
S0-2. CS Actualización de localización, autenticación y obtener datos de abonado
S0-3. CS Conectar aceptación
S1-0a. Decisión de registro de IMS
S1-0b. Descubrimiento de dirección de IMS
S1-1. Generar (inicial) (de-/re-) reg. msg
S1-2. Transmitir
S2-1. Recibir
(inicial)(de-/re-) reg. Msg
[información de ID de terminal; información de indicación de integridad = afirmativa]
por ejemplo SIP REGISTER
[IMPI de ICS especial; integridad protegida = sí]
S2-2. Procesamiento
Si IMPI de ICS especial = verdadero && sí, entonces
(-reconocer reg de ICS y)
- omitir autenticación
S0-4 Finalización de señalización de registro


Red
202
2023
S-CSCF
2024
P-CSCF
201
UE malicioso
S0-1. Transmitir
Por ejemplo SIP REGISTER
[IMPI de ICS especial;
integridad protegida = sí]
S0-2. Recibir
S0-3. Procesamiento:
no existe asociación de seguridad (SA) para
la IMPI de ICS especial en la P-CSCF ->
sol. de REG puede recibirse fuera de
cualquier SA o con una SA no unida a la
IMPI de ICS especial; P-CSCF establecer
la integridad protegida a "no"
o elimina este parámetro
S0-4. Transmitir
por ejemplo SIP REGISTER
[IMPI de ICS especial;
Integridad protegida = no]
S2-1. Recibir
S2-2. Procesamiento
Si IMPI de ICS especial = verdadero && no, entonces
(- reconocer sol. de REG desprotegida y)
-rechazar sol de reg sin proporciona información
de clave para posible SA entre UE y P-CSCF
S0-5. Rechazo de sol. de REG sin proporcionar información de clave para SA


MEM 20232
CPU; CF; Procesador 20231
Tx 20233
Rx 20234
Mensaje de reg
¿IMPI de ICS especial = verdadero? && información de identidad de integridad = sí/no?
En caso afirmativo, entonces
(-reconocer reg de ICS y)
-omitir autenticación
En caso negativo, entonces
(-reconocer sol de REG desprotegida y)
-rechazar sol de reg sin proporcionar información de clave para posible SA entre UE y P-CSCF
por ejemplo SIP REGISTER
[IMPI de ICS especial;
integridad protegida=sí]
por ejemplo SIP REGISTER
[IMPI de ICS especial;
integridad protegida=no]
MEM 20212
Rx 20214
CPU; CF 20211
Generador 20215
Generar
(Inicial) msg de reg
[información de ID
de terminal;
Información de identidad
de integridad = afirmativa],
por ejemplo SIP REGISTER
[IMPI de ICS especial;
integridad protegida=sí
Tx
20213
MEM 20242
Rx 20244
CPU; CF 20211
si no existe SA para la IMPI de
ICS especial del terminal,
entonces integridad protegida=no
Tx
20243