(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 754 216**

(51) Int. CI.:

H04W 8/18 (2009.01)
H04W 8/20 (2009.01)
H04W 4/50 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.11.2015 E 15197121 (5)**

(97) Fecha y número de publicación de la concesión europea: **31.07.2019 EP 3029968**

(54) Título: **Método de aprovisionamiento de un perfil de abonado para un módulo asegurado**

(30) Prioridad:

04.12.2014 FR 1461910

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.04.2020

(73) Titular/es:

IDEMIA FRANCE (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

LARIGNON, GUILLAUME y
DANREE, ARNAUD

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de aprovisionamiento de un perfil de abonado para un módulo asegurado

CAMPO TÉCNICO DE LA INVENCIÓN

El campo de la invención se refiere a un método de aprovisionamiento de un perfil de abonado a un terminal que comprende un módulo asegurado, el terminal y un servidor para aprovisionar perfiles de un abonado.

Actualmente, un terminal de comunicación móvil incluye un módulo asegurado destinado a alojar uno o más perfiles de un abonado a los servicios. En el caso de un teléfono móvil, el servicio básico es ofrecido por un operador (también denominado por el acrónimo MNO (Operador de Red Móvil) por la denominación en inglés "Mobile Network Operator") para el acceso a una red de comunicación móvil para el intercambio de datos a distancia.

Sin embargo, está previsto que un terminal también pueda ofrecer el acceso a otros servicios de terceros, tales como, por ejemplo, un servicio de pago o un servicio de televisión por pago. A modo de ejemplo, una tarjeta de pago bancaria virtual. El módulo asegurado aloja también varios perfiles para acceder a varios servicios.

Se entiende que el perfil del abonado significa al menos los identificadores de la línea del abonado, los datos criptográficos necesarios para su autenticación ante el operador del servicio (claves y algoritmos criptográficos) y los identificadores del operador.

Cuando un abonado desea renovar su oferta de servicios, es necesario actualizar, agregar o sustituir un perfil de abonado en el módulo asegurado.

En el caso de un teléfono móvil, el módulo asegurado es una tarjeta SIM extraíble (el “Módulo de Identidad de Abonado“, "Subscriber Identity Module" en inglés o más comúnmente denominado UICC por "Universal Integrated Circuit Card” “Tarjeta de Circuito Integrado Universal”) que se sustituye para beneficiarse del acceso a una red de comunicación móvil de otro operador.

En el caso de un terminal de tipo M2M (en inglés "Machine to Machine" “Máquina a Máquina”), el módulo asegurado está soldado al terminal y, por lo tanto, no es extraíble. Se le suele designar por eUICC por “embedded Universal Integrated Circuit Card” “Tarjeta de Circuito Integrado Universal integrada)”. El terminal puede ser un vehículo, un dispositivo de telemetría o cualquier aparato de adquisición de datos a distancia. Se espera que el fabricante del terminal proponga una solución para la actualización remota de software del módulo asegurado. Para ello, el operador del servicio integrado en el terminal tiene medios de comunicación inalámbricos seguros para acceder al módulo asegurado y desplegar nuevos perfiles de un abonado.

Se conoce, en el estado de la técnica, soluciones para la actualización remota de un módulo asegurado que es extraíble o no.

La solicitud de patente de Estados Unidos US20130012159A1 da a conocer una solución de despliegue de un nuevo perfil en un módulo asegurado extraíble. El módulo incluye un primer perfil de iniciación para establecer una primera comunicación que permita cargar un segundo perfil de un operador. Cuando se activa el segundo perfil, el primer perfil se configura en un estado inactivo.

La solicitud de patente de Estados Unidos 20140134981A1 da a conocer un método para actualizar el perfil del abonado o cargar varios perfiles en un módulo asegurado soldado. En particular, da a conocer los bloques funcionales del módulo asegurado del abonado y el servidor de aprovisionamiento del perfil del abonado para la preparación del perfil del abonado y su envío seguro según lo especificado por la asociación GSMA (el acrónimo para “Sistema Global para las Comunicaciones Móviles", “Global System for Mobile Communication Association” en inglés.

La solicitud de patente de Estados Unidos US2013217361A1 da a conocer un método que permite actualizar los parámetros de un terminal móvil, tales como, por ejemplo, un APN después de un cambio de perfil de abonado en la tarjeta SIM de dicho terminal.

Estas soluciones no prevén la actualización de los parámetros del entorno operativo del terminal que están asociados con el operador anterior. Por ejemplo, el terminal debe configurarse con parámetros relacionados con su perfil de abonado para conectarse a los servicios del operador, por ejemplo, una dirección IP en la red Internet o una dirección de un punto de acceso de la red de comunicación móvil del operador para acceder a una red de datos de tipo 4G. Lo que antecede es problemático porque la compensación de la configuración del terminal con el módulo asegurado puede evitar la primera conexión al servidor del nuevo operador. Por ejemplo, si la notificación de actualización se envía a través de la red de datos, el operador puede perder la información que es perjudicial para la continuidad del servicio para el cliente.

Otro problema puede ser que el terminal quede configurado con la imagen del operador inicial cargado por el fabricante o el operador del servicio. En este último caso, los parámetros del terminal pueden ser la imagen al inicio del terminal, el logotipo del operador y los códigos de color de la interfaz. El desplazamiento de la configuración entre el terminal y el módulo asegurado puede inducir a error al cliente.

Por lo tanto, es necesario resolver los problemas antes mencionados y proponer una solución global para actualizar un terminal que garantice, a la vez, la actualización del módulo asegurado y la actualización de los parámetros del terminal para garantizar al menos la continuidad del servicio al cliente.

SUMARIO

La invención está definida por las reivindicaciones.

Más concretamente, la invención se refiere a un método de aprovisionamiento de un perfil de abonado a un terminal que comprende un módulo asegurado destinado a alojar el perfil de abonado a una red de comunicación móvil y un entorno operativo del terminal.

Según la invención, el método comprende las siguientes etapas sucesivas ejecutadas por el terminal:

- la recepción de una demanda de aprovisionamiento de un servidor distante que comprende al menos el perfil del abonado y los parámetros de terminal asociados con el perfil,
- la carga del perfil del abonado en el módulo asegurado,
- la recepción de una primera notificación de la activación del perfil en el módulo asegurado desde el módulo asegurado,
- la configuración del entorno operativo con la configuración del terminal, activada por la primera notificación.

