(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 743 576**

(51) Int. CI.:

H04W 8/20 (2009.01)
H04W 8/18 (2009.01)
H04W 12/04 (2009.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.04.2016 PCT/KR2016/003830**

(87) Fecha y número de publicación internacional: **20.10.2016 WO16167536**

(96) Fecha de presentación y número de la solicitud europea: **12.04.2016 E 16780259 (4)**

(97) Fecha y número de publicación de la concesión europea: **31.07.2019 EP 3284274**

(54) Título: **Procedimiento y aparato de gestión de un perfil de un terminal en un sistema de comunicación inalámbrica**

(30) Prioridad:

13.04.2015 US 201562146622 P
20.04.2015 US 201562149732 P
27.11.2015 KR 20150167081
08.03.2016 KR 20160027870

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.02.2020

(73) Titular/es:

SAMSUNG ELECTRONICS CO., LTD. (100.0%)
129, Samsung-ro, Yeongtong-gu, Suwon-si
Gyeonggi-do 16677, KR

(72) Inventor/es:

PARK, JONGHAN;
LEE, DUCKEY;
LEE, SANGSOO;
YEOM, TAESUN y
LEE, HYEWON

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y aparato de gestión de un perfil de un terminal en un sistema de comunicación inalámbrica

Campo técnico

La presente divulgación se refiere a un procedimiento y un aparato para descargar e instalar un servicio de comunicación a y en un terminal en un sistema de comunicación para una conexión de comunicación. Más particularmente, la presente divulgación se refiere a un procedimiento y un aparato para descargar e instalar un perfil en tiempo real en un sistema de comunicación.

Antecedentes de la técnica

Una tarjeta de circuito integrado universal (UICC) es una tarjeta inteligente insertada en un terminal de comunicación móvil, o similares, y se denomina una tarjeta UICC. La UICC puede incluir un módulo de control de acceso para acceder a una red de una operadora móvil. Un ejemplo del módulo de control de acceso puede incluir un módulo universal de identidad de abonado (USIM), un SIM, un módulo de identidad de servicio multimedia (ISIM) del protocolo de Internet (IP), o similares. La UICC que incluye el USIM se denomina generalmente una tarjeta USIM. De manera similar, la UICC que incluye un módulo de SIM se denomina generalmente una tarjeta de SIM. En la siguiente descripción de la presente divulgación, la tarjeta SIM se usa como un término general que incluye la UICC, o similares, en el que están incluidos la tarjeta de UICC, la tarjeta de USIM, y el ISIM. Es decir, la tecnología de la tarjeta SIM puede aplicarse idénticamente a la tarjeta de USIM, la tarjeta ISIM, o incluso a la tarjeta UICC general.

La tarjeta SIM puede almacenar información personal en un abonado de comunicación móvil y realizar autenticación de abonado y una generación de una clave de seguridad de tráfico tras un acceso a una red de comunicación móvil, implementando de esta manera el uso de la comunicación móvil segura.

La tarjeta SIM se fabrica generalmente como una tarjeta especializada para la correspondiente operadora móvil por una solicitud de una operadora móvil especifica tras su fabricación. Se libera de esta manera una tarjeta en la que se monta con antelación información de autenticación para acceder una red, por ejemplo, aplicación de USIM e identidad de abonado móvil internacional (IMSI), un valor K, un valor de comunicación de plataforma abierta (OPc), o similares. Por lo tanto, la correspondiente operadora móvil recibe la tarjeta de SIM fabricada y entrega la tarjeta SIM a un abonado. Posteriormente, si fuera necesario, la tarjeta SIM puede usar tecnologías en el transcurso de la comunicación (OTA), o similares, para realizar gestiones de instalación, modificación, borrado o similares, de aplicaciones en la UICC. Un abonado inserta la tarjeta de UICC en su propio terminal de comunicación móvil para usar una red de la correspondiente operadora móvil y servicios de aplicación. Además, cuando se sustituye un terminal, un abonado saca la tarjeta de UICC del terminal existente e inserta la tarjeta de UICC en un nuevo terminal, de manera que el nuevo terminal puede usar información de autenticación, un número de teléfono de comunicación móvil, un directorio de teléfonos personal o similares, que se almacenan en la UICC.

Sin embargo, la tarjeta SIM es inconveniente para que un usuario de terminal de comunicación móvil reciba servicios de otras operadores móviles. Existe la inconveniencia de que el usuario del terminal de comunicación móvil necesite obtener físicamente la tarjeta SIM para recibir servicios de una operadora móvil. Por ejemplo, también hay inconveniencia en que cuando un usuario de terminal de comunicación móvil viaja a otros países, él/ella necesita obtener una tarjeta SIM en el sitio para recibir servicios de comunicación móviles en el sitio. Un servicio de itinerancia puede resolver en cierto modo los inconvenientes anteriores, pero hay un problema en que el usuario de terminal de comunicación móvil puede no recibir los servicios de itinerancia debido a una cuota costosa y cuando no está establecido un contrato entre las operadoras móviles.

Una porción significativa de los inconvenientes anteriores puede resolverse descargando e instalando el módulo de SIM a y en la tarjeta de UICC. Es decir, el servicio de módulo de SIM de la comunicación móvil a usarse puede descargarse a la tarjeta de UICC en el momento deseado del usuario. La tarjeta UICC puede también descargar e instalar una pluralidad de módulos de SIM y puede seleccionar y usar únicamente uno de la pluralidad de módulos de SIM. La tarjeta de UICC puede estar fijada en un terminal o puede no estar fijada en el terminal. En particular, la UICC fijada en el terminal se denomina una UICC embebida (eUICC). En general, la eUICC fijada en el terminal describe la tarjeta de UICC que puede descargar y seleccionar módulos de SIM de manera remota. De acuerdo con la presente divulgación, la tarjeta de UICC que puede descargar y seleccionar el módulo de SIM de manera remota se denomina comúnmente la eUICC. La UICC fijada en el terminal o no fijada en el terminal entre las tarjetas de UICC que pueden descargar y seleccionar los módulos de SIM de manera remota se denomina comúnmente la eUICC. Además, la información en el módulo de SIM descargado se usa comúnmente como la expresión perfil de eUICC.

La información anterior se presenta como información de antecedentes únicamente, y para ayudar con una compresión de la presente divulgación. No se ha realizado determinación alguna, y no se hace afirmación alguna, en lo que respecta a si algo de lo anterior podría ser aplicable como técnica anterior con respecto a la presente divulgación.

El documento EP 2747466 A1 analiza un procedimiento de suministro de un elemento seguro de un terminal móvil con un perfil de suscripción. El documento WO 2014/092385 A1 analiza un procedimiento para seleccionar un perfil de suministro específico de entre una pluralidad de perfiles de suministro.

Divulgación de la invención

Problema técnico

Los aspectos de la presente divulgación se proporcionan para tratar al menos los problemas y/o desventajas anteriormente mencionados, y para proporcionar al menos las ventajas descritas a continuación. Por consiguiente, un aspecto de la presente divulgación es proporcionar un procedimiento y un aparato para una conexión de comunicación permitiendo que un terminal seleccione un servicio de comunicación en un sistema de comunicación.

Solución al problema

Un terminal en un sistema de comunicación inalámbrica de acuerdo con una realización de la presente divulgación incluye un receptor (denominado transceptor o comunicador) para recibir información de perfil de un servidor de transferencia de información de perfil y para recibir un perfil de un servidor de suministro de perfil usando la información de perfil y un controlador para recibir el perfil a conectarse a un servicio de comunicación.

Un servidor de transferencia de información de perfil en un sistema de comunicación inalámbrica de acuerdo con una realización de la presente divulgación incluye un transmisor y receptor (denominado transceptor o comunicador) para recibir información de perfil de un servidor de suministro de perfil y para transferir la información de perfil a un terminal y un almacenamiento para almacenar la información de perfil (almacenar temporalmente información de perfil).

Un servidor de suministro de perfil en un sistema de comunicación inalámbrica de acuerdo con una realización de la presente divulgación incluye un controlador para generar y encriptar un perfil y un transmisor (denominado transceptor o comunicador) para transmitir información de perfil a un servidor de transferencia de información de perfil y para transferir el perfil encriptado a un terminal que usa una tarjeta de circuito integrado universal embebida (eUICC).

Un procedimiento para descargar un perfil de un terminal en un sistema de comunicación inalámbrica de acuerdo con una realización de la presente divulgación incluye recibir información de perfil de un servidor de transferencia de información de perfil, recibir un perfil de un servidor de suministro de perfil usando la información de perfil, y recibir el perfil a conectarse a un servicio de comunicación.

Un procedimiento para transferir información de perfil de un servidor de transferencia de información de perfil en un sistema de comunicación inalámbrica de acuerdo con una realización de la presente divulgación incluye recibir la información de perfil de un servidor de suministro de perfil y transferir la información de perfil a un terminal.

Un procedimiento para proporcionar un perfil de un servidor de suministro de perfil en un sistema de comunicación inalámbrica de acuerdo con una realización de la presente divulgación incluye generar y encriptar un perfil y transferir el perfil encriptado y generado a un terminal usando una eUICC.

De acuerdo con un aspecto de la presente divulgación, se proporciona un procedimiento para instalar un perfil por un aparato electrónico en un sistema de comunicación inalámbrica. El procedimiento incluye: transmitir, a un primer servidor, un primer mensaje para solicitar información asociada con un perfil; recibir, del primer servidor, un segundo mensaje que incluye información asociada con una dirección de un segundo servidor y un identificador para un evento; transmitir, al segundo servidor, un tercer mensaje para solicitar un perfil basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento; recibir, del segundo servidor, el perfil; e instalar el perfil en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

De acuerdo con otro aspecto de la presente divulgación, se proporciona un aparato electrónico para instalar un perfil en un sistema de comunicación inalámbrica. El aparato electrónico incluye un transceptor y un controlador acoplados con el transceptor. El controlador está configurado para controlar para: transmitir, a un primer servidor, un primer mensaje para solicitar información asociada con un perfil; recibir, del primer servidor, un segundo mensaje que incluye información asociada con una dirección de un segundo servidor y un identificador para un evento; transmitir, al segundo servidor, un tercer mensaje para solicitar un perfil basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento; recibir, del segundo servidor, el perfil; e instalar el perfil en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

De acuerdo con otro aspecto de la presente divulgación, se proporciona un procedimiento por un primer servidor en un sistema de comunicación inalámbrica. El procedimiento incluye: recibir, de un segundo servidor, un primer mensaje que incluye información en un perfil para un aparato electrónico; recibir, del aparato electrónico, un segundo mensaje para solicitar información asociada con un perfil; y transmitir, al aparato electrónico, un tercer mensaje que incluye información asociada con una dirección del segundo servidor y un identificador para un evento. Se transmite un mensaje para solicitar un perfil del aparato electrónico al segundo servidor basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento. El perfil se transmite del segundo servidor al aparato electrónico y se instala en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

De acuerdo con otro aspecto de la presente divulgación, se proporciona un primer servidor en un sistema de comunicación inalámbrica. El primer servidor comprende un transceptor y un controlador acoplado con el transceptor.

