(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 765 739**

(51) Int. CI.:

G06F 21/31 (2013.01)
H04W 4/70 (2008.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04W 12/08 (2009.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.11.2016 PCT/EP2016/076662**

(87) Fecha y número de publicación internacional: **08.06.2017 WO17092968**

(96) Fecha de presentación y número de la solicitud europea: **04.11.2016 E 16794259 (8)**

(97) Fecha y número de publicación de la concesión europea: **16.10.2019 EP 3347849**

(54) Título: **Método, dispositivo y sistema para autenticarse en una red móvil y un servidor para autenticar dispositivos en una red móvil**

(30) Prioridad:

02.12.2015 EP 15306916

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.06.2020

(73) Titular/es:

THALES DIS FRANCE SA (100.0%)
6, rue de la Verrerie
92190 Meudon , FR

(72) Inventor/es:

MAVRAKIS, DANIEL;
ZANNIN, FRANÇOIS;
TROADEC, HERVÉ;
KUC, JEAN-FRANÇOIS y
GIRARD, PIERRE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método, dispositivo y sistema para autenticarse en una red móvil y un servidor para autenticar dispositivos en una red móvil

Campo de la invención

La invención se refiere en general a un método para autenticarse en una red móvil.

Además, la invención se refiere a un servidor para autenticar dispositivos en una red móvil.

Además, la invención también se refiere a un dispositivo para autenticarse en una red móvil.

Por último, la invención se refiere a un sistema para autenticarse también en una red móvil.

El sistema comprende al menos un servidor y un dispositivo. El dispositivo se conecta al servidor. El dispositivo puede ser en particular una tarjeta universal de circuito integrado incrustada (o eUICC) dentro de un entorno de máquina a máquina (o M2M) o Internet de las cosas u objetos (o IoT) o extraíble, como un chip incluido dentro de una tarjeta inteligente, como, por ejemplo, una tarjeta de tipo módulo de identidad de abonado (o SIM) (o similar), desde un dispositivo anfitrión de elemento seguro (o SE), como, por ejemplo, un teléfono móvil.

Dentro de la presente descripción, un SE es un objeto inteligente que incluye un chip que protege físicamente el acceso a los datos almacenados y está destinado a comunicar datos con el mundo exterior, como, por ejemplo, un dispositivo M2M, tal como un dispositivo anfitrión de SE.

Estado de la técnica

El mercado M2M crece año tras año y continúa creciendo. Los objetos conectados correspondientes deberían alcanzar alrededor de 50.000 millones de unidades en 2020. Se sabe que una eUICC identifica un abono mediante el uso de una identidad de abonado móvil internacional (o IMSI), como recurso.

Sin embargo, una solución conocida de este tipo debería experimentar una escasez de recursos. De hecho, la IMSI tiene sólo mil millones de valores para su número de identificación de abono móvil (o MSIN) que se representa con nueve o diez dígitos, como un campo de datos del formato de datos IMSI.

Por lo tanto, existe la necesidad de proporcionar una solución que permita usar eficientemente el recurso disponible, para mitigar el coste de un recurso.

El documento US 2012079581 A1 da a conocer una solución de la técnica anterior.

El documento US 20030186681 A1 da a conocer una técnica en la que un dispositivo usa un único identificador de abono para intentar autenticarse y volver a autenticarse en una red móvil.

Sumario de la invención

La invención propone una solución para satisfacer la necesidad especificada anteriormente, proporcionando un método para autenticar un dispositivo en una red móvil según la reivindicación 1, un servidor correspondiente según la reivindicación 8, un dispositivo correspondiente según la reivindicación 9 y un sistema correspondiente según la reivindicación 12.

El principio de la invención consiste en que un servidor identifica y autentica un dispositivo que usa consecutivamente un primer y un segundo identificador de abono temporal. En primer lugar, cuando sólo se usa el primer identificador de abono temporal, el dispositivo no puede autenticarse en el servidor basándose en unos primeros datos enviados por el dispositivo. En segundo lugar, cuando sólo se usa el segundo identificador de abono temporal, el dispositivo se autentica con éxito en el servidor basándose en los identificadores de abono temporales primero y segundo y unos segundos datos enviados por el dispositivo.

Cabe mencionar que el servidor sólo puede identificar, de manera única, el dispositivo (interlocutor) una vez que el servidor ha recibido un par de los identificadores de abono temporales primero y segundo.

Debe observarse que sólo un identificador de abono temporal está activo en un momento dado, a saber, el primer identificador de abono temporal está activo en primer lugar y el segundo identificador de abono temporal está activo en segundo lugar.

Una vez que el servidor ha identificado el par de identificadores de abono temporales primero y segundo, el servidor también puede determinar uno o varios secretos compartidos con el dispositivo, para autenticar el dispositivo.

La solución de la invención puede ser automática y, por lo tanto, conveniente para un posible usuario, propietario o administrador del dispositivo. Por lo tanto, la solución de la invención es fácil de usar.

La solución de la invención no necesita que el servidor acceda a una información, como, por ejemplo, una ubicación de dispositivo y/o uno o varios identificadores relacionados con el dispositivo u otro dispositivo que actúe conjuntamente con el dispositivo, distinta de los identificadores de abono temporales primero y segundo, los datos primeros y segundos.

La solución de la invención es segura ya que el dispositivo logra autenticarse en el servidor una vez que el dispositivo y el servidor usan tanto el segundo identificador de abono temporal, después del primer identificador de abono temporal, como uno o varios secretos compartidos asociados, como, por ejemplo, una clave compartida asociada para autenticarse en la red móvil.

La solución de la invención permite usar, por ejemplo, una flota de N^2 dispositivos, un intervalo de sólo 2*N identificadores de abono temporales que se asignan por pares de un primer y un segundo identificador de abono temporal a los dispositivos y luego se usan temporalmente durante un período de tiempo para una identificación y una autenticación de los dispositivos. Por lo tanto, se selecciona un segundo identificador de abono temporal en los identificadores de abono temporales disponibles del intervalo, como un número limitado de N posibles segundos identificadores de abono temporales, antes de un procedimiento de activación de dispositivo. El procedimiento de activación de dispositivo permite asignar al dispositivo, como un perfil de abono, al menos un identificador de abono definitivo, que está fuera del/de los intervalo(s) de los identificadores de abono temporales primero y segundo.

Dado que los 2*N identificadores de abono temporales que se usan para un procedimiento de activación de dispositivo son menos que un recuento de los dispositivos que no están activados, existe un riesgo de colisión. La colisión ocurre cuando dos o más dispositivos usan ambos un mismo identificador de abono temporal, como un primer o un segundo identificador de abono temporal, a un mismo tiempo. Se elige un algoritmo para seleccionar el segundo identificador de abono temporal compartido entre el dispositivo y el servidor, para reducir, en la medida de lo posible, el riesgo de colisión.

Ventajosamente, el dispositivo u otro dispositivo que actúa conjuntamente con el dispositivo y el servidor determinan el segundo identificador de abono temporal usando al menos el primer identificador de abono temporal.

En consecuencia, el segundo identificador temporal está enlazado al primer identificador de abono temporal. El enlace puede depender de uno o varios parámetros que se aprovisionan previamente en el lado del dispositivo o, por ejemplo, un primer desafío, que el servidor envía al dispositivo durante una primera sesión de autenticación.

Por lo tanto, el servidor y el dispositivo determinan, de manera común, el segundo identificador de abono temporal que depende de al menos el primer identificador de abono temporal enviado previamente por el dispositivo al servidor durante la primera sesión de autenticación.

El dispositivo incluye un terminal, un terminal de usuario o un SE.

El elemento seguro puede fijarse, soldarse o extraerse de un dispositivo anfitrión de SE.

La invención no impone ninguna restricción en cuanto al tipo de SE.

Como SE extraíble, puede ser una tarjeta de tipo SIM, un módulo extraíble seguro (o SRM), una llave inteligente del tipo USB (acrónimo de “Universal Serial Bus”, bus serial universal), una tarjeta de tipo (micro-) Secure Digital (segura digital) (o SD) o una tarjeta de tipo multimedia (o MMC) o una tarjeta de cualquier formato para acoplarse o conectarse a un dispositivo anfitrión de SE.

Breve descripción de los dibujos

Podrán comprenderse características y ventajas adicionales de la invención más claramente después de leer una descripción detallada de una realización preferida de la invención, dada como un ejemplo indicativo y no limitativo, junto con los siguientes dibujos:

- la figura 1 es un esquema simplificado de una realización a modo de ejemplo de una red móvil con dos servidores remotos y un equipo terminal con un terminal y un SE, estando dispuesto el equipo terminal para activar un primer y un segundo identificador de abono temporal, para autenticarse en primer lugar sin éxito con el primer identificador de abono temporal y en segundo lugar con éxito en la red móvil con el segundo identificador de abono temporal, según la invención; y

- la figura 2 ilustra un ejemplo de un flujo de mensajes intercambiados entre el equipo terminal y la red de la figura 1, de modo que el equipo terminal se identifica, de una manera única, en la red usando los identificadores de abono temporales primero y segundo y se autentica usando, durante una primera sesión de autenticación, una primera clave no compartida con la red y, durante una segunda sesión de autenticación, una segunda clave compartida con la red, respectivamente.

Descripción detallada

A continuación en el presente documento, se considera un caso en el que el método de la invención para

autenticarse en una red móvil se implementa mediante un SE, una máquina o un objeto, como un terminal y un dispositivo anfitrión de SE, y un servidor remoto.