Según una forma de realización, el método comprende, después de la carga, la recepción de una demanda de activación del perfil proveniente del servidor distante, y la primera notificación de activación es una respuesta del módulo asegurado a través de un primer canal asegurado para la demanda de activación.

Según una forma de realización, el método comprende, después de la configuración, la ejecución de un procedimiento de una segunda notificación de la activación del perfil en el módulo asegurado entre el módulo asegurado y el servidor distante.

Según una forma de realización, el método comprende la recepción de una demanda de reinicio del terminal entre la configuración y el procedimiento de la segunda notificación.

Más concretamente, los parámetros del terminal comprenden al menos el nombre de un punto de acceso para una conexión a una red de datos de la red de comunicación móvil.

Según una forma de realización, la demanda de aprovisionamiento comprende, además, una firma del perfil y los parámetros para una demanda de autenticación por parte del módulo asegurado.

Además, la carga se realiza después de la recepción de una notificación de autenticación de la firma.

Según una forma de realización, la demanda de aprovisionamiento se recibe a través de un segundo canal asegurado entre el terminal y el servidor distante, siendo el segundo canal asegurado un intercambio de tipo SMS, CAT_TP o HTTPS.

Más concretamente, los parámetros son específicos de un identificador del terminal.

Según una forma de realización, el método comprende, además, antes de la recepción, la determinación del identificador del terminal mediante el módulo asegurado y el envío del identificador del terminal al servidor distante.

Según una forma de realización, comprende, además, después de la carga, la recepción de la notificación de la carga del perfil desde el módulo asegurado, y luego la recepción de una demanda de activación del segundo perfil desde el servidor distante.

La invención proporciona un terminal que comprende un módulo asegurado destinado a alojar un perfil de abonado en una red de comunicación móvil y un entorno operativo del terminal.

Según la invención, el terminal comprende:

- un medio de recepción de una demanda de aprovisionamiento de un servidor distante que comprende al menos el perfil del abonado y los parámetros de terminal asociados con el segundo perfil,

- medios para cargar el perfil en el módulo asegurado y para recibir una notificación de activación del perfil en el módulo asegurado,

y un medio de configuración del terminal con los parámetros del terminal cuando se recibe la notificación de activación del módulo asegurado.

La invención también proporciona un servidor para aprovisionar un perfil de abonado a una red de comunicación móvil que comprende un registro de perfil, medios de procesamiento para iniciar el aprovisionamiento del perfil a un terminal de abonado y para crear una demanda de aprovisionamiento y un medio de envío de la demanda de aprovisionamiento al terminal.

Según la invención, el servidor comprende, además:

- un registro de parámetros de terminal asociados con el perfil del abonado,

- y la demanda de aprovisionamiento de terminal comprende al menos el perfil de un abonado y los parámetros de terminal asociados con el perfil.

Más concretamente, los parámetros del terminal comprenden al menos el nombre de los puntos de acceso para una conexión a una red de datos de la red de comunicación móvil del perfil del abonado asociado.

Según una forma de realización, el servidor comprende un medio para recibir un identificador del terminal.

Gracias al método de aprovisionamiento según la invención, el terminal se configura después de la activación del perfil cargado en el módulo asegurado. La configuración del terminal se activa al recibir la primera notificación de activación del perfil desde el módulo asegurado hacia el terminal.

Por lo tanto, el terminal se configura con los parámetros del operador de la red de telefonía antes de enviar notificaciones de activación a un servidor distante o a una red de comunicación del servidor de aprovisionamiento del operador.

El método garantiza que las notificaciones a un servidor distante se emitan correctamente. También permite el uso de la red de datos del nuevo operador para enviar notificaciones de activación.

Otras características y ventajas de la presente invención aparecerán más evidentemente al leer la siguiente descripción detallada de las formas de realización de la presente invención proporcionadas a título de ejemplos no limitativos e ilustrados por los dibujos adjuntos, en los que:

BREVE DESCRIPCIÓN DE LAS FIGURAS

La Figura 1 representa un diagrama de las comunicaciones entre un terminal que aloja un módulo asegurado y la red de comunicación de un operador.

La Figura 2 representa más concretamente el servidor para aprovisionar perfiles de abonado para el aprovisionamiento de un módulo asegurado.

La Figura 3 representa un flujo de secuencia del método de aprovisionamiento del módulo asegurado y del terminal.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

La invención se aplica al aprovisionamiento de un perfil de abonado para un servicio y parámetros de terminal asociados con el perfil del abonado. El objetivo de la invención es impedir problemas de correspondencia entre el perfil del abonado al servicio del terminal y la configuración del terminal. El propósito de la invención es describir el método de aprovisionamiento de un nuevo perfil de abonado a un terminal móvil, así como los parámetros del terminal móvil asociado con dicho nuevo perfil.

La Figura 1 es un diagrama de una forma de realización que muestra el ecosistema en donde se utiliza la invención. Se aplica a un terminal móvil 10 que comprende un módulo asegurado 11 destinado a alojar perfiles de abonado. En esta forma de realización, intervienen dos perfiles 11A, 11B, siendo el primer perfil 11A un perfil activado en el módulo asegurado y el perfil 11B es un perfil que se debe aprovisionar en el módulo asegurado 11 para sustituir el perfil 11A o para añadir un segundo perfil activo.

El módulo asegurado 11 es preferiblemente un tipo de circuito integrado UICC para realizar funciones criptográficas que incluyen, en particular, la autenticación del módulo asegurado 11 a un servicio 3A, 3B. El módulo asegurado 11 también puede ser un área de software y hardware de un terminal reconocido como protegido y fiable, también denominado TEE (por “Entono de Ejecución Seguro”, “Trusted Execution Environment” en inglés). El módulo asegurado 11 se comunica con un servidor de aprovisionamiento de perfil de abonado distante 20 para recibir los perfiles de abonado.