El controlador está configurado para controlar para: recibir, de un segundo servidor, un primer mensaje que incluye información en un perfil para un aparato electrónico; recibir, del aparato electrónico, un segundo mensaje para solicitar información asociada con un perfil; y transmitir, al aparato electrónico, un tercer mensaje que incluye información asociada con una dirección del segundo servidor y un identificador para un evento. Se transmite un mensaje para solicitar un perfil del aparato electrónico al segundo servidor basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento. El perfil se transmite del segundo servidor al aparato electrónico y se instala en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

De acuerdo con otro aspecto de la presente divulgación, se proporciona un procedimiento por un segundo servidor en un sistema de comunicación inalámbrica. El procedimiento incluye: transmitir, a un primer servidor, un primer mensaje que incluye información asociada con una dirección del segundo servidor y un identificador para un evento del aparato electrónico; recibir, del aparato electrónico, un segundo mensaje para solicitar un perfil basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento; y transmitir, al aparato electrónico, el perfil a instalarse en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

De acuerdo con otro aspecto de la presente divulgación, se proporciona un segundo servidor en un sistema de comunicación inalámbrica. El segundo servidor incluye un transceptor y un controlador acoplado con el transceptor. El controlador está configurado para controlar para: transmitir, a un primer servidor, un primer mensaje que incluye información asociada con una dirección del segundo servidor y un identificador para un evento del aparato electrónico; recibir, del aparato electrónico, un segundo mensaje para solicitar un perfil basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento; y transmitir, al aparato electrónico, el perfil a instalarse en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

Efectos ventajosos de la invención

Otro aspecto de la presente divulgación es proporcionar un procedimiento y un aparato para descargar un perfil en tiempo real para permitir que un terminal realice una conexión de comunicación en un sistema de comunicación.

Otro aspecto de la presente divulgación es proporcionar un aparato y un procedimiento para proporcionar un perfil a un terminal en un sistema de comunicación.

Breve descripción de los dibujos

Los anteriores y otros aspectos, características, y ventajas de ciertas realizaciones de la presente divulgación se harán más evidentes a partir de la siguiente descripción tomada en conjunto con los dibujos adjuntos, en los que:

La Figura 1 es un diagrama que ilustra un procedimiento de conexión de comunicación móvil de un terminal que usa una tarjeta de circuito integrado universal (UICC) en la que está instalada un perfil de acuerdo con una realización de la presente divulgación;
La Figura 2 es un diagrama que ilustra un procedimiento de conexión de comunicación móvil de un terminal usando una UICC que puede descargar e instalar un perfil de acuerdo con una realización de la presente divulgación;
La Figura 3A es un diagrama que ilustra un procedimiento de conexión de comunicación móvil de un terminal usando una UICC que puede descargar e instalar un perfil de acuerdo con una realización de la presente divulgación;
Las Figuras 3B a 3D son diagramas que ilustran una porción de una operación de la Figura 3A de acuerdo con una realización de la presente divulgación;
La Figura 4 es un diagrama que ilustra una operación de un terminal de punto de venta (PoS) usado en un procedimiento de descarga e instalación de un perfil de las Figuras 3A a 3D de acuerdo con una realización de la presente divulgación;
La Figura 5 es un diagrama que ilustra una pantalla de un terminal antes y después de que se instale un perfil de acuerdo con una realización de la presente divulgación;
Las Figuras 6A y 6B son diagramas que ilustran una operación detallada de un procedimiento de descarga e instalación de un perfil de acuerdo con una realización de la presente divulgación;
La Figura 7 es un diagrama que ilustra un procedimiento de intercambio de un perfil de acuerdo con una realización de la presente divulgación;
La Figura 8 es un diagrama que ilustra una pantalla de un primer terminal y un segundo terminal de acuerdo con la realización de la Figura 7;
Las Figuras 9A y 9B son diagramas que ilustran un procedimiento para cambiar información en un servidor de suministro de información de perfil de acuerdo con una realización de la presente divulgación;
La Figura 10 es un diagrama de bloques que ilustra un servidor de suministro de perfil de acuerdo con una realización de la presente divulgación;
La Figura 11 es un diagrama de bloques que ilustra un servidor de transferencia de información de perfil de acuerdo con una realización de la presente divulgación; y
La Figura 12 es un diagrama de bloques que ilustra un aparato electrónico de acuerdo con una realización de la presente divulgación.

A través de todos los dibujos, se entenderá que los números de referencia similares harán referencia a partes,

componentes y estructuras similares.

Modo para la invención

La siguiente descripción con referencia a los dibujos adjuntos se proporciona para ayudar en una comprensión detallada de diversas realizaciones de la presente divulgación tal como es definida por las reivindicaciones y sus equivalentes. Incluye diversos detalles específicos para ayudar en esa compresión, pero estos han de considerarse como simplemente ejemplares. Por consiguiente, los expertos en la materia en la técnica reconocerán que pueden realizarse diversos cambios y modificaciones de las diversas realizaciones descritas en el presente documento sin alejarse del espíritu y alcance de la presente divulgación. Además, pueden omitirse descripciones de funciones y construcciones bien conocidas por claridad y concisión.

Los términos y palabras usados en la siguiente descripción y reivindicaciones no están limitados a los significados bibliográficos, sino que simplemente se usan para posibilitar un entendimiento claro y consistente de la presente divulgación. Por consiguiente, deberá ser evidente para los expertos en la materia que la siguiente descripción de diversas realizaciones de la presente divulgación se proporciona para el fin de ilustración únicamente, y no para el fin de limitar la presente divulgación según se define por las reivindicaciones adjuntas y sus equivalentes.

Se ha de entender que las formas singulares "un", "una", y "el/la", incluyen referentes plurales, a menos que el contexto dicte claramente de otra manera. Por lo tanto, por ejemplo, la referencia a "una superficie de componente" incluye la referencia a una o más de tales superficies.

En la presente memoria descriptiva, una tarjeta de circuito integrado universal (UICC) es una tarjeta inteligente insertada en un terminal de comunicación móvil y describe un chip que almacena información personal tal como información de autenticación de acceso de red en un abonado de comunicación móvil, un directorio de teléfono, y servicio de mensajes cortos (SMS) para realizar autenticación de abonado y una generación de una clave de seguridad de tráfico tras un acceso a redes de comunicación móviles tales como el sistema global para comunicación móvil (GSM), acceso múltiple por división de código de banda ancha (WCDMA), y la evolución a largo plazo (LTE), implementando de esta manera el uso de la comunicación móvil segura. La UICC incluye aplicaciones de comunicación tales como un módulo de identificación de abonado (SIM), un SIM universal (USIM), y un SIM multimedia (ISIM) de protocolo de Internet (IP) de acuerdo con una clase de redes de comunicación móvil a las que accede un abonado. Además, la UICC puede proporcionar función de seguridad de alto nivel para incluir diversas aplicaciones tales como un monedero electrónico, generación de tiques y un pasaporte electrónico.

En la presente memoria descriptiva, una UICC embebida (eUICC) no es un módulo de seguridad desconectable que puede insertarse en y separarse de un terminal, sino un módulo de seguridad de tipo chip que puede embeberse en un terminal. La eUICC puede usar una tecnología en el transcurso de la comunicación (OTA) para descargar e instalar un perfil. La eUICC puede denominarse la UICC que puede descargar e instalar un perfil.

En la presente memoria descriptiva, un procedimiento para descargar e instalar un perfil a y en una eUICC que usa la tecnología de OTA puede aplicarse también a una UICC desconectable que puede insertarse en y separarse del terminal. Es decir, la realización de la presente divulgación puede aplicarse a la UICC que puede descargar e instalar el perfil usando la tecnología de OTA.

En la presente memoria descriptiva, puede usarse el término UICC intercambiado con el término SIM, y puede usarse el término eUICC intercambiado con el término eSIM.

En la presente memoria descriptiva, un perfil puede describir una aplicación, un sistema de ficheros, un valor de clave de autenticación, o similares, que se almacenan en la UICC y se empaquetan en una forma de software.

En la presente memoria descriptiva, un perfil de USIM puede ser el mismo que el perfil, o puede describir información incluida en una aplicación de USIM en el perfil que se empaqueta en una forma de software.

En la presente memoria descriptiva, un servidor de suministro de perfil puede representarse por preparación de datos de gestor de suscripción (SM-DP), preparación de datos de gestor se suscripción plus (SM-DP+), entidad fuera de tarjeta de dominio de perfil, un servidor de encriptación de perfil, un servidor de generación de perfil, un aprovisionamiento de perfil (PP), un proveedor de perfil, y un titular de credenciales de aprovisionamiento de perfil (titular de PPC).

En la presente memoria descriptiva, un servidor de transferencia de información de perfil puede representarse por una función de descubrimiento y envío (DPF) y un servicio de descubrimiento de gestor de suscripción (SM-DS).

En la presente memoria descriptiva, un servidor de gestión de perfil puede representarse por encaminamiento seguro de gestor de suscripción (SM-SR), encaminamiento seguro de gestor de suscripción plus (SM-SR+), entidad fuera de tarjeta de gestor de perfil de eUICC, o un titular de credenciales de gestión de perfil (titular de PMC), y un gestor de eUICC (EM).

En la presente memoria descriptiva, cuando se nombra el servidor de suministro de perfil, el servidor de suministro de

perfil puede describirse comúnmente como que incluye una función del servidor de gestión de perfil. Por lo tanto, de acuerdo con diversas realizaciones de la presente divulgación, es decir, en la siguiente tecnología, puede realizarse una operación del servidor de suministro de perfil por el servidor de gestión de perfil. De manera similar, una operación del servidor de gestión de perfil o el SM-SR puede realizarse por el servidor de suministro de perfil.

En la presente divulgación, un sistema activador es un servidor que solicita preparación de descarga de perfil del servidor de suministro de perfil. En general, el sistema activador puede ser una parte de un sistema de soporte empresarial de una operadora móvil. Además, el sistema activador puede implementarse como la aplicación del terminal.

El término 'terminal' usado en la presente memoria descriptiva puede describirse como una estación móvil (MS), un equipo de usuario (UE), un terminal de usuario (UT), un terminal inalámbrico, un terminal de acceso (AT), un terminal, una unidad de abonado, una estación de abonado (SS), un dispositivo inalámbrico, un dispositivo de comunicación inalámbrica, una unidad de transmisión/recepción inalámbrica (WTRU), un nodo móvil, un móvil, u otros términos. Diversas realizaciones del terminal pueden incluir un teléfono celular, un teléfono inteligente que tiene una función de comunicación inalámbrica, un asistente digital personal (PDA), un módem inalámbrico, un ordenador portátil que tiene una función de comunicación inalámbrica, un aparato de fotografía tal como una cámara digital que tiene la función de comunicación inalámbrica, un aparato de juegos que tiene la función de comunicación inalámbrica, electrodomésticos para almacenar y reproducir música que tienen la función de comunicación inalámbrica, y electrodomésticos de internet que pueden implementar un acceso y exploración a internet inalámbrico. Diversas realizaciones del terminal pueden incluir también una unidad portátil o terminales en los que están integradas las combinaciones de las funciones. Además, el terminal puede incluir un terminal de máquina a máquina (M2M) y un terminal/dispositivo de comunicación de tipo máquina (MTC), aunque no está limitado a lo mismo. En la presente memoria descriptiva, el terminal puede describirse también como un aparato electrónico.