El SE puede ser un chip incrustado, como, por ejemplo, una eUICC, como un chip soldado, posiblemente de manera extraíble, en una placa de circuito impreso (o PCB) del terminal, un entorno de ejecución de confianza (o TEE), como una zona segura de un procesador de terminal y un entorno de tiempo de ejecución seguro.

El elemento seguro o SE puede tener diferentes factores de forma.

En lugar de estar incrustado, el chip puede portarse por un medio, tal como, por ejemplo, una tarjeta o una llave, como, por ejemplo, una llave USB.

Según otra realización (no representada), el método de la invención para autenticarse en una red móvil se implementa mediante un dispositivo, como una entidad independiente, en un lado de cliente. En otras palabras, el dispositivo, como, por ejemplo, un terminal o un terminal de usuario, no actúa conjuntamente con ningún dispositivo, como, por ejemplo, un SE, para autenticarse en la red usando consecutivamente un primer identificador de abono temporal con una primera clave no compartida con el lado de servidor y un segundo identificador de abono temporal con una segunda clave compartida con el lado de servidor. Según una realización de este tipo (no representada), el dispositivo está adaptado para llevar a cabo las funciones que se describen a continuación y que lleva a cabo el SE y su terminal anfitrión. Por lo tanto, un terminal o un terminal de usuario pueden soportar una aplicación de autenticación de la invención que se soporta en un entorno no de confianza.

Naturalmente, la realización descrita a continuación en el presente documento es sólo con fines de ejemplo y no se considera que reduzca el alcance de la presente invención.

La figura 1 muestra esquemáticamente un equipo 10 terminal (o TEQ) que está conectado a una red 100 móvil que incluye un primer servidor 16 remoto y un segundo servidor 18 remoto.

El TEQ 10, como un sistema para autenticarse en una red móvil, comprende un elemento 12 seguro con un chip, y una máquina en un contexto M2M (o un objeto en un contexto IoT), como un terminal 14.

En lugar de una máquina o un objeto, el terminal o un terminal de usuario puede ser cualquier otro dispositivo, incluido un(os) (micro)procesador(es), como medios para procesar datos, que comprende(n) o está(n) conectado(s) a medios de comunicación inalámbrica para intercambiar datos con el exterior, y que comprende(n) o está(n) conectado(s) a una(s) memoria(s), como medios para almacenar datos.

Dentro de la presente descripción, el adjetivo “inalámbrica” usado dentro de la expresión “medios de comunicación inalámbrica” denota en particular que los medios de comunicación se comunican a través de uno o varios enlaces de radiofrecuencia (o RF) de largo alcance (o LR).

La RF de LR puede fijarse a varios cientos de MHz alrededor de, por ejemplo, 850, 900, 1800, 1900 y/o 2100 MHz.

El terminal o el terminal de usuario puede ser fijo (es decir, no móvil) o móvil.

El terminal o el terminal de usuario puede ser, entre otros, un vehículo, un teléfono móvil, un asistente digital personal (PDA), un vehículo, una caja de configuración, un ordenador de tableta, un ordenador personal (o PC), un ordenador de escritorio, un ordenador portátil, un reproductor de vídeo, un reproductor de audio, una televisión (o TV) portátil, un reproductor multimedia, una consola de juegos, un equipo ultraportátil y/o cualquier tipo de dispositivo electrónico que pueda emitir, de manera consecutiva, un primer y un segundo identificador de abono temporal junto con datos de autenticación no válidos (o falsos) y datos de autenticación válidos respectivamente.

Por motivos de simplicidad, el elemento 12 seguro, el terminal 14, el primer servidor 16 remoto, el segundo servidor 18 remoto y la red 100 móvil se denominan a continuación el SE 12, el TE 14, el primer servidor 16, el segundo servidor 18 y la red 100 respectivamente.

El SE 12 incluye una eUICC, como un chip incrustado, que está bajo el control del TE 14, como un dispositivo anfitrión de SE, en el lado de cliente, y bajo el control de una entidad de tipo de registro de posiciones base (o RPP) que se denomina RPP a continuación, como el segundo servidor 18.

En lugar de un SE integrado, el SE puede ser extraíble y portarse mediante una tarjeta o una llave del tipo USB, una tarjeta de tipo (micro)SD, una MMC o cualquier medio para conectarse o acoplarse, a través de un contacto y/o un enlace sin contacto, a un dispositivo anfitrión de SE.

El adjetivo “sin contacto” significa que cada uno del SE 12 y el TE 14 está conectado a o incluye medios para comunicar datos mientras usa preferiblemente un enlace de radiofrecuencia (o RF) de corto alcance (o SR). El enlace de RF de SR puede estar relacionado con cualquier tecnología que permita al SE 12 intercambiar datos con el TE 14. La RF de SR puede fijarse a 13,56 MHz y estar relacionada con una tecnología de tipo de comunicación de campo próximo (o NFC) o similar, como una tecnología sin contacto.

El SE 12 incluye un(os) (micro)procesador(es) 122 (y/o un(os) (micro)controlador(es)), como medios de procesamiento de datos, una(s) memoria(s) 124, como medios de almacenamiento de datos, y una(s) interfaz/interfaces 126 de entrada/salida (o E/S), conectados todos ellos a través de un bus 123 de datos y control interno. El procesador 122 procesa, controla y comunica datos internamente a todos los demás componentes incorporados dentro del chip y, a través de la(s) interfaz interfaz/interfaces 126 de E/S, con el chip exterior. El procesador 122 puede iniciar acciones, para interactuar directamente con el mundo exterior, de manera independiente del dispositivo anfitrión de SE. Tal capacidad de interacción por iniciativa del SE 12 también se conoce como capacidad proactiva. Según una realización preferida, el SE 12 puede usar comandos de tipo de kit de herramientas SIM (o STK) (o similares), como comandos proactivos. El procesador 122 ejecuta o utiliza una o varias aplicaciones, incluida la aplicación de autenticación de la invención. La memoria 124 almacena preferiblemente un identificador de tarjeta de circuito integrado (o ICCID) único, como un identificador relacionado con el SE 12. La memoria 124 almacena un conjunto de uno o varios primeros identificadores de abono temporales predeterminados, denominados IMSIi a continuación, en asociación con un conjunto de uno o varios segundos identificadores de abono temporales predeterminados, denominados IMSIj a continuación. Los identificadores de abono temporales primero y segundo representan, de manera acumulativa, un número de 2*N de identificadores de abono temporales. Los identificadores de abono temporales primero y segundo son preferiblemente distintos entre sí. El segundo identificador de abono temporal está preferiblemente enlazado al primer identificador de abono temporal usado, para evitar el riesgo de colisión que puede ocurrir con uno o varios otros dispositivos cliente. Entre los otros dispositivos cliente, algunos de los otros dispositivos cliente pueden estar inactivos, es decir, no activados, pero pueden activarse al usar también dos identificadores de abono temporales. Según una realización particular, por ejemplo, una tabla de correspondencia incluye, para una i-ésima fila, un IMSIi, como un primer identificador de abono temporal, y, para una j-ésima columna, un IMSIj, como un segundo identificador de abono temporal, en el que i y j representan un índice de fila y un índice de columna respectivamente. Sólo un identificador de abono temporal, es decir, un IMSIi o un segundo identificador de abono temporal predeterminado IMSIj, está activo en un momento dado. La memoria 124 también almacena una clave única Ki,j para autenticarse en la red 100, como un secreto compartido con el lado de servidor, en asociación con al menos el IMSIj o cada par de IMSIi e IMSIj.

Según la realización particular dada, la tabla de correspondencia incluye además, para la i-ésima fila y la j-ésima columna, la clave asociada Ki,j, como un secreto compartido con el lado de servidor, para autenticarse en la red 100, durante una segunda sesión de autenticación .

El conjunto de uno o varios pares de IMSIi e IMSIj asociado y su clave asociada Ki,j para autenticarse en la red 100 se comparten con una base de datos almacenada en una memoria accesible en el lado de servidor.

Según otra realización, en lugar de tener un único secreto compartido entre el SE 12 y el lado de servidor, se comparten dos o más secretos entre el SE 12 y la base de datos accesible desde el lado de servidor.

El/los secreto(s) se usa(n) como una entrada o un(os) parámetro(s) de configuración de un algoritmo, como, por ejemplo, un Milenage, para autenticarse en la red 100. El algoritmo de autenticación de red también se comparte entre el SE 12 y la base de datos accesible en el lado de servidor.

La memoria 124 puede almacenar uno o varios identificadores, como, por ejemplo, un(os) identificador(es) de máquina (o MI) y/o una(s) identidad(es) de equipo de estación móvil internacional (o IMEI), relacionados con un(os) dispositivo(s) anfitrión/anfitriones de SE. El/los identificador(es) relacionado(s) con uno o varios dispositivos anfitriones de SE predeterminados, como un(os) parámetro(s) de configuración, pueden haberse cargado previamente durante un procedimiento de fabricación.

La memoria 124 puede almacenar datos relacionados con un identificador uniforme de recursos (o URI), un localizador uniforme de recursos (o URL) y/o una dirección de tipo de protocolo de Internet (o IP) de una(s) entidad(es) externas a la(s) que dirigirse, como, por ejemplo , el segundo servidor 18.

La memoria 124 almacena un sistema operativo (o SO).

El SE 12 está configurado para activar sólo un IMSIi, como un primer IMSI temporal.

El SE 12 puede enviar, por iniciativa propia, al dispositivo anfitrión de SE, un comando proactivo para enviar a la red 100 un(os) mensaje(s), como, por ejemplo, un servicio de mensajes cortos (o SMS), datos de servicio suplementario sin estructura (o USSD) y/o mensaje(s) de tipo de datos o similares, incluidos datos para identificarse y/o autenticarse en la red 100.