Se comenzará con una descripción del terminal 10 y del módulo asegurado 11. El terminal 10 es un dispositivo de comunicación móvil, por ejemplo, un tipo de teléfono móvil, un dispositivo de telemetría incorporado o una instalación gestionada a distancia. En esta forma de realización, el módulo asegurado aloja un primer perfil de abonado 11A y el terminal está configurado con los primeros parámetros 14A. Un entorno operativo 13 permite la operación del terminal 10 y su funcionamiento con un servicio 3A de un operador a través del perfil 11A y los parámetros 14A. El entorno operativo se configura mediante archivos de configuración y entre estos archivos de configuración los parámetros de terminal 14A, 14B asociados con los perfiles de abonado 11A, 11B.

Para realizar las funciones de seguridad, el módulo asegurado 11 comprende dominios de seguridad para gestionar protocolos de comunicación con entidades externas, por ejemplo el terminal 10, un servidor de aprovisionamiento de perfil de abonado distante 20 o redes de comunicación móvil, para gestionar los perfiles de abonado y para el alojamiento del identificador del módulo asegurado y de los datos criptográficos, tal como un identificador utilizado para el aprovisionamiento de perfiles de abonado, claves de personalización del módulo asegurado, claves de autenticación y claves de sesión.

El módulo asegurado 11 puede ser extraíble y tener el formato de una tarjeta SIM para insertarse en el terminal móvil 10. El terminal puede ser un teléfono móvil o una tableta multimedia. Los servicios 3A, 3B a los que se autentica el módulo asegurado 11 son, en este caso, las redes de comunicación de telefonía móvil celular 3A, 3B.

En otra forma de realización denominada de tipo M2M, el módulo asegurado 11 (tipo eUICC) está soldado en el terminal 10 y no es extraíble. El módulo asegurado 11 es un circuito integrado que puede autenticarse en una o más redes móviles 3A, 3B, del tipo de red celular. El terminal puede ser un teléfono móvil, un vehículo motorizado o un dispositivo de telemetría, a modo de ejemplo.

Conviene señalar que los servicios 3A, 3B pueden ser servicios de pago que requieren autenticación del usuario por medio de un perfil alojado en el módulo asegurado, tal como un servicio audiovisual de pago, telecomunicaciones por satélite o un servicio de telemetría que utiliza una red de datos privada.

En el contexto de las redes de comunicación móvil 3A, 3B, son utilizadas por un operador y cada una de las redes ofrece un tipo de servidor de comunicación de voz, tipo de mensaje (SMS, Servicio de Mensajes Cortos, en inglés "Short Message Service") pero también una red de datos 30A, 30B. Se entiende que una red de datos 30A, 30B de un operador móvil significa una red 2G, 3G, 4G o LTE. Se trata de una red de comunicación por transmisión de paquetes de datos, del tipo de protocolo de Internet y requiere acceso a un portal del operador cuya dirección debe conocer el terminal 10. Los protocolos de comunicación de las redes de datos de tipo LTE 30A, 30B se definen mediante especificaciones emitidas por organismos de normalización. Se trata, por ejemplo, de las normas emitidas por el Instituto Europeo de Normas de Telecomunicaciones ETSI (European Telecommunication Standards Institute en inglés) o el Proyecto de Acuerdo de tercera Generación, 3GPP (para “third Generation Partnership Project” en inglés).

El acceso al portal del operador se indica mediante los parámetros 14A, 14B en el entorno operativo 13 del terminal 10. Para acceder a una red de datos 30A, 30B, los parámetros 14A, 14B del terminal son los nombres de los puntos de acceso de la red del operador, también denominados APN (Nombre del Punto de Acceso), para "Access Point Name" en inglés. Los parámetros 14A, 14B pueden comprender varios nombres de puntos de acceso con diferentes privilegios dependiendo de las aplicaciones utilizadas en el terminal móvil 10.

El entorno operativo 13 puede ser, por ejemplo, un entorno IOS, Android, Linux (marcas registradas) o cualquier otro tipo de entorno que permita el funcionamiento del terminal 10. El entorno operativo incluye archivos de configuración para la gestión de los parámetros del terminal 10.

Más concretamente, los parámetros 14A, 14B del terminal están asociados con el perfil del abonado alojado en el módulo asegurado 11. Según se describió con anterioridad, pueden ser los datos de puntos de acceso específicos a la red de comunicación móvil 3A, 3B del operador, pero también una imagen del entorno operativo 13 específico para el operador (logotipo, color, animaciones, fotografías, a modo de ejemplo) o parámetros asociados con una aplicación para acceder a un servicio del operador.

Se entiende que los parámetros 14A, 14B del terminal están asociados con el perfil del abonado 11A, 11B, respectivamente, en particular porque los parámetros del terminal 14A generalmente no son compatibles con el perfil del abonado 11B y, por el contrario, los parámetros del terminal 14B no son compatibles con el perfil 11A. Estos son

parámetros que no se pueden usar con otro servicio que no sea el del operador. Estos parámetros están definidos por el operador del perfil del abonado con el que está asociado.

Además, los parámetros del terminal 14A, 14B y las demandas de configuración de los parámetros 14A, 14B en el terminal son específicos del entorno operativo que se ejecuta en el terminal de destino.

Además, el entorno operativo 13 aloja un agente de aprovisionamiento 12. El agente de aprovisionamiento 12 es un intermediario de comunicación entre el servidor distante 20 para aprovisionar el perfil y el módulo asegurado 11. En particular permite, a la recepción de demandas o de notificaciones del servidor distante 20, ejecutar los órdenes apropiados entre el terminal 10 y el módulo asegurado 11. Por el contrario, a la recepción de demandas o notificaciones del módulo asegurado 11, permite ejecutar las órdenes adecadas entre el terminal 10 y el servidor distante 20.

El agente de aprovisionamiento 12 es una entidad del terminal colaborativo con el servidor distante 20. Es emitido y mantenido por la misma entidad a cargo del servidor distante 20. Esta entidad puede ser el operador de un servicio de telecomunicación, el fabricante del módulo asegurado, el fabricante del terminal o un operador de servicios externo. El agente de aprovisionamiento 12 es una aplicación de software alojada por el entorno operativo 13 del terminal, de tipo java, por ejemplo, que utiliza las funciones y métodos de aplicación para recibir demandas, notificaciones, datos y órdenes que se intercambiarán con el módulo asegurado 11 y el servidor distante 20.