En la presente memoria descriptiva, el aparato electrónico puede tener una UICC, que puede descargar e instalar un perfil, embebido en la misma. Cuando la UICC no está embebida en el aparato electrónico, la UICC físicamente separada del aparato electrónico puede insertarse en el aparato electrónico que va a conectarse al aparato electrónico. Por ejemplo, la UICC puede insertarse en el aparato electrónico en una forma de tarjeta. El aparato electrónico puede incluir el terminal. En este caso, el terminal puede ser un terminal que incluye la UICC que puede descargar e instalar el perfil. La UICC puede estar embebida en el terminal y cuando el terminal se separa de la UICC, la UICC puede insertarse en el terminal y puede insertarse en el terminal que va a conectarse al terminal. La UICC que puede descargar e instalar el perfil puede denominarse la eUICC a modo de ejemplo.

En la presente memoria descriptiva, un discriminador de perfil puede denominarse un identificador de perfil (ID de perfil), un ID de tarjeta de circuito integrado (ICCID), y un factor adaptado con un perfil de dominio de seguridad del emisor (ISD-P) o un dominio de perfil (PD). El ID de perfil puede representar identificadores únicos de cada perfil.

En la presente memoria descriptiva, un identificador de eUICC (ID de eUICC) puede ser un identificador único de la eUICC embebida en el terminal y puede descubrirse como un EID. Además, cuando se instala un perfil de aprovisionamiento en la eUICC con antelación, puede ser un perfil ID del correspondiente perfil de aprovisionamiento. Además, de acuerdo con la realización de la presente divulgación, cuando el terminal y el chip de eUICC no están separados entre sí, puede ser un ID de terminal. Además, puede describirse también como un dominio de seguridad específico del chip de eUICC.

En la presente memoria descriptiva, un contenedor de perfil puede describirse como el dominio de perfil. El contenedor de perfil puede ser el dominio de seguridad.

En la presente memoria descriptiva, una unidad de datos de protocolo de aplicación (APDU) puede ser un mensaje para interconexión del terminal con la eUICC. Además, la APDU puede ser un mensaje para interconexión del PP o el PM con la eUICC.

En la presente memoria descriptiva, las credenciales de aprovisionamiento de perfil (PPC) pueden ser un procedimiento que se usa para autenticación mutua y encriptación de perfil entre el PP y la eUICC y una firma. La PPC puede incluir al menos una de una clave simétrica, un certificado y clave personal de Rivest Shamir Adleman (RSA), un certificado y clave personal de criptografía de curva elíptica (ECC), y una autoridad de certificación de raíz (CA de raíz) y cadena de certificado. Además, cuando hay varios PP, diferentes PMC para la pluralidad de PP pueden almacenarse en la eUICC o usarse.

En la presente memoria descriptiva, PMC puede ser un procedimiento que se usa para autenticación mutua y encriptación de datos de transmisión entre el PM y la eUICC y una firma. El PMC puede incluir al menos una de la clave simétrica, el certificado y clave personal de RSA, el certificado y clave personal de ECC, y la CA de raíz y cadena de certificado. Además, cuando hay varios PM, diferentes PMC para la pluralidad de PM pueden almacenarse en la eUICC o usarse.

En la presente memoria descriptiva, un AID puede ser un identificador de aplicación. Este valor puede ser un discriminador que discrimina diferentes aplicaciones en el eUICC.

En la presente memoria descriptiva, una etiqueta, longitud, valor (TLV) de paquete de perfil puede llamarse una TLV de perfil. La TLV de paquete de perfil puede ser un conjunto de datos que representa información que configura un perfil en un formato de TLV.

En la presente memoria descriptiva, un acuerdo de autenticación y clave (AKA) puede representar un algoritmo de autenticación para acceder al proyecto asociación de 3ª generación (3GPP) y red de 3GPP2.

En la presente memoria descriptiva, K es un valor de clave de encriptación almacenado en la eUICC que se usa para el algoritmo de autenticación AKA.

En la presente memoria descriptiva, OPc es un valor de parámetro que puede almacenarse en la eUICC que se usa para el algoritmo de autenticación AKA.

En la presente memoria descriptiva, un programa de aplicación de acceso de red (NAA) puede ser programas de aplicación tal como USIM e ISIM que se almacenan en la UICC para acceder a una red. El NAA puede ser un módulo de acceso de red.

En la siguiente descripción, cuando una descripción detallada de funciones o configuraciones conocidas relacionadas con la presente divulgación pueda oscurecer la comprensión de la presente divulgación, las descripciones detalladas de la misma pueden omitirse.

La Figura 1 es un diagrama que ilustra un procedimiento de conexión de comunicación móvil de un terminal usando una UICC en la que está instalado un perfil de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 1, una UICC 120 puede insertarse en un terminal 110. En este caso, la UICC puede ser un tipo desconectable y puede estar también embebida en el terminal con antelación. Un perfil fijo de la UICC en el que el perfil fijo está instalado describe 'información de acceso' fija que puede acceder a una operadora móvil específica. La información de acceso puede ser un denominado IMSI que es un discriminador de abonado y un valor K o un valor Ki que se requiere para autenticar una red junto con el discriminador de abonado.

El terminal puede usar la UICC para realizar la autenticación junto con un sistema de procesamiento de autenticación (denominado registro de localización doméstico (HLR) o centro de autenticación (AuC)) de una operadora móvil. El procedimiento de autenticación puede ser un procedimiento de AKA. Si la autenticación tiene éxito, el terminal puede usar una red 130 de comunicación móvil del sistema de comunicación móvil para usar servicios de comunicación móviles tales como un teléfono o un uso de datos móviles.

La Figura 2 es un diagrama que ilustra un procedimiento de conexión de comunicación móvil de un terminal usando una UICC que puede descargar e instalar un perfil de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 2, un sistema para descargar e instalar un perfil puede incluir un sistema 210 activador, un servidor 220 de suministro de perfil, un servidor 230 de transferencia de información de perfil, un terminal 240, y una red 250 de operadora móvil.

La eUICC puede insertarse en o embeberse en el terminal 240. El perfil puede descargarse a, e instalarse en la eUICC. Además, el terminal 240 puede usar una red de Internet para realizar la comunicación. La comunicación puede ser comunicación para descargar el perfil. La comunicación puede ser también Wi-Fi, Bluetooth, o similares. La comunicación puede ser también un segundo acceso de red de comunicación móvil separado que usa el perfil que está instalado en la eUICC con antelación. La comunicación puede ser también el segundo acceso de red de comunicación móvil usando un perfil instalado en una UICC 2 o una eUICC 2 que está instalada o montada de manera separada en el terminal 240 distinto de la eUICC. La segunda red de comunicación móvil puede ser la misma que o diferente de la red 250 de operadora móvil de la Figura 2. Es decir, la red de operadora móvil para descargar un perfil y la red de operadora móvil para proporcionar un servicio de comunicación usando el perfil descargado pueden ser las mismas o diferentes entre sí.

Describiendo la operación de la Figura 2, en la operación 260, el sistema 210 activador puede enviar una solicitud para preparación de perfil al servidor de suministro de perfil. El sistema 210 activador puede ser un sistema de soporte empresarial (BSS) de la operadora móvil. La solicitud puede incluir al menos una de la siguiente información.

- discriminador de eUICC;
- información en servidor de transferencia de información de perfil;
- discriminador de perfil o tipo de solicitud de perfil;
- clave de instalación de perfil;
- información de terminal; e
- información de eUICC.

El discriminador de eUICC puede ser un EID.

La información en el servidor de transferencia de información de perfil puede incluir al menos una de la siguiente información.

- dirección o discriminador que especifica uno o una pluralidad de servidores de transferencia de información de perfil; e
- tipo de interconexión con servidor de transferencia de información de perfil.

El discriminador de perfil puede ser un ICCID o un valor que puede corresponder al mismo.

El tipo de solicitud de perfil es información que puede usarse para discriminar una clase de perfil.

Cuando la clave de instalación de perfil está incluida, el servidor 220 de suministro de perfil puede ser información que puede usarse para especificar un perfil específico cuando el terminal usa la clave de instalación de perfil para solicitar el perfil.

La información de terminal es información que puede usarse también para discriminar si el servidor 220 de suministro de perfil proporciona el perfil o una clase de fichero específico.

La información de eUICC es información que puede usarse también para discriminar si el servidor 220 de suministro de perfil proporciona el perfil o una clase de fichero específico.

En la operación 265, el servidor 220 de suministro de perfil puede preparar el perfil. En este caso, si un valor de discriminador de perfil (denominado ICCID) se transfiere a la solicitud de preparación de perfil, puede prepararse el perfil que corresponde al discriminador de perfil. Además, si no hay presente discriminador de perfil, el perfil puede discriminarse usando al menos uno del tipo de solicitud de perfil, la información de terminal, la información de eUICC, y el discriminador de eUICC, y el discriminador de perfil del mismo puede especificarse. En este caso, el discriminador de perfil puede transmitirse a un servidor que transmite la solicitud de preparación de perfil. Además, cuando el discriminador de eUICC está incluido en la solicitud de preparación de perfil, el servidor 220 de suministro de perfil puede descargar o instalar el perfil especificado únicamente a y en la eUICC específica. Cuando el discriminador de eUICC no está incluido en la solicitud de preparación de perfil, el servidor de suministro de perfil puede preparar el perfil sin interconexión del perfil especificado con la eUICC específica y cuando se recibe una solicitud adecuada que incluye el discriminador de eUICC del terminal 240, el perfil puede descargarse también mediante la interconexión del perfil con la correspondiente eUICC.

Además, cuando la clave de instalación de perfil está incluida en la solicitud de preparación de perfil, el servidor de suministro de perfil gestiona la clave de instalación de perfil mediante la interconexión de la clave de instalación de perfil con el perfil específico, y cuando el terminal 240 solicita la descarga del perfil a la clave de instalación de perfil, el perfil específico puede también descargarse. La clave de instalación de perfil puede describirse también como un identificador de evento, ID de evento, o un identificador coincidente, ID coincidente, un código de activación, o un testigo de código de activación AC_testigo. Cuando la clave de instalación de perfil no está incluida en la solicitud de preparación de perfil, en la preparación de perfil, el servidor 220 de suministro de perfil puede generar directamente la clave de instalación de perfil. En este caso, después de la preparación de perfil, el servidor 220 de suministro de perfil puede transferir también la clave de instalación de perfil al sistema 210 activador.

En la operación 270, el servidor 220 de suministro de perfil puede transferir la información de perfil al servidor 230 de transferencia de información de perfil. La transferencia de información de perfil puede describir también el registro de la información de perfil en el servidor 230 de transferencia de información de perfil. El servidor 230 de transferencia de información de perfil puede recibir la información de perfil y registrar la información de perfil recibida. Cuando se registra como se ha descrito anteriormente, la información de perfil puede almacenarse también en el servidor 230 de transferencia de información de perfil.

La información de perfil puede incluir toda o una porción de la siguiente información.

- dirección de servidor de suministro de perfil;
- clave de instalación de perfil; e
- información de eUICC.

La dirección del servidor de suministro de perfil puede ser una dirección de servidor en un tipo de nombre de dominio cualificado (FQDN) completo, una dirección en un tipo de localizador de recurso uniforme (URL) completo, o una dirección de un servidor de IP.

La información de eUICC puede ser un EID específico, un valor que proporciona un resultado de operación de función de troceo al EID específico, o un EID. La operación de función de troceo para el EID describe un cálculo que incluye una operación de función de troceo. Por ejemplo, el EID puede realizarse una vez basándose en la función de troceo, el EID puede realizarse dos veces basándose en la función de troceo, o puede añadirse también información de código secreto con el EID como un factor de la función de troceo. El código secreto puede ser también un valor transferido a un usuario.