Un procedimiento de autenticación de dispositivo anfitrión de SE se inicia preferiblemente por el dispositivo anfitrión de SE cuando lo solicita la red 100.

El SE 12 está configurado para enviar, preferiblemente a petición de un dispositivo anfitrión de SE, el IMSIi a un servidor que se usa para autenticar el SE 12 en la red 100. Dicho envío IMSIi se incluye dentro de una primera sesión de autenticación entre el dispositivo anfitrión de SE y el lado de servidor.

El SE 12 puede recibir una solicitud para enviar una primera respuesta. Tal solicitud de envío de primera respuesta

incluye preferiblemente un primer desafío.

El SE 12 está dispuesto para no autenticarse en el lado de servidor usando el IMSIi durante la primera sesión de autenticación.

Según una realización particular, el SE 12 usa el algoritmo de autenticación de red, el primer desafío y una clave para no autenticarse en la red 100, para generar dinámicamente unos primeros datos. La clave para no autenticarse en la red 100 sólo se almacena dentro de la memoria 124. La clave para no autenticarse en la red 100 puede haber sido aprovisionada previamente durante un procedimiento de fabricación de SE o generada dinámicamente por, por ejemplo, un generador (pseudo)aleatorio. La clave para no autenticarse en la red 100 no se comparte con el lado de servidor.

En lugar del algoritmo de autenticación de red, el primer desafío y la clave para no autenticarse en la red 100, el SE 12 puede usar otro algoritmo de generación de primeros datos, como, por ejemplo, un algoritmo de generación (pseudo)aleatorio, que genera dinámicamente los primeros datos. El algoritmo de generación de primeros datos no se comparte con el lado de servidor.

En lugar de generar dinámicamente los primeros datos, los primeros datos están predefinidos y almacenados estáticamente en la memoria 124 en asociación con el IMSIi y tienen un valor predeterminado, como, por ejemplo, cero o uno para todos los bits de primeros datos, que debe interpretarse en el lado de servidor como datos de autenticación no válidos o falsos.

Se pretende que los primeros datos sean datos de autenticación no válidos o falsos, de modo que los primeros datos enviados no coincidan con ningún dato de autenticación esperado, como un primer resultado esperado generado en el lado de servidor durante la primera sesión de autenticación.

El SE 12 está adaptado para enviar al lado de servidor los primeros datos, como una primera respuesta.

El dispositivo anfitrión de SE (o el SE 12) está dispuesto preferiblemente para recibir un primer mensaje de resultado que incluye un fallo de autenticación basado en los primeros datos.

El SE 12 y el lado de servidor pueden usar el IMSIi enviado por el SE 12 durante la primera sesión de autenticación y uno o varios parámetros de entrada relacionados con un algoritmo de determinación de IMSIj compartido con el lado de servidor, para determinar dinámicamente el IMSIj que va a usarse para iniciar una segunda sesión de autenticación.

El IMSIj se determina preferiblemente, para evitar una colisión de un(os) mismo(s) IMSI temporal(es) usado(s) por uno o varios otros dispositivos cliente. Más exactamente, el IMSIj se determina preferiblemente de modo que dos o más dispositivos cliente que también determinan un IMSIj, como un segundo IMSI temporal, no usen un mismo IMSIj al mismo tiempo durante una segunda sesión de autenticación.

Según una realización particular, el primer desafío, como un parámetro de entrada para un algoritmo de determinación de IMSIj compartido, se usa para determinar dinámicamente el IMSIj. Parte, como, por ejemplo, uno, dos o más bits predeterminados o todos los bits relacionados con el primer desafío se usa, por ejemplo, para determinar un índice j relacionado con una j-ésima columna en la que el IMSIj está situado en asociación con el IMSIi que está situado en un índice i relacionado con la i-ésima fila.

Según otra realización, uno o varios parámetros de entrada se aprovisionan previamente al SE 12 y se comparten con el lado de servidor y se identifican usando el primer desafío recibido del lado de servidor y/u otro(s) parámetro(s) que se usa(n) para seleccionar el IMSIj asociado. El SE 12 y el lado de servidor están dispuestos para determinar dinámicamente, de manera común, el IMSIj asociado con el IMSIi para el SE 12 en cuestión El/los parámetro(s) de entrada seleccionado(s) no se comparte(n) con ningún otro dispositivo cliente que va a identificarse en la red 100 al mismo tiempo, para evitar cualquier riesgo de colisión para el IMSIj asociado, como el segundo IMSI temporal.

Después de un primer intento fallido de autenticarse en la red 100, el SE 12 está configurado para luego desactivar el IMSIi y activar el IMSIj, como un segundo IMSI temporal.

El SE 12 está adaptado para enviar al servidor el IMSIj usado para autenticar el SE 12 en la red 100. Tal envío de IMSIj inicia una segunda sesión de autenticación entre el SE 12 y el lado de servidor.

El SE 12 puede recibir una solicitud para enviar una segunda respuesta. Tal solicitud de envío de segunda respuesta incluye preferiblemente un segundo desafío.

El SE 12 está dispuesto para autenticarse exitosamente en el lado de servidor usando el IMSIj durante la segunda sesión de autenticación.

El SE 12 está configurado para generar dinámicamente unos segundos datos.

Según la realización particular, el SE 12 usa el algoritmo de autenticación de red, el segundo desafío y una clave Ki,j

para autenticarse en la red 100, para generar dinámicamente los segundos datos. El SE 12 y el lado de servidor están dispuestos para determinar posiblemente de forma dinámica, de manera común, la clave Ki,j para autenticarse en la red 100 en asociación con el IMSIj o el par del IMSIi y el IMSIj asociado.

La clave Ki,j para autenticarse en la red 100 es preferiblemente única y está asociada con el SE12 que ha usado el IMSIj o el par del IMSIi y el IMSIj.

La clave Ki,j para autenticarse en la red 100 se almacena en la memoria 124 y en el lado de servidor. La clave Ki,j para la autenticación en la red 100 puede haberse aprovisionado previamente durante un procedimiento de fabricación de SE o generado dinámicamente por un algoritmo de generación de clave compartido entre el SE 12 y el lado de servidor.

El SE 12 está adaptado para enviar al lado de servidor los segundos datos, como una segunda respuesta.

Se pretende que los segundos datos sean datos de autenticación válidos o genuinos. En otras palabras, los segundos datos enviados coinciden con unos segundos datos de autenticación esperados, como un segundo resultado esperado generado dinámicamente en el lado de servidor durante la segunda sesión de autenticación.

El dispositivo 14 anfitrión de SE (o el SE 12) está dispuesto para recibir un segundo mensaje de resultado que incluye un éxito de autenticación basado en el par del IMSIi y su IMSIj asociado y los segundos datos.

El SE 12 está así dispuesto para identificarse y para autenticarse en la red 100 en dos sesiones de autenticación consecutivas mientras se usan dos IMSI temporales consecutivos. Los dos IMSI temporales se determinan preferiblemente de modo que se evite un riesgo de colisión con uno o varios otros dispositivos cliente, tales como SE, que intentan identificarse simultáneamente en la red 100.

Para evitar un riesgo de colisión, el SE 12 comparte con el lado de servidor dos o más pares de IMSI temporales primero y segundo y sus respectivas claves asociadas para la autenticación en la red 100.

El SE 12 incluye una o varias interfaces 126 de E/S para intercambiar datos, a través de un contacto y/o un enlace 13 sin contacto, con el TE 14, como un dispositivo anfitrión de SE.

El TE 14 constituye una máquina (o similar) de una infraestructura de tipo M2M que incluye una flota de máquinas.

El TE 14 puede desempeñar un papel de un módem, para intercambiar, de manera inalámbrica, datos con la red 100 que cubre de forma inalámbrica el TE 14 y el SE 12.

El TE 14 usa el SE 12 para proporcionar acceso a uno o varios servicios de comunicación inalámbrica, tal como, por ejemplo, un SMS, un(os) servicio(s) de comunicación de tipo de protocolo de Internet (o IP) y/o similares, que son accesibles a través o por la red 100.

El TE 14 puede incluir un teclado (no representado) y una pantalla de visualización (no representada), como una interfaz hombre-máquina (o IHM) de TE. La IHM de TE permite que un usuario de TE interactúe con el TE 14.

El TE 14 incluye un(os) (micro)controlador(es) y/o un(os) (micro)procesador(es) 142, como medios de procesamiento de datos, una o varias memorias 144, como medios de almacenamiento de datos, y una o varias interfaces de E/S 146 , que están todos conectados a través de un bus 143 de datos y control interno.

La memoria 144 de TE almacena preferiblemente un IMEI1 y/o similar, como un(os) identificador(es) relacionado(s) con el TE 14.

El TE 14 incluye o está conectado a un módem. El módem permite intercambiar datos, a través de uno o varios enlaces 15 de RF de LR, como enlaces inalámbricos, con la red 100.

El TE 14 puede obtener preferiblemente en primer lugar del SE 12 un IMSIi, como un primer IMSI temporal, usando, por ejemplo, un comando de tipo “LEER IMSI”, como una solicitud para obtener un IMSI que está activo actualmente en el SE 12.

Una vez que se recibe el IMSIi, el TE 14 puede enviar preferiblemente a la red 100 una “Solicitud de vinculación de IMSIi”, como una primera solicitud para vincularse a la red 100, para iniciar una primera sesión de autenticación con la red 100.

El TE 14 puede recibir preferiblemente de la red 100 un primer desafío y enviar al SE 12 el primer desafío.