El agente de aprovisionamiento 12 puede comunicarse con el módulo asegurado 11 a través de un primer canal asegurado C1. Para ello, comprende medios para recibir y enviar datos 122. Se trata de un canal de comunicación seguro que comprende el uso del protocolo APDU, Unidad de Datos de Protocolo de Aplicación (para "Application Protocol Data Unit" en inglés) definido en la norma ISO/SEC 7816-4. La norma define los intercambios que comprenden las demandas y respuestas entre el terminal 10 y el módulo asegurado 11. También se puede mencionar a la norma GlobalPlatform v.2.2.1 que define un marco de intercambios para acceder a los dominios de seguridad de un módulo asegurado. Más concretamente, la norma define, en particular, órdenes APDU para transmitir datos entre el terminal 10 y el módulo asegurado 11, intercambios que pueden iniciarse mediante una aplicación del terminal o un servidor distante para el aprovisionamiento de perfiles.

El módulo asegurado 11 a través del agente de aprovisionamiento 12 puede comunicarse con el servidor distante 20 a través de un segundo canal asegurado C2. Este segundo canal asegurado C2 utiliza SMS, el protocolo CAT_TP (por "Card Application Toolkit Transport Protocol") o el protocolo HTTPS (por "HyperText Transfer Protocol Secure"). Por ejemplo, el módulo asegurado 11 y el agente de aprovisionamiento 12 pueden poner en práctica protocolos de comunicaciones tales como normalizados en las normas ETSI TS 102 226, 3GPP TS 31.111 o 3GPP TS 31.116. El canal asegurado se establece, por ejemplo, mediante una fase de autenticación mutua por medio de datos criptográficos aprovisionados en un dominio seguro del módulo asegurado 11.

Dentro del marco de un aprovisionamiento de un perfil de abonado en el módulo asegurado, el servidor 20 o el módulo asegurado 11 inicia un procedimiento de intercambio de un perfil de abonado. La Figura 2 da a conocer con mayor precisión las funciones de un servidor distante 20 para aprovisionar un perfil en un módulo asegurado del tipo eUICC.

El servidor 20 de getsión de un perfil de abonado a una red de comunicación móvil utiliza medios para preparar un perfil de abonado, la demanda de aprovisionamiento y los medios de transmisión al módulo asegurado 11.

Para ello, se utiliza un registro 21 que comprende los perfiles de abonado 11A, 11B para una red de comunicación móvil. El operador de la red de comunicación móvil actualiza el registro. Un perfil contiene los datos utilizados para el funcionamiento de un perfil de abonado para acceder y utilizar el servidor del operador, en particular los identificadores de abonado para la red (IMSI, por sus siglas en inglés, "International Mobile Subscribe Identity", Identidad Internacional del Abonado Móvil), las claves de autenticación, un dominio de seguridad del operador, también denominado MNO-SD, una aplicación de acceso a la red, designada por NAA por "Network Access Application", Aplicación de Acceso a la Red.

Para un caso de aprovisionamiento en un módulo asegurado soldado al terminal, la estructura de un perfil de abonado aprovisionado en el módulo asegurado 11 está designada por el Perfil de Seguridad de Dominio Emisor, ISD-P ("Issuer Secutity Domain Profile" en inglés) y se especifica en la norma GSMA "Remote Provisioning Architecture for Embedded UICC Technical Specification", versión 2.0. El perfil del abonado contiene al menos la información especificada en la norma GSMA.

Además, según la invención, el servidor 20 comprende un registro 22 de parámetros de terminal 14A, 14B asociados con el perfil de un abonado. Estos parámetros dependen del modelo de terminal que se define según un modelo de fabricante o un identificador de terminal IMEI, Identidad Internacional de Equipo Móvil ("International Mobile Equipment Identity" en inglés, a modo de ejemplo). El identificador es preferiblemente exclusivo del terminal 10 y se puede unir a un modelo de fabricante específico conocido por el servidor distante 20. Los operadores de la red de

comunicación móvil 3A, 3B establecen los parámetros 14A, 14B asociados con su perfil de abonado en función del identificador del terminal.

Además, el servidor incluye medios de procesamiento 24 para iniciar el aprovisionamiento del perfil a un terminal de abonado y para crear una demanda para aprovisionar un perfil de abonado al módulo asegurado. El aprovisionamiento puede ser iniciado por el operador o por el abonado. Los medios de preparación de la demanda de aprovisionamiento de un perfil de abonado de designa por el SM-DP (por "Subscription Manager Data Preparation" en inglés) en la norma GSMA.

El servidor 20 comprende medios 23 para establecer un protocolo de intercambio seguro con el módulo asegurado a través del terminal 10. Estos medios de comunicación están designados en la norma GSMA por SM-SR (por "Subscription Manager Secure Rounting"). Según lo especificado para el módulo asegurado, el servidor 20 puede establecer el canal asegurado C2 con el módulo asegurado 11 de tipo HTPPS, CAT_TP, SMS. Por supuesto, el terminal 10 y el módulo asegurado 11 comprenden los medios adaptados para el funcionamiento mutuo del canal asegurado C2 con el servidor 20.

Conviene señalar que una entidad de software recíproca a la entidad SM-SR del servidor está presente en el módulo asegurado 11 para establecer el protocolo de intercambio. Esta entidad está designada por ISD-R, Emisor de Seguridad de Dominio Raíz (por "Issuer Security Domain Root" en inglés) de conformidad con la norma GSMA.

Según la invención, la demanda de aprovisionamiento del terminal comprende al menos el perfil de un abonado 11B y los parámetros del terminal 14B asociados con el perfil 11B. Los parámetros del terminal móvil 14A, 14B pueden ser preparados con el perfil de abonado 11A, 11B por el operador o durante la preparación de la demanda de aprovisionamiento al módulo asegurado 11 con el objetivo del aprovisionamiento por el SM-DP del servidor.

Por ejemplo, la demanda de aprovisionamiento requiere la creación de un perfil de abonado en el módulo asegurado y puede incluir para su ejecución el comando APDU "INSTALL COMMAND" en el terminal 10 para la instalación del perfil 11B en el módulo asegurado 11. La demanda de aprovisionamiento prevé una respuesta del módulo asegurado y el estado de ejecución de la órden.