Como se ha descrito anteriormente, si la información de perfil se transfiere a o se registra en el servidor 230 de transferencia de información de perfil, en la siguiente operación 275, la información de perfil puede transferirse al terminal 240 que está conectado a la eUICC que corresponde a la información de eUICC. La transferencia de la

información de perfil al terminal 240 puede realizarse por uno de los siguientes procedimientos.

En un primer procedimiento, si el terminal 240 solicita la información de perfil del servidor 230 de transferencia de información de perfil usando la dirección del servidor de transferencia de información de perfil almacenada en el terminal 240 o la eUICC (por ejemplo, transmisión de un mensaje de solicitud de información de perfil), el servidor 230 de transferencia de información de perfil transfiere la correspondiente información al terminal (por ejemplo, transmisión de un mensaje de respuesta de información de perfil) cuando hay información de perfil que corresponde a la información de eUICC recibida en la operación 270 usando la información de eUICC transferida.

En un segundo procedimiento, el terminal 240 puede registrarse en el servidor 230 de transferencia de información de perfil con antelación usando la dirección del servidor de transferencia de información de perfil almacenada en el terminal 240 o la eUICC con antelación. La información transferida después del registro puede incluir la siguiente información.

- información de eUICC; e
- información para posibilitar que el servidor de transferencia de información de perfil transfiera información al terminal.

La información para posibilitar que el servidor de transferencia de información de perfil transfiera información al terminal puede ser una de la siguiente información.

- dirección de IP e información de puerto del terminal; e
- información sobre el servidor de transferencia de información e información de testigo de transferencia de información pre-registrada en el terminal.

La información pre-registrada en el servidor de transferencia de información puede ser otro servidor de transferencia de información conectado y establecido basándose en una IP con antelación para permitir que el terminal 240 reciba la información de perfil. El servidor de transferencia de información puede proporcionar la información de testigo de transferencia de información al terminal 240 para establecer una interfaz, y si el terminal 240 transfiere el testigo de transferencia de información al servidor 230 de transferencia de información de perfil, el servidor 230 de transferencia de información de perfil puede transferir la información de perfil y transferir el testigo de información al servidor de transferencia de información para permitir que el servidor de transferencia de información transfiera la información de perfil al terminal 240 que corresponde al testigo de transferencia de información.

Cuando la información de perfil se transfiere del servidor 220 de suministro de perfil al servidor 230 de transferencia de información de perfil, el servidor 230 de transferencia de información de perfil puede transferir la información de perfil al terminal 240 registrado.

Además, para el primer y segundo procedimientos, la información de perfil puede también ser información en un tipo codificado con un código de respuesta rápida (QR). El terminal 240 puede decodificar la información en el tipo codificado con el código de QR para realizar acuse de recibo de la información de perfil.

Si el terminal 240 recibe la información de perfil, en la operación 280, el terminal 240 puede usar la dirección del servidor de suministro de perfil y la clave de instalación de perfil incluidas en la información de perfil para solicitar el suministro del perfil al servidor 220 de suministro de perfil. El terminal 240 puede transmitir un mensaje de solicitud de perfil al servidor 220 de suministro de perfil. En detalle, el terminal 240 puede usar la dirección de FQDN de la dirección del servidor de suministro de perfil incluida en la información de perfil para obtener la dirección de IP de un servidor de nombres de dominio y solicitar el suministro del perfil a la correspondiente dirección de IP. En este caso, el terminal 240 puede transferir directamente la clave de instalación de perfil al servidor 220 de suministro de perfil o puede autenticar el servidor 220 de suministro de perfil y a continuación proporcionar la clave de instalación al servidor 220 de suministro de perfil. En este caso, el procedimiento de autenticación puede ser el siguiente procedimiento a modo de ejemplo.

El terminal 240 genera un valor aleatorio de eUICC 1 o un valor aleatorio de terminal que tiene suficiente longitud y proporciona el valor aleatorio de eUICC generado 1 o el valor aleatorio de terminal al servidor 220 de suministro de perfil. El servidor 220 de suministro de perfil usa una clave personal que corresponde a un certificado digital del servidor 220 de suministro de perfil para calcular un valor de firma digital y transfiere el valor de firma digital al terminal 240 junto con el certificado.

El terminal 240 verifica si se emite el certificado de una organización que tiene autoridad para emitir un certificado y a continuación si la verificación pasa, usa el certificado para verificar la firma. Si se verifica la firma y por lo tanto la firma es precisa, puede determinarse que el procedimiento de autenticación tiene éxito.

La operación de generación del valor aleatorio de eUICC o el valor aleatorio de terminal y verificación del certificado y firma puede realizarse por el terminal 240 o la eUICC.

El terminal 240 puede transferir también datos de generación de clave de encriptación, que pueden usarse para la encriptación del perfil, al servidor 220 de suministro de perfil. Los datos de generación de clave de encriptación pueden

transferirse junto con el valor de firma generado por la eUICC y el certificado digital de la eUICC. El certificado digital puede transferirse junto con un certificado de fabricante de eUICC (EUM) que emite el certificado. El valor de firma generado por la eUICC puede incluir la firma calculada, que incluye el valor aleatorio del servidor de suministro de perfil recibido del servidor 220 de suministro de perfil.

Posteriormente, antes de la operación 285, el servidor 220 de suministro de perfil puede verificar el valor de firma transferida del terminal 240.

El procedimiento de verificación puede ser como sigue a modo de ejemplo.

El certificado de EUM recibido se verifica como una clave pública de un emisor de certificados (CI) raíz fiable o una clave pública del certificado raíz CI que se almacena en el servidor 220 de suministro de perfil.

Si el certificado de EUM se verifica satisfactoriamente, el certificado de eUICC recibido se verifica usando la clave pública del certificado de EUM.

Si el certificado de eUICC es válido, el valor de firma recibido se verifica usando la clave pública del certificado.

Si se determina en el procedimiento de verificación que el certificado de eUICC no es válido, el servidor 220 de suministro de perfil no descarga el perfil al terminal 240 y puede finalizar la operación. El servidor 220 de suministro de perfil puede notificar al terminal 240 de un resultado de fallo de verificación.

Si toda la verificación es válida, el servidor 220 de suministro de perfil puede usar los datos de generación de clave de encriptación recibidos y el perfil datos de generación de clave de encriptación generados por el servidor de suministro de perfil para generar una clave de sesión de encriptación. La clave de sesión de encriptación puede ser una clave de sesión SCP03t, una clave de sesión SCP03, o una clave de sesión SCP11.

Volviendo a la Figura 2, en la operación 285, el servidor 220 de suministro de perfil puede transferir el perfil al terminal 240. El servidor 220 de suministro de perfil puede usar la clave de sesión de encriptación para encriptar el perfil o usar una clave de encriptación generada aleatoriamente para encriptar el perfil y a continuación encriptar la clave de encriptación aleatoria con la clave de sesión de encriptación y transferir la clave de encriptación aleatoria encriptada al terminal 240. El terminal 240 puede descargar e instalar el perfil a y en la eUICC.

En la operación 290, el terminal 240 puede instalar el perfil y a continuación activar el perfil. Mediante la activación del perfil, un procedimiento de apertura para usar un servicio de comunicación a través de la descarga del perfil al terminal 240 puede finalizar.

En la operación 295, el terminal 240 puede usar el perfil instalado en la eUICC para autenticar el sistema de comunicación móvil y a continuación usar la red de comunicación móvil.

Mediante el procedimiento de la Figura 2, el terminal 240 puede descargar el perfil a la eUICC en tiempo real y puede usar el servicio de comunicación. De acuerdo con la realización de la presente divulgación, la información de perfil puede transferirse automáticamente al terminal 240 y el terminal 240 puede usar la información de perfil para solicitar automáticamente el perfil del servidor 220 de suministro de perfil. Además, pueden proporcionarse los procedimientos de autenticación y verificación para la descarga de perfil del terminal 220 y el servidor 220 de suministro de perfil.

De acuerdo con una realización de la presente divulgación, el servidor 220 de suministro de perfil puede ser un servidor que está operado por una operadora móvil o un fabricante de eUICC y el servidor 230 de transferencia de información de perfil puede ser un servidor que se opera por un proveedor de servicio de telecomunicación móvil o una eUICC o fabricante de terminal. Tras la fabricación de la eUICC en la descarga de perfil usando la eUICC, no se define si descargar el perfil de alguno de los proveedores de red. Esto puede determinarse de acuerdo con si el usuario está suscrito en el servicio de comunicación de cualquiera de los proveedores de red. Por lo tanto, un usuario accede a un servidor operado por el proveedor de red del servicio de comunicación suscrito para descargar el perfil, pero puede no conocer información en el mismo tras la generación de la eUICC. Como resultado, es esencial obtener la dirección del servidor de suministro de perfil para descargar el perfil. De acuerdo con la realización de la presente divulgación, el terminal 240 puede recibir la información de perfil del servidor 230 de transferencia de información de perfil que es el servidor operado por la eUICC o el fabricante de terminal en el momento de descargar del perfil y solicitar el perfil del servidor 220 de suministro de perfil que corresponde a la información de perfil en tiempo real.

La Figura 3A es un diagrama que ilustra un procedimiento de conexión de comunicación móvil de un terminal usando una UICC que puede descargar e instalar un perfil de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 3A, en la operación 325, un usuario 303 de terminal visita un centro 301 de suscripción para solicitar la suscripción o apertura. El usuario 303 de terminal puede visitar un punto de venta (PoS) para solicitar la suscripción o la apertura a un agente. En la operación 326, puede obtenerse la información en el terminal que el usuario 303 de terminal solicita la suscripción o la apertura del terminal de PoS. La información en el terminal puede ser información de identificación tal como un código de QR, un código de barras, y un número de serie. Por ejemplo, el agente puede usar el terminal de PoS para explorar el código de QR visualizado en un recuadro del terminal o una

pantalla. El código de QR puede incluir al menos una de la siguiente información.

- EID; e
- ID de DPF (información de identificación en el servidor de transferencia de información de perfil).

El EID es el discriminador de eUICC.

El ID de DPF puede ser un discriminador que puede corresponder a la dirección de FQDN, la dirección de URL, o la dirección de IP del servidor de transferencia de información de perfil.

Posteriormente, en la operación 327, el terminal de PoS puede transferir una solicitud de apertura a un sistema de soporte empresarial de operador de red móvil (BSS de MNO) 305 de una operadora móvil. La solicitud de apertura puede transferir la dirección de EID y DPF.

En la operación 328, el BSS de MNO 305 puede realizar un procedimiento interno (por ejemplo, registrar información de IMSI en HLR) que requiere la apertura y a continuación transferir una solicitud de descarga de perfil al servidor 307 de suministro de perfil. El servidor 307 de suministro de perfil puede ser SM-DP+. La solicitud de descarga de perfil puede corresponder a la solicitud de preparación de perfil de la Figura 2.

En la operación 329, el servidor 307 de suministro de perfil puede transferir la información de perfil al servidor 309 de transferencia de información de perfil. El servidor 309 de transferencia de información de perfil puede recibir la información de perfil y registrar la información de perfil recibida. La información de perfil puede incluir la dirección del servidor de suministro de perfil y la información de eUICC. La dirección del servidor de suministro de perfil puede ser una dirección de servidor en un tipo FQDN, una dirección en un tipo de URL completo, o una dirección de un servidor de IP. La información de eUICC puede ser un EID específico, un valor que proporciona un resultado de operación de función de troceo al EID específico, o un EID. La operación de la Figura 3A corresponde a la operación 270 de la Figura 2 y por lo tanto otras descripciones detalladas hacen referencia a la operación 270 de la Figura 2.