El TE 14 puede recibir preferiblemente del SE 12 unos primeros datos y enviar a la red 100 los primeros datos.

El TE 14 puede recibir preferiblemente de la red 100 un primer mensaje de resultado que incluye un fallo de autenticación basado en los primeros datos.

El TE 14 puede obtener preferiblemente del SE 12 un IMSIj, como un segundo IMSI temporal, usando, por ejemplo,

un comando de tipo “LEER IMSI”, como una solicitud para obtener un IMSI que está activo actualmente en el SE 12.

Una vez que se recibe el IMSIj, el TE 14 puede enviar preferiblemente a la red 100 una “Solicitud de vinculación de IMSIj”, como una segunda solicitud para vincularse a la red 100, para iniciar una segunda sesión de autenticación con la red 100.

El TE 14 puede recibir preferiblemente de la red 100 un segundo desafío y enviar al SE 12 el segundo desafío.

El TE 14 puede recibir preferiblemente del SE 12 unos segundos datos y enviar a la red 100 los segundos datos.

El TE 14 puede recibir preferiblemente de la red 100 un segundo mensaje de resultado que incluye un éxito de autenticación basado en los segundos datos.

La red 100 incluye una o varias entidades de tipo de estación transceptora de base (o BTS) (no representadas).

La BTS permite el intercambio de datos, a través del/de los enlace(s) 15 inalámbrico(s), con el TE 14 y/o el SE 12.

La BTS está conectada, dentro de la red 100, a un centro de conmutación móvil (o MSC) y a una entidad 16 de tipo de registro de posiciones visitado (o RPV) que se denomina RPV a continuación.

El MSC puede enrutar llamadas, mensajes y datos destinados y/o procedentes del TE 14 en una zona de RF administrada por el MSC.

El MSC procesa cualquier mensaje entrante procedente de cualquier terminal cubierto, como, por ejemplo, el TE 14, para vincularlo a la red 100.

El MSC sirve al TE 14 y al SE 12. El MSC está conectado a o integrado dentro del RPV que está representado como una misma entidad 16 de red. El MSC puede interrogar al RPV, como un primer servidor, para determinar dónde se encuentra el abonado en cuestión.

El RPV 16 incluye una base de datos de abonados, una vez que los abonados tienen IMSI definitivos. Cada registro de abonado incluye uno o varios identificadores relacionados con el SE 12, como, por ejemplo, su(s) IMSI definitivo(s).

La base de datos de abonados incluye preferiblemente el IMSI definitivo, como un identificador relacionado con el SE 12 que puede desplazarse a una zona de RF a la que el MSC sirve y gestiona a través de una cobertura de radio relacionada con las BTS.

Además o alternativamente, la base de datos de abonados puede incluir otra información relacionada con cada abonado, como, por ejemplo, un número de directorio de abonado internacional de estación móvil (o MSISDN), como un número usado para identificar al abonado, datos de autenticación, un(os) servicio(s) a los que se permite que acceda el abonado, una dirección de RPP relacionada con el abonado, un punto de acceso de GPRS y/u otros datos. El/los servicio(s) de GSM puede(n) incluir un servicio de SMS y/o de llamada (telefónica).

El RPV 16 puede permitir o no permitir preferiblemente uno o varios servicios que el abonado puede usar.

El RPV 16 está conectado, a través de un enlace 17 de cable, al RPP 18, como el segundo servidor.

El MSC/RPV 16 puede recibir preferiblemente en primer lugar del TE 14 una “Solicitud de vinculación de IMSIi”, como una primera solicitud para vincularse a la red 100, que incluye o va o acompañada de un IMSIi, como un primer IMSI temporal.

Una vez que se recibe el IMSIi, el MSC/RPV 16 puede enviar preferentemente al RPP 18 una “Solicitud de autenticación de IMSIi”, como una primera solicitud de autenticación, que incluye o va acompañada de un IMSIi, como un primer IMSI temporal para iniciar una primera sesión de autenticación.

El MSC/RPV 16 puede recibir preferiblemente del RPP 18 un primer desafío y un primer resultado esperado.

El MSC/RPV 16 puede enviar preferiblemente al TE 14 el primer desafío.

El MSC/RPV 16 puede recibir preferiblemente del TE 14 unos primeros datos.

El MSC/RPV 16 puede comparar preferiblemente los primeros datos con el primer resultado esperado.

Si los primeros datos no coinciden con el primer resultado esperado, entonces el MSC/RPV 16 puede enviar preferiblemente al TE 14 un primer mensaje de resultado que incluye un fallo de autenticación basado en los primeros datos.

De lo contrario, si los primeros datos coinciden con el primer resultado esperado, el MSC/RPV 16 puede enviar preferiblemente al TE 14 un primer mensaje de resultado que incluye un éxito de autenticación basado en los

primeros datos.

El MSC/RPV 16 puede recibir preferiblemente del TE 14 una “Solicitud de vinculación de IMSIj”, como una segunda solicitud para vincularse a la red 100, que incluye o va acompañada de un IMSIj, como un segundo IMSI temporal.

Una vez que se recibe el IMSIj, el MSC/RPV 16 puede enviar preferiblemente al RPP 18 una “Solicitud de autenticación de IMSIj”, como una segunda solicitud de autenticación, que incluye o va acompañada de un IMSIj, como un segundo IMSI temporal para iniciar una primera sesión de autenticación.

El MSC/RPV 16 puede recibir preferiblemente del RPP 18 un segundo desafío y un segundo resultado esperado.

El MSC/RPV 16 puede enviar preferiblemente al TE 14 el segundo desafío.

El MSC/RPV 16 puede recibir preferiblemente del TE 14 unos segundos datos.

El MSC/RPV 16 puede comparar preferiblemente los segundos datos con el segundo resultado esperado.

Si los segundos datos coinciden con el segundo resultado esperado, entonces el MSC/RPV 16 puede enviar preferiblemente al TE 14 un segundo mensaje de resultado que incluye un éxito de autenticación basado en los segundos datos.

De lo contrario, si los segundos datos no coinciden con el segundo resultado esperado, el MSC/RPV 16 puede enviar preferiblemente al TE 14 un segundo mensaje de resultado que incluye un fallo de autenticación basado en los segundos datos.

El RPP 18 incluye (o está conectado a) una memoria 182.

La memoria 182 almacena una base de datos central.

El RPP 18 puede enviar datos de abonado a un RPV cuando el abonado en cuestión se desplaza a una zona de RF a la que sirve el RPV.

El RPP 18 puede proporcionar preferiblemente, cuando se le solicite, información de enrutamiento que incluye un IMSI definitivo, para enrutar una llamada al abonado en cuestión.

El RPP 18 se identifica mediante un URI, como, por ejemplo, un URL y/o una dirección de tipo IP, como un(os) identificador(es) de servidor. El/los identificador(es) de servidor se almacenan(n) preferiblemente dentro del SE 12 (o el TE 14).

El RPP 18, como un servidor por aire (u OTA), está incluido dentro de la red 100.

Alternativamente, en lugar de un servidor incluido dentro de la red 100, el servidor (no representado), como un servidor por Internet (OTI), está conectado a la red 100.

Alternativamente, el RPP 18 es un servidor OTA y un servidor OTI.

El RPP 18 puede ser operado por un operador de red de origen móvil, como un operador de red móvil (o MNO) o un operador de red virtual móvil (o MVNO), un proveedor de servicios o en su nombre.

El RPP 18 está alojado en un ordenador.

El RPP 18 gestiona la base de datos central.

Alternativamente, otro servidor (no representado) que está conectado al RPP 18 gestiona la base de datos central.

La base de datos central incluye datos relacionados con abonados que están autorizados a acceder a uno o varios servicios proporcionados por o a través de la red 100.

La base de datos central incluye un conjunto de perfiles de abonado definitivos que incluyen IMSI definitivos que quedan por asignar a dispositivos de cliente, como, por ejemplo, el SE 12, que deben identificarse y autenticarse, cada uno, usando dos IMSI temporales consecutivos.

La base de datos central puede incluir otros datos que están asociados con cada identificador SE definitivo, como por ejemplo:

- un(os) servicio(s) de comunicación de GSM que el abonado ha solicitado o se le ha(n) permitido;

- un(os) ajuste(s) de GPRS para permitir que el abonado acceda a un servicio de comunicación de paquetes de datos;

- una ubicación actual del abonado.

El RPP 18 puede usarse para gestionar la movilidad de los abonados actualizando su ubicación en zonas de ubicación (o LA) geográfica.

Según la invención, el RPP 18 está configurado para identificar y autenticar un dispositivo cliente usando consecutivamente dos IMSI temporales.

El RPP 18 está configurado para recibir un IMSIi, como un primer IMSI de abono temporal, que se usa para identificar el dispositivo cliente en la red 100, para iniciar una primera sesión de autenticación.

Cabe señalar que no es posible identificar el dispositivo cliente que ha enviado el IMSIi dado que se supone que un LOCI o un IMEI relacionado con el dispositivo cliente no se conoce a partir del RPV 16 y el RPP 18. Si dos o más dispositivos cliente están intentando vincularse con un mismo IMSIi a un mismo MSC/RPV 16 de servicio a un mismo tiempo, entonces el MSC/RPV 16 de servicio puede comportarse de manera diferente de acuerdo con su implementación durante tal caso de colisión. Según una realización particular, el RPP 18 está configurado para almacenar dentro de la memoria 182 sólo el último IMSIi recibido entre todos los IMSIi que se reciben a un mismo tiempo y se consideran un primer IMSI temporal.