Cualquiera que sea el modo de preparación de los parámetros del terminal móvil 14B para su aprovisionamiento, es importante tener en cuenta que se envían con la misma demanda para aprovisionar el perfil del abonado 11B al que están asociados o durante el mismo protocolo de aprovisionamiento de perfil de abonado 11B. Esto permite que el terminal 10 se aprovisione anticipadamente con los parámetros correspondientes 14B para activar el perfil aprovisionado 11B.

Conviene observar que, en una forma de realización, la demanda de aprovisionamiento puede ir acompañada de una firma 17 del perfil del abonado 11B y los parámetros del terminal 14B para la autenticación por el módulo asegurado 11.

La Figura 3 representa el flujo de secuencia del método de aprovisionamiento del perfil del abonado 11B y los parámetros 14B del terminal. El módulo asegurado 11 contiene un perfil de abonado activo 11A y el terminal móvil 10 está configurado con los parámetros 14A.

Antes de iniciar el aprovisionamiento de un segundo perfil de abonado, debe asegurarse de que el servidor distante 20 conozca el modelo del terminal de abonado 10. El identificador del modelo del terminal puede ser el número IMEI, a modo de ejemplo. En un primer caso, el servidor distante 20 ha recibido la información de identificación del terminal 10 por parte del operador. En un segundo caso, el módulo asegurado 11 inicia una demanda 201 para recibir un identificador del terminal 10. El terminal 10 transmite el identificador del terminal 10 por medio de una respuesta 202 hacia el módulo asegurado 11.

Posteriormente, el módulo asegurado 11 envía el identificador del terminal al servidor distante 20 mediante un mensaje de envío 203, a través del canal asegurado C2.

El servidor distante 20 procesa durante una etapa 204 el mensaje que contiene el identificador del terminal y determina los parámetros del terminal a asociar con el módulo asegurado 11. El servidor distante 20 dispone de una base de datos de una pluralidad de configuración de parámetros de terminal en función de un operador.

En una forma de realización del método, se puede prevér que el servidor distante 20 que aloja los medios de procesamiento 24 de la demanda de aprovisionamiento (la entidad SM-DP) reciba los parámetros del terminal 14B a través de un canal de comunicación asegurado de otro servidor del operador de perfil de abonado.

Cuando el servidor distante 20 recibe una demanda para aprovisionar un segundo perfil de abonado 11B para cargarlo en el módulo asegurado, el servidor distante 20 prepara una demanda de aprovisionamiento. La demanda contiene el perfil de abonado 11B, los parámetros del terminal 14B, así como, pero no necesariamente, una firma de los parámetros del perfil 11B y 14B con un certificado del módulo asegurado 11.

El servidor distante 20 transmite al agente de aprovisionamiento 12 la demanda de aprovisionamiento 205 a través del canal asegurado C2. El agente de aprovisionamiento 12 realiza la recepción de la demanda de aprovisionamiento 205 del servidor distante 20 que comprende al menos el perfil de abonado 11B y los parámetros de terminal 14B asociados con el perfil 11B.

En una etapa 206, el agente de aprovisionamiento 12 realiza un almacenamiento temporal en una memoria volátil del terminal móvil 10 de los parámetros del terminal 14B asociados con el segundo perfil 11B aprovisionado.

Conviene señalar que en esta fase el terminal móvil 10 todavía está configurado con los parámetros del terminal 14A asociado con el perfil de abonado 11A que también se activa en el módulo asegurado 11.

Si hay una firma presente en la demanda de aprovisionamiento, el agente de aprovisionamiento 12 realiza una demanda de autenticación 207 de la firma ante el módulo asegurado 11.

El módulo asegurado 11 realiza una autenticación 208 de la firma del perfil de abonado 11B y de los parámetros del terminal móvil 14B.

En caso de autenticación satisfactoria, el módulo asegurado 11 transmite una notificación 209 para la validación de la firma 17 ante el agente de aprovisionamiento 12. En el caso contrario, el proceso de aprovisionamiento se suspende.

Al recibir la notificación de validación 209, el agente de aprovisionamiento 12 envía una demanda de carga 210 del segundo perfil de abonado en el módulo asegurado 11. Los parámetros del terminal 14B se mantienen almacenados en la memoria del terminal.

A continuación, el módulo asegurado 11 realiza la instalación 211, en archivos de configuración, de información del perfil de abonado 11B. Durante esta etapa 211, se instala un dominio seguro del tipo ISD-P específico para el perfil de abonado 11B en el módulo asegurado 11.

Una notificación 212 del estado de la carga del perfil de abonado 11b se transmite al agente de aprovisionamiento 12. La notificación 212 es una respuesta a la demanda 210. También se proporciona una notificación de respuesta 213 de la ejecución de la carga al servidor distante 20 desde el agente de aprovisionamiento 12 a través del canal asegurado C2. Las notificaciones 212, 213 informan al terminal y al servidor distante 20 del estado de la carga del perfil 14B en el módulo asegurado.

Al recibir una notificación 213 de una carga válida, el servidor 20 transmite una demanda de activación 214 por un lado del perfil de abonado 11B en el módulo asegurado 11 y por otro lado los parámetros 14B del terminal al agente de aprovisionamiento 12. La demanda de activación 214 puede incluir una órden APDU para ser ejecutada por el terminal de tipo STORE DATA que contiene las instrucciones de activación al módulo asegurado 11 para activar el perfil de abonado 11B. Dicha demanda puede prevér una respuesta de estado de la ejecución de la activación. La demanda de activación 214 también contiene las instrucciones para que el agente de aprovisionamiento 12 realice la configuración de los parámetros del terminal 14B.

La demanda de activación 214 puede enviarse, a través del canal asegurado C2, inmediatamente en respuesta a la recepción de la notificación de carga 213 o emitirse bajo la validación de una condición adicional, por ejemplo, una duración o una orden de activación.

Posteriormente, el agente de aprovisionamiento 12 transmite una demanda de activación 215 del perfil de abonado 11B al módulo asegurado 11. Se trata de la ejecución de la orden APDU contenida en la demanda 214. Las instrucciones para que el agente de aprovisionamiento 12 realice la configuración de los parámetros del terminal 14B está pendiente.