En la operación 330, el servidor 309 de transferencia de información de perfil transfiere información de envío a un terminal 311. La información de envío puede ser notificación de envío. El servidor 309 de transferencia de información de perfil recupera la información que corresponde a la información de eUICC de la información de perfil basándose en la información de perfil recibida del servidor 307 de suministro de perfil. El servidor 309 de transferencia de información de perfil puede almacenar o registrar la información relacionada con la eUICC con antelación. Por ejemplo, mediante las operaciones 321, 322, 323, y 324 de la Figura 3A, el servidor 309 de transferencia de información de perfil puede obtener la información relacionada con la eUICC.

En la operación 321, el terminal 311 solicita el EID de una eUICC 313 del terminal. En la operación 322, la eUICC 313 proporciona el EID al terminal 311. En la operación 323, el terminal 311 puede solicitar el registro de la información relacionada con la eUICC del servidor 309 de transferencia de información de perfil. Por ejemplo, el terminal 311 puede proporcionar el EID de la eUICC 313 o el resultado de la operación de función de troceo del EID y solicitar el almacenamiento o registro del mismo al servidor 307 de transferencia de información de perfil. En la operación 324, el servidor 307 de transferencia de información de perfil puede transmitir el resultado registrado al terminal 311.

Como se ha descrito anteriormente, por las operaciones 321 a 324, el servidor 307 de transferencia de información de perfil puede obtener la información relacionada con la eUICC. Cuando se registra o almacena la información relacionada con la eUICC que corresponde a la información de perfil recibida en la operación 329, el servidor 307 de transferencia de información de perfil puede transmitir la información de clave al correspondiente terminal 311.

En la operación 331, el terminal 311 que recibe la información de envío solicita la información de perfil del servidor 309 de transferencia de información de perfil. El terminal 311 puede transmitir el mensaje de solicitud de transferencia de información de perfil. En la operación 332, el servidor 309 de transferencia de información de perfil puede transmitir la información de perfil al terminal 311. La operación 331 puede realizarse sin recibir la información de envío en la operación 330. En otras palabras, cuando el terminal se opera manualmente en el usuario 303 de terminal o el centro 301 de suscripción, la operación 332 puede realizarse también y puede realizarse también por otras condiciones.

En la operación 333, el terminal 311 puede usar la información de perfil para solicitar el perfil. El terminal 311 puede usar la información de perfil recibida para solicitar el perfil del servidor 307 de suministro de perfil. Por ejemplo, el terminal 311 puede transmitir el mensaje de solicitud de perfil al servidor 307 de suministro de perfil. La operación de la Figura 3A corresponde a la operación 280 de la Figura 2, y por lo tanto otras descripciones detalladas hacen referencia a la operación 280 de la Figura 2.

En la operación 334, un terminal puede descargar el perfil e instalar el perfil descargado. La operación de autenticación y verificación para descargar un perfil hace referencia a la siguiente descripción de la operación 280 de la Figura 2.

El terminal 311 puede activar el perfil instalado y usar el perfil activado para usar un servicio de comunicación a través de la red de comunicación móvil. La operación detallada de la misma hace referencia a la descripción de la correspondiente operación en la Figura 2.

La operación de la Figura 2 puede aplicarse a la Figura 3A y la descripción de la Figura 3A que corresponde a la Figura 2 hace referencia a la descripción de la Figura 2.

Las Figuras 3B a 3D son diagramas que ilustran en detalle una porción de una operación de la Figura 3A de acuerdo con una realización de la presente divulgación.

Haciendo referencia a las Figuras 3B a 3D, se describirá en mayor detalle un ejemplo de las operaciones 321 a 324 y 329 a 332 en la Figura 3A.

Haciendo referencia a la Figura 3B, puede describirse una operación interna de un terminal 341, dividiéndose en un cliente de envío y una función de gestión remota (RMF). Además, un servidor de transferencia de información de perfil (DPF) 347 puede interconectar con un servidor 345 de envío adicional, y el servidor 345 de envío puede interconectar con un cliente de envío del terminal 341. La siguiente operación del cliente de envío y la RMF corresponde a la operación del terminal.

En la operación 351, si se enciende una fuente de alimentación del terminal 341, el terminal puede estar conectado a la Internet.

En la operación 352, el terminal 341 puede leer la información de eUICC y la información de DPF de una eUICC 343. La información de eUICC puede ser el EID y la información de DPF puede ser el ID de DPF.

En la operación 353, la RMF puede leer información básica almacenada en el terminal 341 para seleccionar un servicio de envío.

En la operación 354, el terminal 341 puede transmitir un mensaje de solicitud de servicio de envío a la DPF 347. En la operación 355, el terminal 341 puede transmitir un mensaje de solicitud de servicio de envío a la DPF 347. Un mensaje de respuesta de envío puede incluir información de establecimiento de envío.

El terminal puede leer la información de establecimiento obtenida en línea para seleccionar el servicio de envío.

La información puede incluir al menos uno de un ID de servicio de envío, un ID de servidor de envío, y un ID de cliente de envío. Por conveniencia, la correspondiente información se denomina información de servicio de envío.

En la operación 356, la RMF del terminal puede solicitar el registro en el cliente de envío del terminal. Una solicitud de registro puede incluir al menos uno del RMFID y servicio de envío. En el caso de un servicio de envío de terceros, la RMF puede interconectar con el cliente de envío que corresponde al ID de servicio de envío. Sin embargo, la RMF puede combinarse con el cliente.

En la operación 357, el cliente de envío puede establecer una interfaz con el servidor 345 de envío. El procedimiento detallado puede ser diferente para cada servicio de envío. El cliente de envío necesita mantener la conexión mientras la conexión de Internet del servidor 345 de envío con el terminal es normal.

En la operación 358, el cliente de envío transfiere un mensaje de solicitud de registro al servidor 345 de envío. El mensaje de solicitud de registro puede incluir el discriminador de terminal y el RMFID. El RMFID puede ser un ID que discrimina las aplicaciones.

En la operación 359, el servidor 345 de envío puede transmitir el mensaje de respuesta de envío al terminal 341. El servidor 345 de envío puede emitir un testigo de envío que corresponde a un par de terminal y RMF y transferir el testigo de envío emitido al cliente de envío.

En la operación 360, el cliente de envío puede transmitir un mensaje de respuesta de registro a la RMF. El cliente de envío puede transmitir el testigo de envío a la RMF. El testigo de envío puede transmitirse a la DPF 347 para usarse como un uso para transmitir la notificación de envío al terminal.

Haciendo referencia a la Figura 3C, en la operación 361, el terminal 341 puede generar un testigo de EID del EID. El testigo de EID puede ser un EID de función de troceo.

En la operación 362, el terminal 341 puede transmitir un informe de servicio de envío a la DPF 347. El terminal 341 puede usar el informe de servicio de envío para registrar el servicio de envío. El informe de servicio de envío puede incluir al menos uno del EID, la información de servicio de envío, el testigo de envío, y el testigo de EID.

En la operación 363, la DPF 347 puede interconectar con el servidor 345 de envío. En este caso, la interconexión puede estar basada en un esquema de mantenimiento de la conexión.

En la operación 364, la DPF 347 puede generar el ID de notificación de envío (PNID).

En la operación 365, la DPF 347 puede transferir información que incluye al menos uno de testigo de envío, PNID, y testigo de EID al servidor 345 de envío. La DPF 347 puede transmitir el ID de notificación de envío que incluye al menos uno del testigo de envío, el PNID, y el testigo de EID al servidor 345 de envío.

En la operación 366, el servidor 345 de envío puede transferir el ACK de notificación de envío a la DPF 347.

En la operación 367, el servidor 345 de envío transfiere la notificación de envío al terminal 341. El servidor 345 de envío puede usar el testigo de envío para especificar un cliente de envío específico y a continuación transferir la notificación de envío al terminal. La notificación de envío puede incluir al menos uno del testigo de envío, el PNID, y el testigo de EID.

En la operación 368, el terminal 341 puede transferir el ACK de notificación de envío al servidor 345 de envío. El ACK de notificación de envío puede incluir al menos uno del testigo de envío y el PNID.

En la operación 369, el servidor 345 de envío puede transferir de nuevo el ACK de notificación de envío a la DPF 347. El ACK de notificación de envío puede incluir al menos uno del testigo de envío y el PNID.

En la operación 370, el cliente de envío puede transferir la notificación de envío a la RMF. La notificación de envío puede incluir el testigo de EID.

En la operación 371, el terminal 341 puede usar una dirección de DPF pre-establecida para transmitir una solicitud de evento a la DPF 347. La solicitud de evento puede incluir el EID.

En la operación 372, la DPF 347 puede transferir la información de evento registrada incluida en la respuesta de evento al terminal 341. En el ejemplo anterior, puesto que la DPF 347 no tiene aún un evento para el correspondiente terminal 341, puede transferirse un discriminador que indica que el evento no está presente (sin evento).

Haciendo referencia a la Figura 3D, en la operación 373, el servidor 349 de suministro de perfil puede transferir la información de perfil a la DPF 347. La operación 373 puede corresponder a la operación 329 de la Figura 3A.

En la operación 374, la DPF 347 realiza acuse de recibo de la información de servicio de envío, el testigo de envío, el testigo EID, o similares, que corresponde a la correspondiente eUICC 343.

En la operación 375, la DPF 347 transfiere la notificación de envío al correspondiente servidor 345 de envío basándose en la información que se ha realizado acuse de recibo. La notificación de envío puede incluir al menos uno del testigo de envío, el PNID, y el testigo de EID.

En la operación 376, el servidor 345 de envío puede transferir el ACK de notificación de envío a la DPF 347.

En la operación 377, el servidor 345 de envío transfiere la notificación de envío al terminal 341. El servidor 345 de envío puede usar el testigo de envío para especificar el cliente de envío específico y a continuación transferir la notificación de envío al terminal. La notificación de envío puede incluir al menos uno del testigo de envío, el PNID, y el testigo de EID.

En la operación 378, el terminal 341 puede transferir el ACK de notificación de envío al servidor 345 de envío. El ACK de notificación de envío puede incluir al menos uno del testigo de envío y el PNID.

En la operación 379, el servidor 345 de envío puede transferir de nuevo el ACK de notificación de envío a la DPF 347. El ACK de notificación de envío puede incluir al menos uno del testigo de envío y el PNID.

En la operación 380, el cliente de envío puede transferir la notificación de envío a la RMF. La notificación de envío puede incluir el testigo de EID.

En la operación 381, el terminal 341 puede convertir el testigo de EID al EID.

La operación 382 puede corresponder a la operación 331 de la Figura 3. En la operación 382, el terminal 341 transmite la solicitud de evento a la DPF 347. La solicitud de evento puede incluir el EID.

En la operación 383, la DPF 347 puede transmitir la respuesta de evento al terminal 341. La solicitud de evento puede incluir el EMID e ID de evento. A diferencia de la operación 372, puesto que el evento recibido del servidor 349 de suministro de perfil, la operación 383 puede recibir la dirección y el ID de evento del servidor de suministro de perfil que puede procesar el correspondiente evento.