Según una realización particular, si se reciben dos o más, como un número M, mismos IMSIi antes que cualquier IMSIj de uno o varios MSC/RPV de servicio, entonces la primera solicitud de vinculación de red más reciente (es decir, el último IMSIi recibido) se rechaza con un código de retorno particular, como, por ejemplo, un código de retorno que cumpla la norma 3GPP ARIB, ATIS, ETSI, TSDSI, TTA y TTC TS 29.002 y TS 29.02, tal como “VALOR DE DATOS INESPERADOS”, como una respuesta de INFORMACIÓN DE AUTENTICACIÓN-ENVÍO-MAPA. Todos los dispositivos cliente correspondientes (que han emitido el mismo IMSIi) afectados por dicha colisión tienen que volver a intentarlo usando un algoritmo de retroceso. El algoritmo de retroceso permite retrasar a un momento posterior, por separado y de manera aleatoria, otro inicio de un procedimiento de vinculación de red por cada dispositivo cliente en cuestión. El algoritmo de retroceso que cada dispositivo cliente soporta tiene una raíz única que permite posponer de manera única otro inicio de un procedimiento de vinculación de red. El algoritmo de retroceso permite aumentar preferiblemente de manera exponencial el tiempo de retraso con un número creciente de colisiones. El algoritmo de retroceso puede ser del tipo del algoritmo de retroceso de Ethernet (IEEE 802.3).

Según otra realización, si se reciben dos o más, como un número M, mismos IMSIi antes que cualquier IMSIj de uno o varios MSC/RPV de servicio, entonces el RPP 18 gestiona sólo el último IMSIi recibido mediante tratamiento con el dispositivo cliente correspondiente usando un IMSIj asociado y un(os) secreto(s) compartido(s), para autenticar el dispositivo cliente correspondiente en cuestión. Los otros dispositivos cliente que hayan emitido el otro (M-1) IMSIi tienen que volver a intentar más adelante un inicio de un procedimiento de vinculación de red.

El IMSIi recibido por el RPP 18 durante la primera sesión de autenticación y uno o varios parámetros de entrada relacionados con un algoritmo de determinación de IMSIj compartido con el dispositivo cliente los usan preferiblemente el RPP 18 y el dispositivo cliente para determinar dinámicamente el IMSIj que va a usarse para iniciar una segunda sesión de autenticación.

El IMSIj se determina preferiblemente para evitar una colisión de un(os) mismo(s) IMSI temporal(es) usado(s) por uno o varios otros dispositivos cliente. Más exactamente, el IMSIj se determina preferiblemente de modo que dos o más dispositivos cliente que también determinan un IMSIj, como un segundo IMSI temporal, no utilicen un mismo IMSIj al mismo tiempo durante una segunda sesión de autenticación, respectivamente.

Según una realización particular, un primer desafío, como un parámetro de entrada para un algoritmo de determinación de IMSIj compartido, se usa para determinar dinámicamente el IMSIj. Parte, como, por ejemplo, uno, dos o más bits, o todos los bits relacionados con el primer desafío se usa, por ejemplo, para determinar un índice j relacionado con una j-ésima columna en la que el IMSIj, como un segundo identificador de abono temporal, está situado en asociación con el IMSIi, como un primer identificador de abono temporal, que está situado en un índice i relacionado con la i-ésima fila.

Según otra realización, uno o varios parámetros de entrada se aprovisionan previamente a los dispositivos del cliente y se comparten con el RPP 18 y se identifican mediante el uso de un primer desafío que va a enviar el RPP 18 y/u otro(s) parámetro(s) que se usa(n) para seleccionar el IMSIj asociado. El RPP 18 y el dispositivo cliente están dispuestos para determinar dinámicamente, de manera común, el IMSIj asociado con el IMSIi para el dispositivo cliente en cuestión. El/los parámetro(s) de entrada seleccionado(s) no se comparte(n) con ningún otro dispositivo cliente para identificarse en la red 100 al mismo tiempo, para evitar cualquier riesgo de colisión.

Según una realización particular, el RPP 18 usa un primer algoritmo de autenticación de red, el primer desafío y una clave que no se comparte con el dispositivo cliente, para generar un primer resultado esperado. La clave sólo se almacena en la memoria 182, es decir, sólo puede accederse a la clave en el lado de servidor (y no el lado de cliente). La clave se ha aprovisionado previamente a la memoria 182.

El primer algoritmo de autenticación de red puede ser el algoritmo conocido A3 para una norma de GSM o similar.

Según una realización particular, el RPP 18 usa un segundo algoritmo de autenticación de red, el segundo desafío y

una clave Ki,j para autenticarse en la red 100, para generar dinámicamente un segundo resultado esperado. El segundo algoritmo de autenticación de red se comparte con el dispositivo cliente. El segundo algoritmo de autenticación de red puede ser el algoritmo conocido A3 para una norma de GSM o similar. El segundo algoritmo de autenticación de red puede ser o bien el primer algoritmo de autenticación de red o bien distinto del primer algoritmo de autenticación de red. El RPP 18 y el dispositivo cliente están dispuestos para determinar dinámicamente, de manera común, la clave Ki,j para autenticarse en la red 100 en asociación con el IMSIj o el par del IMSIi y el IMSIj asociado.

La clave Ki,j para autenticarse en la red 100 es preferiblemente única y está asociada con el dispositivo cliente identificado.

La clave Ki,j para autenticarse en la red 100 se almacena dentro de la memoria 182 y en el lado de cliente. La clave Ki,j para autenticarse en la red 100 se ha aprovisionado previamente y compartido entre el RPP 18 y el dispositivo cliente. La clave Ki,j para autenticarse en la red 100 está asociada con el par del IMSIi y el IMSIj asociado.

La base de datos central incluye un conjunto de IMSI temporales, para identificar y autenticar dispositivos cliente.

El RPP 18 está dispuesto preferiblemente para determinar el IMSIj asociado de tal manera que sólo el dispositivo cliente que envía previamente el IMSIi pueda determinar, de manera común con el RPP 18, el IMSIj asociado, para minimizar un riesgo de colisión.

Para un par dado de un IMSIi y un IMSIj asociado, hay un dispositivo cliente único que usa el par del IMSIi y el IMSIj asociado. Por lo tanto, se evita el riesgo de colisión entre dos o más dispositivos cliente que intentan identificarse al mismo tiempo.

El RPP 18 está configurado para generar datos que permitan al RPP 18 y al dispositivo cliente determinar, de manera común, el IMSIj que va a asociarse con el IMSIi. Los datos generados se usan entonces como un primer desafío que va a enviarse al dispositivo cliente que ha enviado previamente el IMSIi. Por lo tanto, cuando el RPP 18 recibe al mismo tiempo de dos o más dispositivos cliente un mismo IMSIi, el RPP 18 puede separar claramente los dispositivos cliente que intentan vincularse a la red 100 asignando a cada uno de los dispositivos cliente un primer desafío único que permite determinar un IMSIj dedicado asociado. Debido al uso de un primer desafío único con un sólo dispositivo cliente, el dispositivo cliente determina, de manera común con el RPP 18, un único IMSIj que el dispositivo cliente (y no cualquier otro dispositivo cliente) va a usar para una segunda sesión de autenticación.

La base de datos central comprende, según una realización preferida, una tabla de correspondencia que puede configurarse y compartirse al menos en parte con cada dispositivo cliente de una flota de dispositivos cliente que pueden activarse de este modo.

La tabla de correspondencia se crea preferiblemente de forma dinámica. Más exactamente, se proporcionan datos durante al menos una segunda sesión de autenticación para un dispositivo cliente que ya ha realizado una primera sesión de autenticación con un resultado de fallo. Los datos proporcionados dinámicamente pueden originarse a partir o a través de otra entidad, tal como, por ejemplo, un centro de autenticación (o AuC) (no representado) o similares.

La tabla de correspondencia puede ser del tipo siguiente, como ejemplo:

IMSIi\IMSIj	IMSI2	IMSI4
IMSI1	RAND11-SRES11	RAND12-SRES12
	RAND21-K11-SRES21	RAND22-K12-SRES22
IMSI3	RAND21-SRES13	RAND22-SRES14
	RAND23-K13-SRES23	RAND24-K14-SRES24

En aras de la simplicidad, la tabla de correspondencia representada incluye sólo dos filas y dos columnas con cuatro IMSI temporales diferentes. La primera columna incluye un conjunto de los primeros IMSIi temporales que van a recibirse de los dispositivos cliente para una primera sesión de autenticación. La primera fila incluye un conjunto de los IMSIj que van a asociarse con el IMSIi y van a usarse, de manera común, con cada dispositivo cliente para una segunda sesión de autenticación. El IMSIj es preferiblemente distinto del IMSIi. Por ejemplo, el IMSIi pertenece a un primer intervalo predeterminado de IMSI, mientras que el IMSIj pertenece a un segundo intervalo predeterminado de IMSI que es independiente del primer intervalo predeterminado de IMSI. La segunda fila incluye, para un IMSIi dado, y una columna dada entre la segunda y la tercera columna, un IMSIj asociado correspondiente. Por lo tanto, cuando hay dos dispositivos cliente que usan simultáneamente el mismo IMSI1, como el primer IMSI temporal, la red 100 usa, por un lado, un primer valor RAND11 de un primer desafío que permite que la red 100 determine, de manera común con un primer dispositivo cliente, el IMSI2 asociado, como el segundo IMSI temporal, y, por otro lado, un segundo valor RAND12 de otro primer desafío que permite que la red 100 determine, de manera común con un segundo dispositivo cliente, el IMSI4 asociado, como el segundo IMSI temporal. Para el primer dispositivo cliente, la

red 100 usa un primer valor SRES11 de un primer resultado esperado que permite que la red 100 no autentique el primer dispositivo cliente que usa el IMSI1, como el primer IMSI temporal. El primer resultado esperado SRES11 puede ser un valor (pseudo)aleatorio o uno fijo predeterminado que no puede obtenerse en el lado de cliente, de modo que la red 100 no puede autenticar el dispositivo del cliente que usa el primer IMSI1 temporal en cuestión durante una primera sesión de autenticación. La segunda o la tercera columna incluye, para un IMSIj dado, y una fila dada entre la segunda y la tercera fila, un IMSIi asociado correspondiente.