El módulo asegurado 11 realiza entonces la operación de activación 216 del perfil del abonado 11B, esta operación se da a conocer, por ejemplo, en la norma GSMA mencionada anteriormente. En esta fase, el perfil de abonado 11B se activa en el módulo asegurado, en el caso contrario se suspende el método de aprovisionamiento. Esta operación puede prevér la desactivación del perfil de abonado 11A. Además, esta operación prevé la respuesta del módulo asegurado 11 a la orden de activación 214 del servidor 20 que contiene el estado de la operación de activación en el módulo asegurado 11.

La notificación de activación 217 se transmite al agente de aprovisionamiento 12. Esta notificación también puede proporcionar una notificación para ser enviada al servidor 20. La notificación 217 se recibe desde el módulo asegurado 11 a través del canal asegurado C1. Esta notificación es la respuesta a la orden de activación 214 del servidor 20, que comprende el estado de la operación de activación.

Al recibir esta notificación, el agente de aprovisionamiento 12 realiza la configuración 218 del entorno del terminal 10 con los parámetros 14B. Los parámetros 14B son parámetros para lograr el acceso a un servicio asociado con el operador del perfil de abonado 11B que está activado. Por ejemplo, el nombre del punto de acceso a una red de datos del operador del perfil de abonado 11B se configura en el entorno 13 del terminal 10. Los parámetros del terminal 14A asociados con el perfil 11A que acaba de desactivarse están desactivados. Si el perfil 11A no se ha desactivado, los parámetros 14A se mantienen activos en el terminal 10.

La configuración 218 activada por la notificación 217 asegura que el terminal esté configurado con la configuración compatible con el perfil activado en el módulo asegurado. La configuración se realiza antes de enviar una notificación de activación al servidor distante 20 o a una red de comunicación 3B del operador.

Una vez que la configuración 218 del terminal 10 se realizó con los parámetros 14B, el módulo asegurado 11 envía una demanda de reactivación 219 del terminal 10 al entorno operativo del terminal. Lo que antecede puede ser la órden proactiva REFRESH APDU. La orden realiza la ejecución de un procedimiento de conexión de red 3B del perfil activado en el módulo asegurado.

El método comprende, además, un procedimiento de notificación de activación 220 entre el servidor distante 20 y el módulo asegurado 11 a través del canal asegurado C2. El método de notificación 220 valida la instalación del segundo perfil 11B en el módulo asegurado recíprocamente con el servidor de aprovisionamiento de perfil distante 20. Este procedimiento de notificación prevé el intercambio de mensajes y puede ejecutar la eliminación del primer perfil de abonado 11A si se ha deshabilitado. Conviene señalar que esta etapa de notificación está de conformidad con el procedimiento de instalación de un nuevo perfil en el módulo asegurado de conformidad con la norma GSMA antes citada.

En una forma de realización, el procedimiento de notificación 220 se realiza entre el módulo asegurado 11 y un servidor distante de la red de comunicación del operador del perfil 11B. El procedimiento de notificación, por ejemplo, utiliza el acceso a la red de datos configurada por los parámetros 14B.

También está previsto después de la configuración 218 del terminal, una notificación de activación 221 de los parámetros del terminal 14B en el entorno operativo 13 del terminal 10 desde el terminal al servidor distante 20. La notificación 221 está asociada en la notificación 217. La notificación 221 es la respuesta de estado de la operación de activación del perfil 11B en el módulo asegurado 11. Gracias a la invención, esta notificación puede transmitirse, por ejemplo, a través de la red de datos cuyo acceso se establece mediante los parámetros 14B.

Al recibir las notificaciones de activación de conformidad con la configuración 218, el servidor distante 20 actualiza sus registros 21, 22 para introducir el perfil de abonado activo en el módulo asegurado 11 y los parámetros del terminal configurados en el terminal 10.

Gracias a la presente invención, el método de aprovisionamiento asegura que el terminal esté configurado con los parámetros del operador antes del envío de las notificaciones 220 y 221 al servidor distante 20 (o a un servidor distante de la red de comunicación del operador). Se garantiza la correspondencia de las configuraciones de los servidores distantes y del terminal. La continuidad del servicio está asimismo garantizada.

REIVINDICACIONES

1. Método de aprovisionamiento de un perfil de abonado a un terminal (10) que comprende un módulo asegurado (11) destinado a alojar el perfil de abonado (11B) a una red de comunicación móvil (3B) y un entorno operativo (13) del terminal (10), caracterizado porque comprende las siguientes etapas sucesivas ejecutadas por el terminal (10):

- la recepción de una demanda de aprovisionamiento (205) procedente de un servidor distante (20) que comprende al menos el perfil del abonado (11B) y los parámetros del terminal (14B) asociados con el perfil (11B),

- la carga (210) del perfil de abonado (11B) en el módulo asegurado (11),

- después de dicha carga, la recepción de una notificación (212) de la carga (210) del perfil de abonado (11B) desde el módulo asegurado (11) y el envío de una notificación (213) informando al servidor distante (20) de dicha carga,

- la recepción de una demanda de activación (214) de dicho perfil (11B) del servidor distante (20),

- la recepción de una primera notificación de la activación (217) del perfil (11B) en el módulo asegurado (11) que se emite desde el módulo asegurado (11),

- la configuración (218) del entorno operativo (13) con los parámetros del terminal (14B) activados por la primera notificación (217).

2. Método según la reivindicación 1, caracterizado porque la primera notificación de activación (217) es una respuesta del módulo asegurado (11) a través de un primer canal asegurado (C1) a la demanda de activación (215).

3. Método según cualquiera de las reivindicaciones 1 a 2, caracterizado porque comprende después de la configuración (218) la ejecución de un procedimiento de una segunda notificación (220) de la activación del perfil (11B) en el módulo asegurado (10) entre el módulo asegurado (11) y el servidor distante (20).

4. Método según la reivindicación 3, caracterizado porque comprende la recepción de una demanda para reiniciar el terminal (219) entre la configuración (218) y el procedimiento de la segunda notificación (220).

5. Método según cualquiera de las reivindicaciones 1 a 4, caracterizado porque los parámetros del terminal (14B) comprenden al menos el nombre de un punto de acceso para una conexión a una red de datos (30B) de la red de comunicación móvil (3B).