Posteriormente, como se ilustra en la Figura 2 o 3A a 3D, la descarga de perfil puede progresarse también. Además, puede progresarse también un procedimiento de control remoto descrito en la realización de las Figuras 9A y 9B a continuación.

La Figura 4 es un diagrama que ilustra una operación de un terminal de PoS usado en un procedimiento de descarga e instalación de un perfil de las Figuras 3A a 3D de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 4, tras realizar la operación 360 de la Figura 3B, se muestra una operación ejemplo de un terminal 410 de PoS y un ejemplo de un diseño del recuadro 405 del terminal. La información 407 de código puede visualizarse en el diseño 405 de recuadro del terminal para obtener la información en el terminal. En la información 407 de código, puede visualizarse la información tal como un código de QR, un código de barras

bidimensional, un código de barras unidimensional, y un número de serie. Como la información 407 de código, puede codificarse al menos uno del EID de la eUICC incluida en el terminal y la información de dirección del servidor de transferencia de información de perfil. El terminal 410 de PoS puede usar una tecnología de ACK de información de código (por ejemplo, lector de código de QR, lector de código de barras, lector de reconocimiento óptico de caracteres (OCR), y similares) para explorar la información 407 de código, obteniendo de esta manera la información en el terminal. El terminal 410 de PoS puede visualizar un resultado de exploración de la información 407 de código en una región 417 de identificación de información de código y visualizar un resultado de identificación de información de código en una región 420 de visualización. La región 420 de visualización también puede omitirse.

Una región 430 de entrada de solicitud de apertura puede visualizarse también en el terminal 410 de PoS. La solicitud de apertura incluye una solicitud para transferir la información en el terminal al MNO o al BSS de MNO. Si hay una entrada a la región 430 de entrada de solicitud de apertura, como la operación 365 de la Figura 3C, el terminal 410 de PoS puede transferir la información en el terminal al sistema de BSS del MNO. Es decir, el EID o la información de identificación (información de dirección) del servidor de transferencia de información de perfil pueden transferirse al BSS de MNO.

La Figura 5 es un diagrama que ilustra una pantalla de un terminal antes y después de que se instale un perfil de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 5, el número 510 de referencia representa la pantalla del terminal antes de que se instale el perfil y el número 520 de referencia representa la pantalla del terminal después de que se instala el perfil. Haciendo referencia al número 510 de referencia, la información sobre el fabricante de eUICC puede representarse en una primera región 513 antes de que se instale el perfil. El fabricante de eUICC y el fabricante de terminal pueden ser el mismo que o diferentes entre sí. Si el perfil está instalado o activado puede representarse en la segunda región 515. El número 510 de referencia es una operación antes de que se instale el perfil y por lo tanto puede representar información que puede representar si el perfil está instalado actualmente, tal como sin perfil, sin instalación de perfil y sin activación de perfil.

Haciendo referencia al número 520 de referencia, si el perfil está instalado, la pantalla puede cambiarse en comparación con el número 510 de referencia. La información de proveedor del perfil instalado puede representarse en una tercera región 523. La información de proveedor puede ser un nombre de un proveedor de red que corresponde al perfil instalado. La información de usuario del perfil instalado puede representarse en una cuarta región 525. Puede representarse la información de un nombre, un teléfono, o similares, de un usuario que corresponde a la información de suscripción del usuario.

Las Figuras 6A y 6B son diagramas que ilustran una operación detallada de un procedimiento de descarga e instalación de un perfil de acuerdo con una realización de la presente divulgación.

Las Figuras 6A y 6B ilustran en detalle un ejemplo de las operaciones después de la operación 280 de la Figura 2 y la operación 380 de la Figura 3D. Por lo tanto, la operación de las Figuras 6A y 6B puede ser una operación que puede aplicarse a las Figuras 2 a 3D.

Haciendo referencia a la Figura 6A, en la operación 640, un terminal 620 puede obtener información de perfil. El terminal 620 recibe la dirección y la clave de instalación de perfil del servidor de suministro de perfil del servidor de transferencia de información de perfil. De acuerdo con la realización de la Figura 6A, una eUICC 630 se inserta en o se embebe en el terminal 620 y la operación del terminal 620 y la eUICC 630 pueden analizarse como la operación interna del terminal.

En la operación 642, el terminal 620 puede introducir un código secreto usando la información de clave de instalación de perfil obtenida. La operación 642 no es esencial y si no hay código secreto, puede no realizarse como una opción.

En la operación 644, el terminal 620 solicita una generación de un desafío de eUICC de la eUICC 630.

En la operación 646, si el terminal 620 solicita la generación del desafío de eUICC, la eUICC 630 genera el desafío de eUICC y a continuación lo almacena.

En la operación 648, la eUICC 630 transfiere el desafío de eUICC generado e información de certificación, información de certificado, al terminal 620. La información de certificación, información de certificado, puede incluir una clase de certificados de eUICC y una clase de claves de encriptación usables. La información de clave de encriptación puede describir un parámetro de curva elíptica. La información de clave de encriptación puede ser plural y puede incluir información de manera separada para usarse para generar una firma e información usada para verificar la firma.

En la operación 650, el terminal 620 puede transferir el desafío de eUICC y la información de certificado que incluye adicionalmente la información de dirección del servidor de suministro de perfil incluida en la información de perfil a un servidor 610 de suministro de perfil que corresponde a la información de dirección.

En la operación 652, el servidor 610 de suministro de perfil puede comprobar si el servidor de suministro de perfil recibido es válido. Puede comprobarse si el servidor de suministro de perfil recibido es válido verificando si la

información de dirección recibida del servidor de suministro de perfil es la misma que su propia dirección de servidor o realiza acuse de recibo de si la información de dirección recibida del servidor de suministro de perfil corresponde a cualquiera de una pluralidad de direcciones válidas. Si el procedimiento de comprobación de si el servidor de suministro de perfil recibido es válido falla, el servidor 610 de suministro de perfil puede transferir un código de error al terminal 620 y detener la operación de descarga de un perfil.

El servidor 610 de suministro de perfil puede comprobar también la información de certificado. Puede comprobarse si el tipo de certificado es válido. Además, puede comprobarse si la información de clave de encriptación puede soportarse por el servidor 610 de suministro de perfil. La comprobación puede ser un procedimiento de comparación de si la información de clave de encriptación para la firma de la eUICC 630 coincide con la información de clave de encriptación que puede verificarse por el servidor 610 de suministro de perfil con si la información de clave de encriptación para la verificación por la eUICC 630 coincide con la información de clave de encriptación usada para generar la firma por el servidor 610 de suministro de perfil. Si el procedimiento de comprobación es válido, el servidor 610 de suministro de perfil puede almacenar el tipo de certificado a usarse y la información de encriptación y a continuación generar un ID de transacción. El servidor 610 de suministro de perfil puede realizar acuse de recibo de si el siguiente mensaje de solicitud del terminal 620 es válido usando el ID de transacción. El ID de transacción puede ser también un identificador de evento, ID de evento. El servidor de suministro de perfil puede a continuación generar un desafío de DP. El desafío de DP puede ser un desafío del SM-DP o un desafío del servidor de suministro de perfil. El desafío de DP puede ser un número aleatorio de 16 bytes. El servidor 610 de suministro de perfil puede a continuación generar la DP_señal. La DP_señal puede ser un valor de firma generado por el servidor 610 de suministro de perfil, en el que el valor de firma incluye desafío_eUICC, desafío_DP, ID de transacción.

Si la operación 652 se realiza normalmente, el servidor 610 de suministro de perfil puede transferir la información de autenticación al terminal 620 en la operación 654. El servidor 610 de suministro de perfil puede transferir el ID de transacción, el desafío de DP, la DP_señal, un certificado de un servidor de suministro de perfil, e información de Certificado_a_usarse al terminal 620. El certificado del servidor de suministro de perfil puede ser un algoritmo de firma digital de curva elíptica (ECDSA). El Certificado_a_usarse puede ser información que incluye el tipo de certificado y la información de encriptación que se almacena en el servidor 610 de suministro de perfil.

En la operación 656, el terminal 620 puede transferir un tiempo actual del terminal, la dirección del servidor de suministro de perfil, la clave de instalación de perfil, la información de terminal, el código secreto de función de troceo a la eUICC 630, además de la información recibida. En este caso, el código secreto de función de troceo puede transferirse cuando se realiza la operación 642. Además, antes de realizar la operación 656, el terminal 620 puede mapear y almacenar el ID de transacción y la dirección del servidor de suministro de perfil juntos.

En la operación 658, la eUICC puede verificar el servidor de suministro de perfil basándose en la información recibida. La eUICC 630 verifica el certificado del servidor de suministro de perfil. La verificación puede ser un esquema de verificación de firma que usa un certificador CI o una clave pública del certificado CI que se almacenan en la eUICC 630. La verificación de firma puede ser verificación que usa la clave pública seleccionada usando la información incluida en el Certificado_a_usarse. Si la verificación pasa, la eUICC 630 verifica la DP1_firma recibida. La verificación puede ser una verificación de firma que usa la clave pública incluida en el certificado del servidor de suministro de perfil. Si la verificación pasa, la eUICC 620 autentica el servidor de suministro de perfil.

El terminal puede a continuación generar un par de claves de una clave pública desechable y una clave personal. El par de claves de la clave pública y clave personal se genera de manera separada en diferentes valores pares por el servidor de suministro de perfil. Cuando únicamente se intercambia la clave pública entre los valores así generados entre sí, puede compartirse una clave de sesión combinando la clave pública con la clave personal. En este caso, la clave pública se vuelve desechable, y por lo tanto una nueva clave de sesión puede compartirse cada vez que se descarga el perfil. En este caso, para transferir de manera segura la clave pública, se transfiere el valor de firma calculado usando la clave pública. Para este fin, la eUICC 630 puede realizar una firma usando la clave personal pre-almacenada en la eUICC 630, que incluye el desafío de DP recibido junto con la clave pública desechable de la eUICC 630. La firma se realiza incluyendo el desafío de DP, y por lo tanto el servidor 610 de suministro de perfil puede autenticar la eUICC 630. La firma puede incluir al menos una del ID de transacción, la dirección del servidor de suministro de perfil, la clave de instalación de perfil, la información de terminal, la información de eUICC, y el valor de código secreto de función de troceo además de lo mismo para verificar adicionalmente el servidor 610 de suministro de perfil. Por conveniencia, la firma se denomina señal_eUICC. Tras la generación de la firma, la firma puede generarse seleccionando la clave personal de la eUICC que coincide con el tipo de certificación y la información de clave de encriptación usada en el Certificado_a_usarse recibido.

En la operación 660, la eUlCC 630 puede transferir información de autenticación de eUlCC al terminal 620. La información de autenticación de eUICC puede incluir al menos una de la clave pública desechable de la eUICC, la dirección del servidor de suministro de perfil, la clave de instalación de perfil, la información de terminal, la información de eUICC, el valor de código secreto de función de troceo, la señal_eUICC, el certificado de eUICC, y el certificado de fabricante de eUICC que emite el certificado de eUICC.