Cada par de IMSIi e IMSIj asociado está asociado con uno o varios dispositivos cliente que se identifican en la tabla de correspondencia.

Luego, para el primer dispositivo cliente, la red 100 usa un primer valor RAND21 de un segundo desafío, un primer valor K11 de una clave Ki,j para autenticar el cliente, un primer valor SRES21 de un segundo resultado esperado que permite que la red 100 autentique con éxito el primer dispositivo cliente. El primer valor K11 de la clave Ki,j para autenticar el cliente se comparte previamente con el primer dispositivo cliente, para autenticar con éxito el primer dispositivo cliente durante una segunda sesión de autenticación. El segundo resultado esperado ha de obtenerse también en el lado de cliente, de modo que la red 100 logre autenticar el dispositivo cliente que usa el segundo IMSI temporal en cuestión asociado con el primer IMSI temporal.

Por lo tanto, el segundo IMSIj temporal que va a usarse depende al menos del primer IMSIi temporal, para evitar un riesgo de colisión en el lado de servidor.

El segundo IMSIj temporal que va a usarse depende preferiblemente del primer IMSIi temporal y del primer desafío, para evitar un riesgo de colisión en el lado de servidor.

El RPP 18 se conecta preferiblemente a un AuC (no representado) que se usa para generar dinámicamente un primer y un segundo desafío y un primer y un segundo resultado esperado para un primer y un segundo IMSI temporal, respectivamente.

El RPP/AuC 18 puede recibir preferiblemente del MSC/RPV 16 una “Solicitud de autenticación de IMSIi”, como una primera solicitud de autenticación, que incluye o va acompañada de un IMSIi.

El RPP/AuC 18 puede generar preferiblemente un primer desafío y un primer resultado esperado.

El RPP/AuC 18 puede enviar preferiblemente al MSC/RPV 16 el primer desafío y el primer resultado esperado.

El RPP/AuC 18 puede recibir preferiblemente del MSC/RPV 16 una “Solicitud de autenticación de IMSIj”, como una segunda solicitud de autenticación, que incluye o va acompañada de un IMSIj, como un segundo IMSI temporal para iniciar una segunda sesión de autenticación.

El RPP/AuC 18 puede consultar preferiblemente desde una base de datos una clave que está asociada con el par de IMSIi e IMSIj mientras proporciona el par de IMSIi e IMSIj.

El RPP/AuC 18 puede recibir preferiblemente de la base de datos consultada la clave asociada que está con el par de IMSIi e IMSIj.

El RPP/AuC 18 puede generar preferiblemente un segundo desafío.

El RPP/AuC 18 puede generar preferiblemente un segundo resultado esperado usando la clave que está asociada con el par de IMSIi e IMSIj.

El RPP/AuC 18 puede enviar preferiblemente al MSC/RPV 16 el segundo desafío y el segundo resultado esperado.

La figura 2 representa una realización a modo de ejemplo del método 20 de la invención para autenticarse en la red 100 implementada por el TEQ 10, como un sistema cliente, y la red 100, como un sistema de servidor.

Se supone que el TEQ 10 incluye dos entidades, a saber, el SE 12 (no representado) y el TE 14 (no representado), que están implicados como un dispositivo cliente único. Sin embargo, cada mensaje intercambiado o cada acción que se describe en el lado de TEQ puede llevarse a cabo por al menos una entidad, el SE 12 y/o el TE 14.

Se supone que el SE 12 no tiene acceso a, por ejemplo, el LOCI, como información de ubicación de SE, y/o el IMEI, como un identificador relacionado con el TE 14. El SE 12 actúa conjuntamente con el TE 14, para identificarse y preferiblemente autenticarse en la red 100 en una activación del TEQ 10. Por lo tanto, el SE 12 soporta la aplicación de autenticación de la invención, como una aplicación de abono de arranque, que permite identificarse y autenticarse en la red 100 usando consecutivamente un primer IMSI temporal o IMSI1, y un segundo IMSI temporal o IMSI2, como dos IMSI temporales diferentes.

Se supone además que el SE 12 almacena un ICCID1, como un identificador único relacionado con el SE 12 que el SE 12 no puede enviar al lado de la red 100.

Se supone además que la red 100 incluye varias entidades, como, por ejemplo, el RPV 16 (no representado) y el RPP 18 (no representado) y posiblemente el AuC (no representado), que están implicadas como dos o más servidores. Sin embargo, cada mensaje intercambiado o cada acción que se describe en el lado de red puede llevarse a cabo por al menos una entidad, como, por ejemplo, el RPV 16, el RPP 18 y/o el AuC, como un servidor.

Se supone además que la red 100 comparte con un mismo dispositivo cliente al menos un par de IMSIi, como un primer identificador de abono temporal, e IMSIj, como un segundo identificador de abono temporal, y una Ki para autenticarse en la red 100 que está asociada con el IMSIj (o el par de IMSIi e IMSIj). El dispositivo cliente se identifica dentro de la tabla de correspondencia. Por lo tanto, según tal realización, la red 100 comparte en particular sólo con el TEQ 10 que se identifica con el ICCID1 dentro de la tabla de correspondencia, el IMSI1, como un primer identificador de abono temporal, el IMSI2 asociado, como un segundo identificador de abono temporal, y una clave única K11, como una Ki, para autenticarse en la red 100 que está asociada con el IMSI2 (o el par del IMSI1 y su IMSI2 asociado). Por lo tanto, la red 100 no tiene riesgo de colisión que gestionar.

En primer lugar, se enciende el TEQ 10.

El TEQ 10 activa 22 sólo el IMSI1.

El TEQ 10 envía a la red 100 una “Solicitud de vinculación de IMSI1”, como una solicitud 24 para vincularse a la red 100 que incluye o está acompañada del IMSI1. Tal primera solicitud 24 de vinculación de red inicia una primera sesión de autenticación.

Una vez que la red 100 ha recibido el IMSI1, la red 100 detecta que el IMSI1 es un primer IMSI temporal, ya que, por ejemplo, el IMSI1 pertenece a un primer intervalo predeterminado de IMSI.

Luego, la red 100 almacena el IMSI1, como el último IMSI1 recibido.

La red 100 genera o recupera 26, es decir, accede a, preferiblemente un primer desafío RAND11.

La red 100 genera o recupera 26, es decir, accede a, un primer resultado esperado o SRES11 usando el primer desafío RAND11, un primer algoritmo de autenticación de red y una clave que preferiblemente no se comparte con el TEQ 10 para la primera sesión de autenticación.

En lugar de acceder al SRES11 justo después de haber obtenido el RAND11, la red 100 accede al SRES11 justo antes de una primera etapa 214 de comparación que se describe a continuación.

La red 100 envía al TEQ 10 el RAND11, como una solicitud 28 para enviar una primera respuesta que incluye o está acompañada del RAND11.

Una vez que el TEQ 10 ha recibido el RAND11, el TEQ 10 genera o recupera 210 unos SRESx o primeros datos usando, por ejemplo, unos primeros datos cargados previamente o un algoritmo de generación (pseudo)aleatorio o un primer algoritmo de autenticación de red y una clave no compartida con la red 100 para la primera sesión de autenticación.

El TEQ 10 envía a la red 100 los primeros datos, como una primera respuesta 212.

La red 100 analiza si los primeros datos coinciden o no con el primer resultado esperado comparando los primeros datos con el primer resultado esperado, como la primera etapa 214 de comparación.

Si la red 100 determina que los primeros datos coinciden con el primer resultado esperado, entonces la red 100 envía al TEQ 10 un primer mensaje de resultado (no representado) que incluye un éxito de autenticación basado en los primeros datos.

De lo contrario, es decir, si la red 100 determina que los primeros datos no coinciden con el primer resultado esperado, la red 100 envía al TEQ 10 un primer mensaje 216 de resultado que incluye un fallo de autenticación basado en los primeros datos.

Sólo si el primer mensaje de resultado recibido incluye un fallo de autenticación basado en los primeros datos, el TEQ 10 determina 218 un IMSI2 asociado con el IMSI1 usando el IMSI1.

Además, el TEQ 10 determina 218 una K11, como una clave Ki para autenticares en la red 100, que está asociada con el IMSI2 y se comparte con la red 100.

El TEQ 10 cambia del IMSI1 al IMSI2, es decir, activa 220 sólo el IMSI2.

Luego, el TEQ 10 envía a la red 100 una “Solicitud de vinculación de IMSI2”, como una solicitud 222 para vincularse a la red 100 que incluye o está acompañada del IMSI2. Tal segunda solicitud 222 de vinculación de red inicia una segunda sesión de autenticación.

Una vez que la red 100 ha recibido el IMSI2, la red 100 detecta que el IMSI2 es un segundo IMSI temporal, dado

que, por ejemplo, el IMSI2 pertenece a un segundo intervalo predeterminado de IMSI que es distinto del primer intervalo predeterminado de IMSI que se usa para el primer IMSI temporal.

Luego, la red 100 captura el IMSI1 recibido almacenado, como, por ejemplo, el último IMSI1 recibido.