6. Método según cualquiera de las reivindicaciones 1 a 5, caracterizado porque la demanda de aprovisionamiento comprende, además, una firma (17) del perfil (11B) y parámetros (14B) para una demanda de autenticación (207) por el módulo asegurado (11).

7. Método según la reivindicación 6, caracterizado porque la carga (210) se realiza después de la repceción de una notificación de autenticación (209) de la firma (17).

8. Método según cualquiera de las reivindicaciones 1 a 7, caracterizado porque la demanda de aprovisionamiento se recibe a través de un segundo canal asegurado (C2) entre el terminal (10) y el servidor distante (20), siendo el segundo canal asegurado un intercambio de tipo SMS, CAT_TP o HTTPS.

9. Método según la reivindicación 8, caracterizado porque los parámetros (14B) son específicos de un identificador del terminal (10).

10. Método según la reivindicación 9, caracterizado porque comprende, además, antes de la recepción (205), la determinación (202) del identificador del terminal (10) por el módulo asegurado (11) y el envío (203) del identificador del terminal (10) al servidor distante (20).

11. Un terminal (10) que comprende un módulo asegurado (11) destinado a alojar un perfil de abonado (11B) a una red de comunicación móvil (3B) y un entorno operativo (13) del terminal (10), caracterizado porque comprende:

- un medio de recepción (121) de una demanda de aprovisionamiento de un servidor distante (20) que comprende al menos el perfil de abonado (11B) y los parámetros (14B) del terminal (10) asociados con dicho perfil, recibiendo dicho medio de recepción, además, una demanda de activación (214) de dicho perfil (11B) del servidor distante (20);

- medios de carga del perfil (11B) en el módulo asegurado (11) y de recepción de una notificación de activación (217) del perfil (11B) en el módulo asegurado (11),

- medios para recibir, después de la carga del perfil de abonado (11B), una notificación (212) de la carga (210) del perfil de abonado (11B) emitida desde el módulo asegurado (11), y para enviar una notificación (213) informando al servidor distante (20) de dicha carga,

- y un medio de configuración del terminal (10) con los parámetros del terminal (14B) cuando se recibe la notificación de activación (217) desde el módulo asegurado (11).

12. Servidor de aprovisionamiento (20) de un perfil de abonado (11B) a una red de comunicación móvil (3B) que comprende un registro (21) del perfil, medios de procesamiento (24) para iniciar el aprovisionamiento del perfil a un terminal de abonado y para crear una demanda de aprovisionamiento y una demanda de activación (214) de dicho perfil y un medio de envío (23) de la demanda de aprovisionamiento y de la demanda de activación al terminal, que comprende, además:

- un registro (22) de parámetros de terminal (14A, 14B) asociado con el perfil del abonado,

- en tanto que la demanda de aprovisionamiento del terminal comprende al menos el perfil de un abonado (11B) y los parámetros del terminal (14B) asociados con el perfil (11B),

estando el servidor configurado para enviar al terminal la demanda de activación (214) de dicho perfil después de recibir una notificación (213) del terminal que informa al servidor distante (20) de la carga del perfil del abonado (11B) en el módulo asegurado (11).

13. Servidor según la reivindicación 12, caracterizado porque los parámetros del terminal (14B) comprenden al menos el nombre de los puntos de acceso para una conexión a una red de datos (30B) de la red de comunicación móvil (3B) del perfil del abonado asociado.

14. Servidor según la reivindicación 13, caracterizado porque comprende un medio de recepción de un identificador del terminal (10).

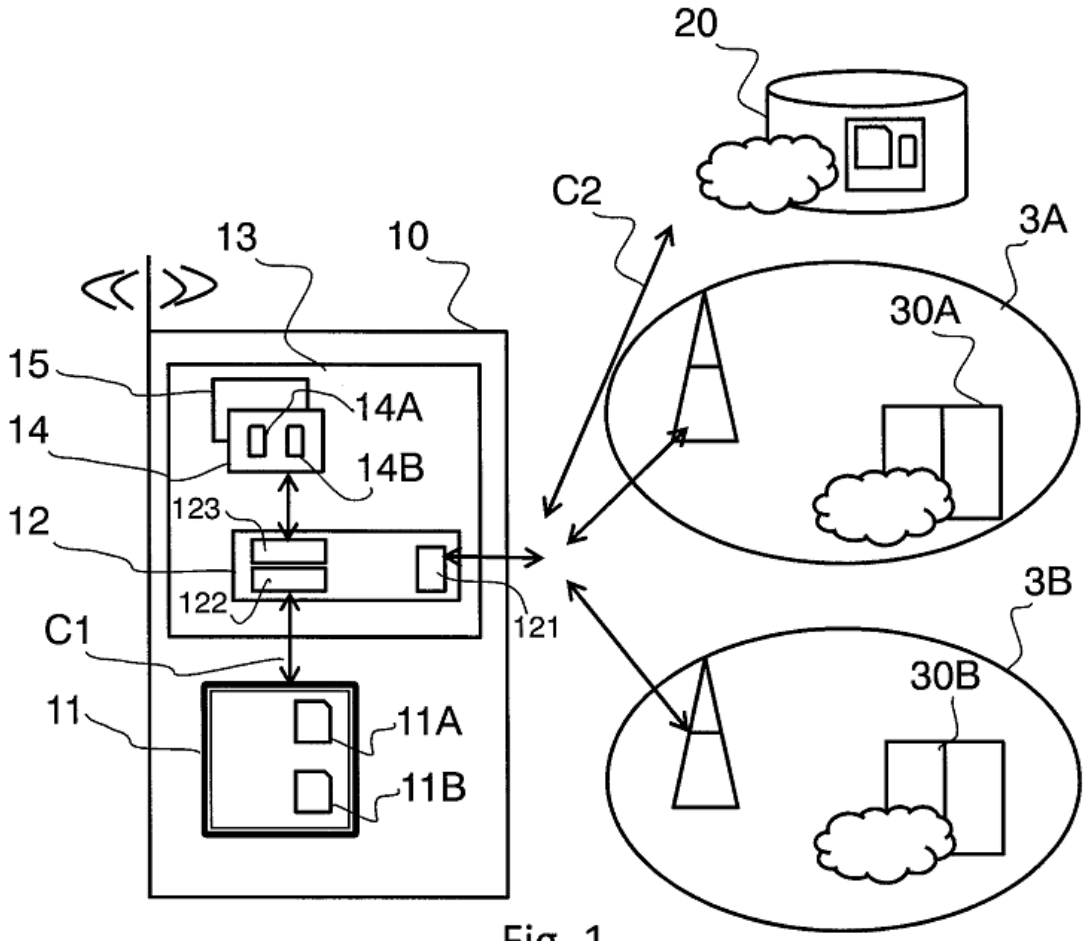
20
C2
3A
30A
13
10
15
14A
14
14B
123
12
122
121
3B
30B
C1
11
11A
11B