Haciendo referencia a la Figura 6B, en la operación 662, el terminal 620 puede transmitir el mensaje de solicitud de perfil al servidor 630 de suministro de perfil. El mensaje de solicitud de perfil transmitido al servidor 630 de suministro

de perfil puede incluir la información de autenticación de eUICC recibida de la eUICC 630. El terminal 620 puede transferir al menos uno de un ID de transacción que es la dirección del servidor de suministro de perfil que corresponde al ID de transacción almacenado antes de realizar la operación 656, la clave pública desechable de la eUICC, la dirección del servidor de suministro de perfil, la clave de instalación de perfil, la información de terminal, la información de eUICC, el valor de código secreto de función de troceo, la señal_eUICC, el certificado de eUICC, y el certificado de fabricante de eUICC que emite el certificado de eUICC al servidor 610 de suministro de perfil.

En la operación 664, después de que se ha realizado acuse de recibo de si hay un ID de transacción válido realizando acuse de recibo del ID de transacción recibido en la operación 662, si no está presente, el servidor 610 de suministro de perfil puede devolver el código de error al terminal 620 y finalizar el procedimiento de descarga. El ID de transacción válido puede indicar que el ID de transacción se almacena en un repositorio o una memoria del servidor de suministro de perfil a consultarse, y un ejemplo de la operación del servidor de suministro de perfil que corresponde al ID de transacción puede ser el de la operación 654 que se realiza, pero se recibe en primer lugar un mensaje que corresponde a la operación 662. Sin embargo, cuando el mensaje de la operación 662 ya se ha recibido y el mensaje de la operación 662 se recibe usando el mismo ID de transacción, en algunos casos, puede no devolverse el código de error. Por ejemplo, cuando se transmite un segundo mensaje de solicitud de perfil mientras se realiza la operación 664 que va a describirse más adelante en el primer mensaje recibido en la operación 662, el código de error para el segundo mensaje de solicitud de perfil no vuelve pero el segundo mensaje puede descartarse.

Posteriormente, para la solicitud del perfil determinada como la transacción normal, el servidor 610 de suministro de perfil puede verificar la eUICC. El servidor 610 de suministro de perfil puede verificar el certificado de fabricante de eUICC. La verificación puede estar basada en un esquema de verificación de un certificado de fabricante de eUICC extrayendo en primer lugar y usando la clave pública del certificado de CI almacenado en el servidor 610 de suministro de perfil o usando directamente la clave pública almacenada. Posteriormente, el servidor 610 de suministro de perfil puede usar la clave pública del certificado extraído del certificado del fabricante para verificar el valor de firma incluido en el certificado de eUICC recibido, verificando de esta manera el certificado de eUICC. Posteriormente, el servidor de suministro de perfil puede usar la clave pública incluida en el certificado de eUICC verificado para verificar el valor señal_eUICC. En este caso, si la verificación pasa, el servidor 610 de suministro de perfil autentica la eUICC 630.

Posteriormente, el servidor 610 de suministro de perfil puede verificar si la clave de instalación de perfil AC_testigo es válida. Esto puede ser un procedimiento de realización de acuse de recibo de si la correspondiente clave de instalación de perfil está incluida en el valor almacenado en el repositorio del servidor de suministro de perfil y si hay el perfil descargable que corresponde a la clave de instalación de perfil almacenada. Además, si fuera necesario, el servidor 610 de suministro de perfil puede verificar el código secreto de función de troceo. Esto puede estar basado en un esquema de comparación de manera sencilla con el código secreto de función de troceo y un esquema de cálculo y comparación de un código secreto con nuevamente función de troceo. Posteriormente, el servidor 610 de suministro de perfil puede comparar la información de terminal, la información de eUICC, o similares, para determinar adicionalmente si puede instalarse el perfil. La información puede incluir también finalización de red accesible e información de región de memoria instalable.

Únicamente cuando la verificación pasa, el servidor 610 de suministro de perfil puede aprobar la descarga de perfil y a continuación realizar el siguiente procedimiento. Si la verificación falla, el servidor 610 de suministro de perfil devuelve un código de retorno al terminal 620 y puede finalizar el procedimiento de descarga de un perfil. En este caso, se borra el ID de transacción y el desafío de DP que se almacenan antes de la finalización del procedimiento de descarga. Si la verificación finaliza, como se describe más adelante, el servidor 610 de suministro de perfil puede generar el par de claves de una clave pública desechable del servidor de suministro de perfil y una clave secreta. La información de clave de encriptación usada para generar el par de claves asimétricas desechables necesita usar la clave de encriptación incluida en el Certificado_a_usarse recibido en la operación 654. Como se ha descrito anteriormente, el servidor 610 de suministro de perfil puede generar la clave de sesión usando la clave secreta y la clave pública desechable recibida de la eUICC. Para la generación de la clave de sesión, puede usarse adicionalmente información de certificado (CRT) e información de EID. Además, el servidor 610 de suministro de perfil puede generar DP_firma2. La DP_firma2 es un valor de firma que usa la clave personal previamente almacenada del servidor de suministro de perfil y puede ser un cálculo del valor de firma para el valor que incluye la clave pública desechable de la eUICC. Además, el servidor 610 de suministro de perfil puede usar la clave de sesión generada para generar el paquete de perfil encriptado. El paquete de perfil encriptado puede generarse por uno de los siguientes dos procedimientos.

En un primer procedimiento, se realiza encriptación usando un esquema de encriptación SCP03t con la clave de sesión generada para el paquete de perfil que no está encriptado.

En un segundo procedimiento, se realiza encriptación combinando el paquete de perfil de encriptación encriptado con una clave aleatoria previamente generada de manera aleatoria para el paquete de perfil no encriptado con una clave aleatoria de encriptación obtenida encriptando la clave aleatoria con la clave de sesión generada.

El paquete de perfil encriptado puede incluir adicionalmente la CRT que puede usarse para generar la clave de sesión de la eUICC, la clave pública desechable del servidor de suministro de perfil, y la DP_firma2 generada.

Posteriormente, en la operación 666, el servidor 610 de suministro de perfil puede transferir el paquete de perfil encriptado al terminal 620.

En la operación 668, el terminal 620 puede transmitir el paquete de perfil a la eUICC 630. El terminal 620 puede transferir datos no de encriptación en el paquete de perfil. El terminal 620 puede discriminar datos no encriptados de una pluralidad de datos encriptados en el paquete de perfil encriptado y segmentar los datos no encriptados en un tamaño en el que los datos no encriptados pueden transmitirse a la eUICC, y transferir los datos no encriptados segmentados a la eUICC 630. El procedimiento de transferencia puede ser un procedimiento de uso de ALMACENAR APDU de DATOS.

Además, la discriminación de los datos no encriptados puede estar basada en un esquema de discriminación de un valor de etiqueta incluido en el paquete de perfil encriptado. El valor de etiqueta es el primer 1 byte o 2 bytes de datos en el paquete de perfil encriptado y realiza acuse de recibo de bytes de longitud para discriminar y transferir un límite de fin de los datos no encriptados.

Los datos no encriptados pueden incluir la CRT, una clave pública de DP desechable, y un valor DP_firma2.

En la operación 670, la eUICC puede verificar la firma y generar una clave de decodificación. La eUICC 630 puede verificar la DP_firma2. Esto puede ser un esquema de verificación de firma que usa la clave pública que se ha realizado acuse de recibo previamente del certificado del servidor de suministro de perfil. Si la verificación pasa, la eUICC 630 puede generar la clave de sesión para decodificar el paquete de perfil encriptado usando la CRT recibida, el valor de clave pública desechable del servidor de suministro de perfil, el valor de EID, y el valor de clave pública personal desechable de la eUICC almacenada únicamente en la eUICC.

En la operación 672, el terminal 630 realiza acuse de recibo de datos después del límite de los datos no encriptados que se discriminan en el momento de realizar la operación 668 como los datos encriptados y cuando realiza acuse de recibo de si una etiqueta específica está presente para determinar una etiqueta que indica los datos encriptados, realiza acuse de recibo del siguiente byte de longitud para realizar acuse de recibo de un tamaño de los datos encriptados, y transfiere los datos que se ha realizado acuse de recibo que corresponden a los datos encriptados a la eUICC 630. En este caso, los datos encriptados pueden transmitirse de manera separada a la eUICC 630 usando un comando de almacenamiento de datos.

Posteriormente, en la operación 674, el terminal 610 puede realizar un procedimiento similar la operación 672 en los siguientes datos encriptados. En este caso, mediante el procedimiento de transmisión de la clave aleatoria de encriptación descrito cuando se genera el paquete encriptado por el segundo procedimiento en la operación 664, cuando la eUICC 630 recibe la clave aleatoria de encriptación, para los siguientes datos de encriptación, la eUICC 630 puede decodificar la clave aleatoria de encriptación con la clave de sesión para extraer la clave aleatoria y a continuación usar la clave aleatoria como la clave de sesión que decodifica los siguientes datos de encriptación.

Posteriormente, en la operación 676, el terminal 620 puede realizar acuse de recibo de otro valor de etiqueta y el byte de longitud que discrimina los datos de encriptación para discriminar una pluralidad de datos de encriptación y puede transferir cada uno de los datos de encriptación a la eUICC 630 usando una pluralidad de comandos de almacenamiento de datos.

La eUICC realiza la decodificación en cada uno de los datos encriptados usando la clave de sesión o la clave aleatoria decodificada, y a continuación instala el perfil en una unidad instalable usando la información de unidad instalable de perfil incluida en la misma. La información de unidad de información de unidad instalable se instala para realizar la decodificación de los siguientes datos encriptados. Si la transmisión y la decodificación de todos los datos encriptados y la instalación de toda la información de unidad instalable se completa repitiendo la operación, la eUICC 630 puede transferir el resultado correspondiente al terminal 620 y el resultado puede transferirse incluso al servidor 610 de suministro de perfil en la operación 678.

En la realización de la presente divulgación, el terminal y la eUICC se describen de manera separada, pero la eUICC puede estar incluida en o insertada en el terminal. Por lo tanto, en la realización de la presente divulgación, la operación entre el terminal y la eUICC puede analizarse también como la operación interna del terminal que incluye la eUICC.

De acuerdo con la operación como se ha descrito anteriormente, puede realizarse la autenticación y verificación para la eUICC y el servidor de suministro de perfil, la descarga del paquete de perfil, la transferencia del paquete de perfil, y la operación de instalación de perfil.

Si la operación de instalación de perfil finaliza, el terminal 610 puede transferir un comando de activación del perfil a la eUICC 630 para activar el perfil y realiza la autenticación para el sistema de comunicación móvil como en la operación 295 de la Figura 2 usando el perfil activado y a continuación si la autenticación pasa, puede usar la red de comunicación móvil.

La Figura 7 es un diagrama que ilustra un procedimiento de intercambio de un perfil de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 7, en la operación 750, se supone que un primer terminal 725 incluye la eUICC en la que está instalado el perfil donde el discriminador de perfil es ICCID1.

En la operación 755, un usuario 705 de terminal puede seleccionar el perfil (perfil donde el discriminador de perfil es el ICCID1) de un menú del primer terminal 725 para seleccionar un menú de transferencia. El menú de transferencia puede denominarse también un intercambio de dispositivo. Es decir, en la operación 755, puede introducirse un comando de intercambio de perfil y un comando de intercambio de dispositivo.

En la operación 757, el primer terminal 725 puede obtener el EID y/o información de dirección de DFP de un segundo terminal 730. Una pantalla del primer terminal 725 puede guiar un procedimiento para obtener el EID del segundo terminal 730 y la información de dirección del servidor de transferencia de información de perfil al usuario, y obtener el EID del segundo terminal y la información de dirección del servidor de transferencia de información de perfil. El procedimiento puede ser como sigue.