La red 100 asocia el IMSI2 con el IMSI1 recibido. La red 100 identifica un par único del IMSI1 y el IMSI2 asociado, como un par de IMSI temporales. De este modo, la red 100 determina, basándose, por ejemplo, en la tabla de correspondencia, que el par único del IMSI1 y el IMSI2 está asociado con el dispositivo del cliente que se identifica como ICCID1, como un identificador relacionado con el TEQ 10.

Por lo tanto, la red 100 no necesita recibir del TEQ 10 ningún identificador relacionado con el TEQ 10, tal como un IMEI o similar, u otra información, como, por ejemplo, información relacionada con una ubicación del TEQ 10.

La red 100 sabe que el último IMSI2 recibido está relacionado con un segundo intento de autenticarse en la red 100 después de un primer intento de autenticarse en la red 100 que ha fallado.

La red 100 también determina 224 una K11, como una clave Ki para autenticarse en la red 100, que se comparte con el TEQ 10 basándose, por ejemplo, en la tabla de correspondencia compartida al menos en parte entre la red 100 y el TEQ 10.

Luego, la red 100 genera o recupera 226, es decir, accede a, preferiblemente un segundo desafío RAND21 que va a usarse de manera común para autenticarse en la red 100. El RAND21 es preferiblemente aleatorio.

La red 100 genera o recupera 226, es decir, accede a, un SRES21 o un segundo resultado esperado usando el segundo desafío RAND21, un segundo algoritmo de autenticación de red y la clave K11 que se comparten ambos preferiblemente con el TEQ 10 para la segunda sesión de autenticación.

En lugar de acceder al SRES21 justo después de haber obtenido el RAND21, la red 100 accede al SRES21 justo antes de una segunda etapa 234 de comparación que se describe a continuación.

La red 100 envía al TEQ 10 el RAND21, como una solicitud 228 para enviar una segunda respuesta que incluye o va acompañada del RAND21.

Una vez que el TEQ 10 ha recibido el RAND21, el TEQ 10 genera 230 unos SRESy o segundos datos usando preferiblemente el segundo algoritmo de autenticación de red y la clave K11 que se comparten ambos con la red 100 para la segunda sesión de autenticación.

El TEQ 10 envía a la red 100 los segundos datos, como una segunda respuesta 232.

La red 100 analiza si los segundos datos coinciden o no con el segundo resultado esperado comparando los segundos datos con el segundo resultado esperado, como la segunda etapa 234 de comparación.

Si la red 100 determina que los segundos datos no coinciden con el segundo resultado esperado, entonces la red 100 envía al TEQ 10 un segundo mensaje de resultado (no representado) que incluye un fallo de autenticación basado en los segundos datos.

De lo contrario, es decir, si la red 100 determina que los segundos datos coinciden con el segundo resultado esperado, la red 100 envía al TEQ 10 un segundo mensaje 236 de resultado que incluye un éxito de autenticación basado en los segundos datos.

Una vez que se autentica con éxito usando el IMSI1 y el IMSI2 asociado, la red 100 puede volver a usar el IMSI1 y el IMSI2 asociado para identificar y autenticar otro dispositivo cliente que comparta con la red el IMSI1 y el IMSI2 asociado y uno o varios secretos asociados.

Luego, la red 100 envía al TEQ 10 uno o varios mensajes (no representados) que incluyen datos, como, por ejemplo, al menos un identificador de abono definitivo o permanente incluido dentro de un perfil de abono permanente que va a activarse en el TEQ 10. Los datos en cuestión pueden haberse cifrado en el lado de la red 100.

El TEQ 10, y más exactamente el SE 12, se actualiza, después de un posible descifrado de datos, y puede usar los datos así recibidos, como, por ejemplo, el perfil de abono permanente.

La solución de la invención permite autenticar, después de un cambio de abono temporal en el lado del TEQ 10, un dispositivo cliente en la red.

La solución de la invención no necesita implicar a ningún usuario de TEQ, excepto posiblemente para enviar datos de autenticación de usuario, cuando corresponda.

Por lo tanto, la solución de la invención es transparente para el usuario, aparte de una posible operación de autenticación de usuario.

La solución de la invención puede ser automática y, por lo tanto, rápida, es decir, típicamente de menos de 5 segundos, y eficiente.

La solución de la invención es compatible con la infraestructura de red móvil existente.

La solución de la invención es segura ya que, por un lado, la red autentica el dispositivo cliente usando dos identificadores temporales y un(os) secreto(s) compartido(s) entre el dispositivo cliente y la red y, por otro lado, el dispositivo cliente autentica posiblemente un usuario de dispositivo cliente.

La realización descrita no pretende limitar el alcance de la invención en cuestión. Pueden darse otras realizaciones. Como otro ejemplo de realización, en lugar de intercambiar, a través de uno o varios MSC/RPV (o una o varias entidades de gestión de movilidad (o MME) relacionadas con una red de evolución a largo plazo (o LTE)) o similares, con un único servidor remoto, como, por ejemplo, el RPP 18 (o un servidor de abonado de origen (o HSS) relacionado con la red LTE) o similares, el dispositivo cliente intercambia con varios servidores remotos.

REIVINDICACIONES

1. Método para autenticar un dispositivo en una red móvil,

- una vez encendido, el dispositivo activa (22) un primer identificador de abono temporal, estando el primer identificador de abono temporal activo en primer lugar;

- el dispositivo envía a un primer servidor el primer identificador (24) de abono temporal y unos primeros datos (212);

- el primer servidor envía al dispositivo un primer mensaje (216) de resultado que incluye un fallo de autenticación basado en los primeros datos;

caracterizado por que el método comprende además las siguientes etapas:

- entonces el dispositivo determina (218) un segundo identificador de abono temporal y al menos un secreto asociado con al menos el segundo identificador de abono temporal, estando el segundo identificador de abono temporal asociado con el primer identificador de abono temporal;

- el dispositivo cambia (220) del primer identificador de abono temporal al segundo, estando el segundo identificador de abono temporal activo en segundo lugar;

- el dispositivo genera (230) unos segundos datos usando al menos un secreto;

- el dispositivo envía al primer servidor el segundo identificador (222) de abono temporal y los segundos datos (232);

- el primer servidor determina (224), basándose en al menos el segundo identificador de abono temporal, el al menos un secreto; y

- el primer servidor envía al dispositivo un segundo mensaje (236) de resultado que incluye un éxito de autenticación basado en los identificadores de abono temporales primero y segundo asociados y los segundos datos.

2. Método según la reivindicación 1, en el que, antes de recibir el primer mensaje de resultado que incluye el fallo de autenticación, el método comprende las siguientes etapas:

- el primer servidor envía al dispositivo una solicitud (28) para enviar una primera respuesta, incluyendo la primera solicitud de respuesta un primer desafío;

- el dispositivo envía al primer servidor los primeros datos, como primera respuesta;

- el primer servidor accede a un primer resultado esperado;

- el primer servidor compara (214) la primera respuesta con el primer resultado esperado;

- el primer servidor determina que la primera respuesta no coincide con el primer resultado esperado.

3. Método según la reivindicación 1 ó 2, en el que, antes de recibir el segundo mensaje de resultado que incluye el éxito de autenticación, el método comprende las siguientes etapas:

- el primer servidor envía al dispositivo una solicitud (228) para enviar una segunda respuesta, incluyendo la segunda solicitud de respuesta un segundo desafío;

- el dispositivo envía al primer servidor los segundos datos, como segunda respuesta;

- el primer servidor accede a un segundo resultado esperado;

- el primer servidor compara (234) la segunda respuesta con el segundo resultado esperado;

- el primer servidor determina que la segunda respuesta coincide con el segundo resultado esperado.

4. Método según la reivindicación 2 ó 3 que depende de la reivindicación 2, en el que el dispositivo y el primer servidor determinan el segundo identificador de abono temporal usando al menos el primer identificador de abono temporal.

5. Método según la reivindicación 4, en el que, estando el dispositivo conectado o acoplado a un elemento seguro, el elemento seguro genera los segundos datos usando el segundo desafío y una clave para autenticarse en la red móvil, estando la clave para autenticarse en la red móvil asociada con al menos el segundo identificador de abono temporal y compartiéndose con el primer servidor, y el elemento seguro envía al dispositivo los segundos datos.

6. Método según la reivindicación 2 ó 3, en el que, estando el primer servidor conectado o acoplado a un segundo servidor, el segundo servidor genera y envía al primer servidor el primer resultado esperado y/o en el que el

segundo servidor genera y envía al primer servidor el segundo resultado esperado.

7. Método según la reivindicación 6, en el que, almacenando el elemento seguro al menos un identificador relacionado con el elemento seguro, el segundo servidor recupera el identificador relacionado con el elemento seguro y una clave para autenticarse en la red móvil, basándose en el primer identificador de abono temporal y el segundo identificador de abono temporal asociado, compartiéndose la clave para autenticarse en la red móvil entre el elemento seguro y el segundo servidor.

8. Primer servidor (18) para autenticar un dispositivo en una red móvil,

pudiendo el primer servidor:

- recibir del dispositivo (12) un primer identificador (24) de abono temporal y unos primeros datos (212);

- enviar al dispositivo (12) un primer mensaje (216) de resultado que incluye un fallo de autenticación basado en los primeros datos;

caracterizado por que el primer servidor está configurado para entonces:

- recibir del dispositivo (12) un segundo identificador (222) de abono temporal y unos segundos datos (232), estando el segundo identificador de abono temporal asociado con el primer identificador de abono temporal;

- determinar (224), basándose en al menos el segundo identificador de abono temporal, el al menos un secreto; y

- enviar al dispositivo (12) un segundo mensaje (236) de resultado que incluye un éxito de autenticación basado en los identificadores de abono temporales primero y segundo asociados y los segundos datos.