Fig. 1

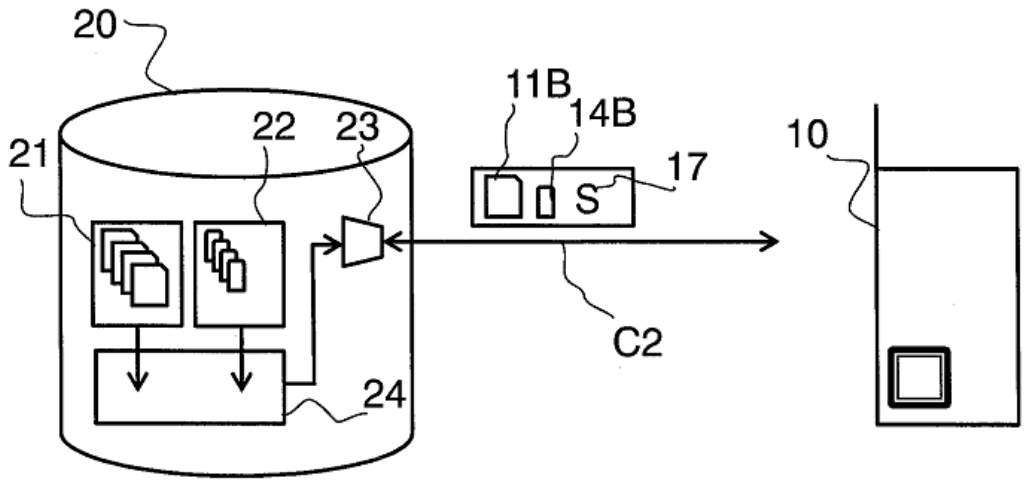
20
11B
14B
22
23
21
17
S
10
C2
24

Fig. 2

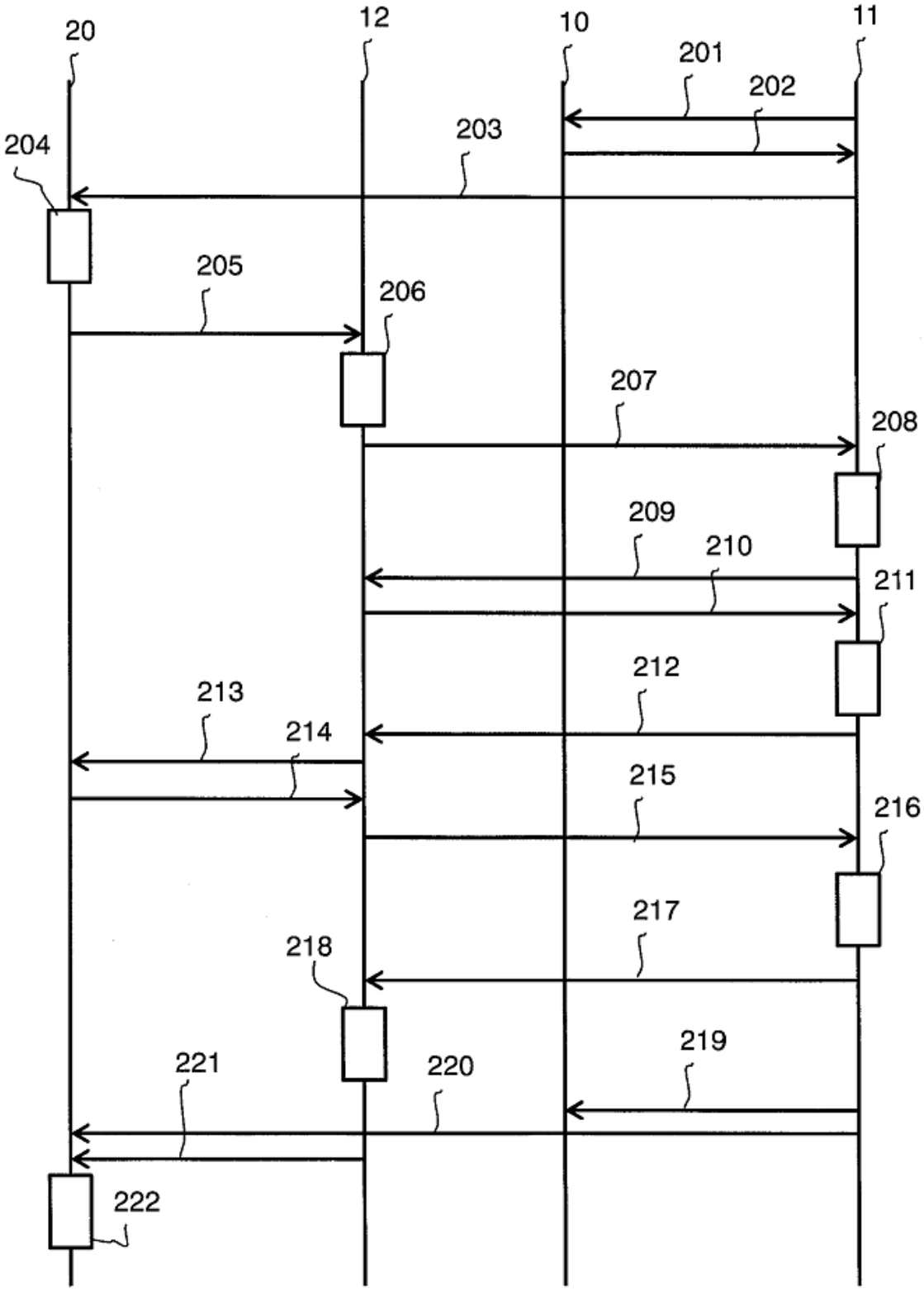
20
12
10
11
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222

Fig. 3