9. Dispositivo (12) para autenticarse en una red móvil,

pudiendo el dispositivo, una vez encendido:

- activar (22) un primer identificador de abono temporal, estando el primer identificador de abono temporal activo en primer lugar;

- enviar a un primer servidor (18) el primer identificador (24) de abono temporal y unos primeros datos (212);

- recibir del primer servidor (18) un primer mensaje (216) de resultado que incluye un fallo de autenticación basado en los primeros datos;

caracterizado por que el dispositivo está configurado para entonces:

- determinar (218) un segundo identificador de abono temporal y al menos un secreto asociado con al menos el segundo identificador de abono temporal, estando el segundo identificador de abono temporal asociado con el primer identificador de abono temporal;

- cambiar (220) del primer identificador de abono temporal al segundo, estando el segundo identificador de abono temporal activo en segundo lugar;

- generar (230) unos segundos datos usando el al menos un secreto;

- enviar al primer servidor (18) el segundo identificador (222) de abono temporal y los segundos datos (232); y

- recibir del primer servidor (18) un segundo mensaje (236) de resultado que incluye un éxito de autenticación basado en los identificadores de abono temporales primero y segundo asociados y los segundos datos.

10. Dispositivo según la reivindicación 9, en el que el dispositivo incluye un terminal, un terminal de usuario o un elemento seguro.

11. Dispositivo según la reivindicación 10, en el que el elemento seguro incluye:

- una tarjeta de tipo SIM;

- una eUICC;

- un SRM;

- una llave inteligente de tipo USB;

- una tarjeta de tipo SD;

- una tarjeta de tipo microSD;

- una tarjeta de tipo MMC.

12. Sistema para autenticar un dispositivo en una red móvil,

comprendiendo el sistema al menos un servidor (16, 18) y el dispositivo (12), estando el dispositivo conectado al servidor,

una vez encendido, el dispositivo puede:

- activar (22) un primer identificador de abono temporal, estando el primer identificador de abono temporal activo en primer lugar;

- enviar a un primer servidor el primer identificador (24) de abono temporal y unos primeros datos (212);

el primer servidor puede enviar al dispositivo un primer mensaje (216) de resultado que incluye un fallo de autenticación basado en los primeros datos;

caracterizado por que el dispositivo está configurado para entonces:

- recibir el primer mensaje (216) de resultado que incluye un fallo de autenticación basado en los primeros datos;

- determinar (218) un segundo identificador de abono temporal y al menos un secreto asociado con al menos el segundo identificador de abono temporal, estando el segundo identificador de abono temporal asociado con el primer identificador de abono temporal;

- cambiar (220) del primer identificador de abono temporal al segundo, estando el segundo identificador de abono temporal activo en segundo lugar;

- generar (230) unos segundos datos usando el al menos un secreto;

- enviar al primer servidor el segundo identificador (222) de abono temporal y los segundos datos (232); y

por que el primer servidor está configurado para entonces:

- recibir el segundo identificador (222) de abono temporal y los segundos datos (232), estando asociado el segundo identificador de abono temporal con el primer identificador de abono temporal;

- determinar (224), basándose en al menos el segundo identificador de abono temporal, el al menos un secreto; y

- enviar al dispositivo un segundo mensaje (236) de resultado que incluye un éxito de autenticación basado en los identificadores de abono temporales primero y segundo asociados y los segundos datos.

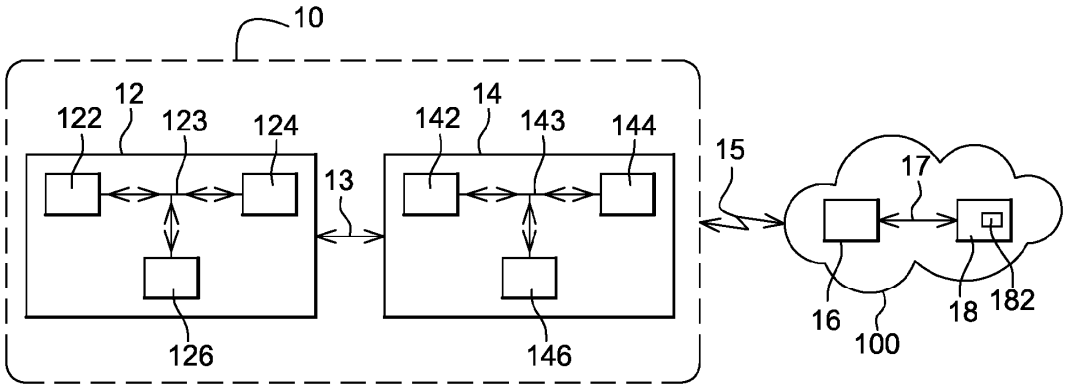

Fig. 1

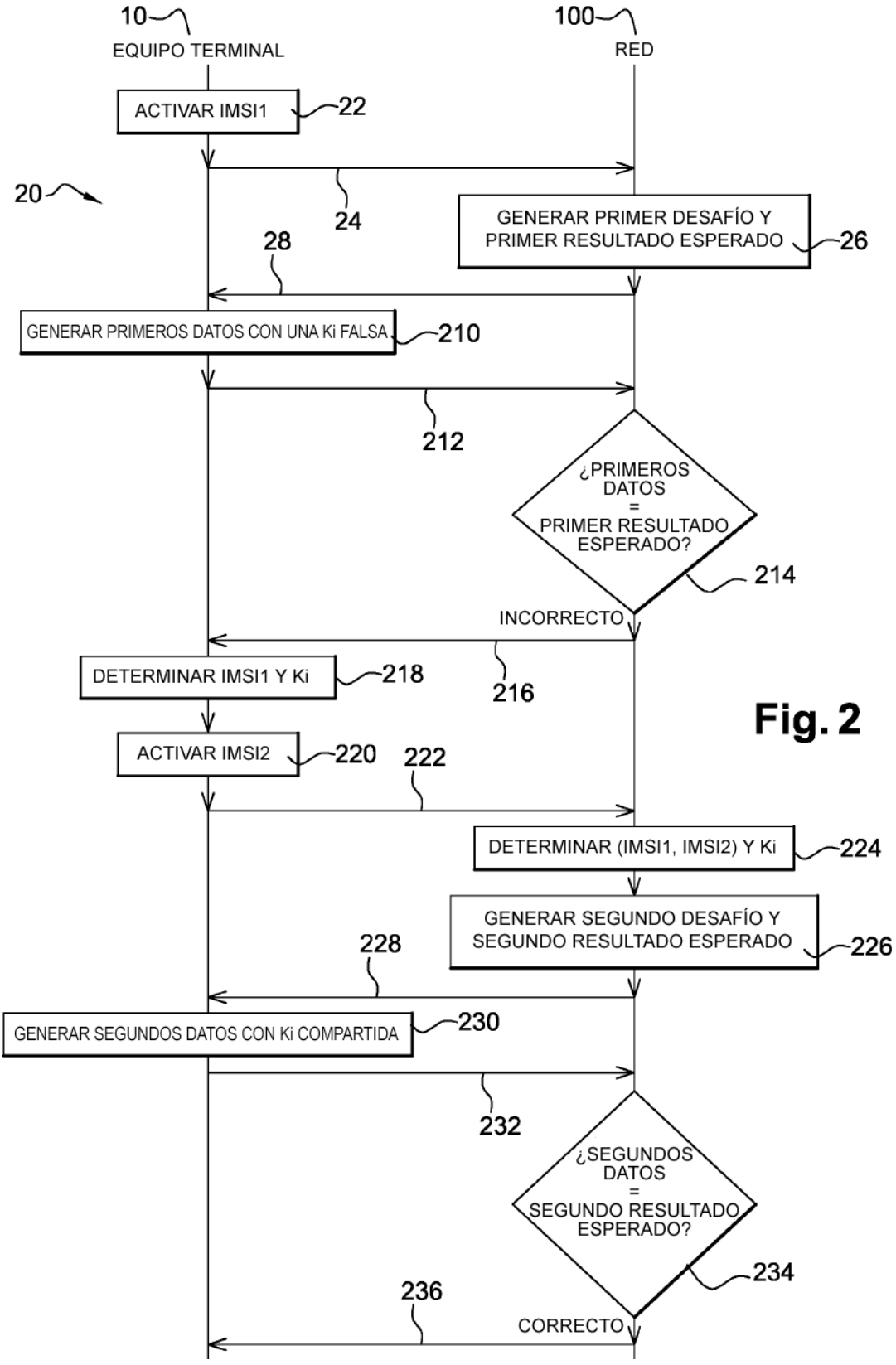
10
EQUIPO TERMINAL
100
RED
ACTIVAR IMSI1
22
20
24
GENERAR PRIMER DESAFÍO Y PRIMER RESULTADO ESPERADO
26
28
GENERAR PRIMEROS DATOS CON UNA Ki FALSA
210
212
¿PRIMEROS DATOS = PRIMER RESULTADO ESPERADO?
214
INCORRECTO
DETERMINAR IMSI1 Y Ki
218
216
ACTIVAR IMSI2
220
222
DETERMINAR (IMSI1, IMSI2) Y Ki
224
GENERAR SEGUNDO DESAFÍO Y SEGUNDO RESULTADO ESPERADO
226
228
GENERAR SEGUNDOS DATOS CON Ki COMPARTIDA
230
232
¿SEGUNDOS DATOS = SEGUNDO RESULTADO ESPERADO?
234
236
CORRECTO

Fig. 2