En un primer procedimiento, si el código de barras, el código de QR, o el código de barras bidimensional en el que el EID y/o la información de dirección del servidor de transferencia de información de perfil representada en la pantalla o el recuadro del segundo terminal 730 se explora por una cámara del primer terminal 725, la información se decodifica por el primer terminal 725 para obtener el EID y la dirección del servidor de transferencia de información de perfil que corresponde al segundo terminal 730.

En un segundo procedimiento, después de que se seleccione un procedimiento de emparejamiento de Bluetooth seleccionando la información que corresponde al segundo terminal 730 entre información de terminal de conexión de Bluetooth representada después de una conexión de comunicación de campo cercano (por ejemplo, Bluetooth) en la pantalla del primer terminal 725, el EID del segundo terminal 730 y la información de dirección del servidor de transferencia de información de perfil se transfieren del segundo terminal 730 al primer terminal 725 a través de Bluetooth.

En la operación 759, el primer terminal 725 puede transmitir un mensaje de solicitud de intercambio de dispositivo. Como se ha descrito anteriormente, si el primer terminal 725 obtiene la información en el segundo terminal 730, el primer terminal 725 puede enviar la solicitud para que el dispositivo intercambie a un sistema de BSO de MNO 710. El intercambio de dispositivo puede transferirse también por el servidor de suministro de perfil después de que se realice el procedimiento de autenticación mutua de un servidor 715 de suministro de perfil y el primer terminal 725, y puede realizarse después de que el usuario pueda realizar los procedimientos de autenticación tales como autenticación de ID/contraseña (PW), autenticación de único inicio de sesión, autenticación de huella digital, un historial de código secreto, y una entrada de la clave de instalación de perfil a través de una página de portal web proporcionada por el sistema de BSS de MNO 710.

En la operación 761, el sistema de BSS de MNO 710 puede transmitir el comando de descarga de perfil para el segundo terminal 730 al servidor 715 de suministro de perfil. Si se determina que la solicitud de intercambio de dispositivo enviada al sistema de BSS de MNO 710 es adecuada, el sistema de BSS de MNO 710 puede solicitar una instalación de perfil que corresponde a un nuevo discriminador de perfil ICCID2 para el segundo terminal 730 por el servidor 715 de suministro de perfil.

En la operación 770, el servidor 715 de suministro de perfil transfiere la información de perfil en el segundo terminal 725 al servidor 720 de transferencia de información de perfil. En la operación 775, el servidor 725 de transferencia de información de perfil transfiere la información de perfil recibida al segundo terminal 730. En la operación 780, el segundo terminal 730 solicita la descarga de perfil del servidor 715 de suministro de perfil basándose en la información de perfil recibida. En la operación 785, el segundo terminal 730 puede descargar un perfil del servidor 715 de suministro de perfil para instalar el perfil. Las operaciones 770 a 785 de la Figura 7 corresponden a las operaciones 270 a 285 de la Figura 2 y por lo tanto la operación detallada hace referencia a la descripción de la Figura 2.

En la operación 791, el servidor 715 de suministro de perfil puede notificar al BSS de MNO 710 que la instalación de perfil del segundo terminal 730 está completa.

En la operación 793, el BSS de MNO 710 puede conectar la información de perfil que corresponde al ICCID2 a información de suscripción que corresponde al perfil almacenado en el primer terminal 725 existente y en la operación 795, puede activar el correspondiente perfil. La activación puede conseguirse realizando el aprovisionamiento de la información apropiada de modo que los sistemas de comunicación móvil de MNO tales como un sistema de HLR y un sistema de AuC pueden usar el servicio de comunicación móvil usando el perfil. La información apropiada puede ser el IMSI, valor K, o similares, y si no, puede ser cambiar un valor de estado de un valor de bandera sencillo.

Además, en la operación 797, el BSS de MNO 710 puede desactivar el perfil que corresponde al ICCID1 para activar un terminal para usar un servicio. El BSS de MNO puede borrar también el perfil del primer terminal por un procedimiento similar al procedimiento de descarga de un perfil en tiempo real. Un orden de las operaciones 793 a 797 puede cambiarse y alguna de las operaciones puede omitirse, añadirse o combinarse.

La Figura 8 es un diagrama que ilustra una pantalla de un primer terminal y un segundo terminal de acuerdo con la realización de la Figura 7.

Haciendo referencia a la Figura 8, el número 810 de referencia es una pantalla de un primer terminal en la operación 750 de la Figura 7, y el número 850 de referencia es una pantalla de un segundo terminal en la operación 750 de la Figura 7. En la pantalla 810, la información en el fabricante de eUICC del primer terminal puede visualizarse en una primera región 811 de la eUICC del primer terminal. La información en el perfil instalado en el primer terminal puede visualizarse en una segunda región 813 del primer terminal. Se supone que el perfil está instalado en el primer terminal, y por lo tanto puede visualizarse la información en el perfil instalado en el primer terminal. La información en el perfil visualizado en la segunda región 813 puede seleccionarse por el usuario. La información en el fabricante de eUICC del segundo terminal puede visualizarse en una primera región 851 del segundo terminal y la información en el perfil instalado en el segundo terminal puede visualizarse en una segunda región 853 del segundo terminal. Puesto que se supone que el perfil no está instalado en el segundo terminal, la información que representa que no hay instalado perfil puede visualizarse en la segunda región 853.

Si se selecciona la información en el perfil visualizado en la segunda región 813 del primer terminal, puede visualizarse una pantalla como el número 820 de referencia en el primer terminal. Una tercera región 825 del primer terminal es una región de gestión de perfil. Una región 826 que indica el intercambio de dispositivo o el intercambio de perfil puede visualizarse en la región de gestión de perfil. Además, puede visualizarse adicionalmente una región 827 en la que está activado el perfil, una región 828 en la que está asociado el perfil, o similares. Si la entrada de usuario está presente en cada región de visualización, puede realizarse la operación correspondiente.

Si la entrada de usuario está presente en la región 826, un mensaje que indica el intercambio de dispositivo o el intercambio de perfil que corresponde a la operación 755 de la Figura 7 puede transferirse al BSS de MNO.

Posteriormente, se realizan las operaciones después de 760 de la Figura 7 y por lo tanto, el perfil puede desactivarse o borrarse en el primer terminal y el perfil puede instalarse en el segundo terminal. Como resultado, en la pantalla del primer terminal, como el número 830 de referencia, la información en el fabricante de eUICC puede visualizarse en una región 831 y la correspondiente información puede visualizarse en una región 833 debido a la desactivación o el borrado de perfil. En la pantalla del segundo terminal, como el número 860 de referencia, la información en el fabricante de eUICC puede visualizarse en una región 861 y la información en el perfil instalado puede visualizarse en una región 863.

Las Figuras 9A y 9B son diagramas que ilustran un procedimiento para cambiar información en un servidor de suministro de información de perfil de acuerdo con una realización de la presente divulgación.

En la realización de las Figuras 9A y 9B, se supone que el servidor de suministro de información de perfil es la DPF. El caso en el que un servidor de gestión de perfil realiza las siguientes operaciones se describe a continuación, pero la operación del servidor de gestión de perfil puede realizarse también por el servidor de control de perfil. El servidor de gestión de perfil puede ser un EM a modo de ejemplo.

Haciendo referencia a las Figuras 9A y 9B, el sistema de proveedor (MNO en las Figuras 9A y 9B) puede cambiar la información de DPF (es decir, que incluye la información de dirección) almacenada en la eUICC específica de manera remota. El cambio de la dirección de servidor de DPF es para considerar diversas situaciones tales como el caso de cambiar y procesar la dirección del servidor dependiendo de las normativas de un área específica cuando la dirección del servidor de DPF está fijada en el terminal. En este caso, aunque no se ilustra en los dibujos, el cambio puede controlarse únicamente por el servidor de gestión de perfil específico o el servidor de suministro de perfil específico. En este caso, la información que determina que el servidor específico puede ser posible puede almacenarse en la eUICC. La información almacenada en la eUICC puede ser una porción de la información incluida en el certificado que se almacena en el certificado del servidor. Por ejemplo, la información puede ser un nombre de sujeto, un nombre común, un identificador de sujeto, o un número de serie de certificado. El tipo de información puede ser un FQDN, un nombre de dominio, o un identificador de objeto (OID). Un procedimiento de información de DPF de cambio se describirá con referencia a las Figuras 9A y 9B.

Haciendo referencia a la Figura 9A, en la operación 941, un BSS de MNO 910 puede transferir un mensaje de solicitud de gestión remota de eUICC a un servidor 915 de gestión de perfil. En este caso, el mensaje de solicitud de gestión remota incluye un valor de tipo de gestión remota que describe el cambio de la dirección de DPF, y transfiere la información de DPF (o ID de DPF o al menos una dirección de DPF) a cambiarse. En la operación 943, el servidor 915 de gestión de perfil (o servidor de suministro de perfil o servidor de control de perfil) genera un ID de evento usado hasta que se complete el procesamiento para la correspondiente solicitud. En la operación 945, el servidor 915 de gestión de perfil transmite un valor de ID de evento al BSS de MNO 910. Es decir, se devuelve el valor de ID de evento.

Posteriormente, en la operación 947, el servidor 915 de gestión de perfil transmite un mensaje de registro de solicitud de evento, solicitud de evento de registro, al servidor 920 de transferencia de información de perfil. El servidor 915 de gestión de perfil puede transferir la información de eSIM, la dirección del servidor de gestión de perfil, y la información de ID de evento a un servidor 920 de transferencia de información de perfil. La dirección del servidor de gestión de perfil y el ID de evento pueden ser el mismo tipo que la información de instalación de perfil de la Figura 2. En la operación 949, el servidor 920 de transferencia de información de perfil puede notificar al servidor 915 de gestión de perfil de la recepción normal de la transferencia. Por ejemplo, la recepción normal de la transferencia puede notificarse por un mensaje de registro de respuesta de evento, registrar respuesta de evento. Cuando el mensaje de recepción

normal no se recibe durante un tiempo predeterminado, el servidor 915 de gestión de perfil puede realizar de nuevo la operación 947.

En la operación 951, el servidor 920 de transferencia de información de perfil transfiere la información de envío a un terminal 925. La información de envío puede ser notificación de envío. El servidor 920 de transferencia de información de perfil puede transferir un mensaje (información de envío) que indica que hay información para gestionar de manera remota el perfil en el terminal 925 al terminal 925. En la operación 953, el terminal 925 transfiere la información de eSIM al servidor 920 de transferencia de información de perfil. La información de eSIM puede ser la información en el EID de una eUICC 930 o la función de troceo que aplica información del EID. La información de eSIM puede transmitirse incluyéndose en un mensaje de solicitud de identificador de evento solicitud de ID de evento.

En la operación 955, el servidor 920 de transferencia de información de perfil transfiere un mensaje de respuesta al terminal 925. El mensaje de respuesta puede ser un mensaje de respuesta de identificador de evento respuesta de ID de evento. El terminal 925 puede recibir la dirección del servidor de gestión de perfil y el ID de evento del servidor 920 de transferencia de información de perfil. Las operaciones 951 a 953 pueden basarse en el mismo procedimiento que el procedimiento usado en la operación 275 de la Figura 2.

En la operación 957, el terminal 925 puede transferir el ID de evento al servidor 915 de gestión de perfil. El terminal 925 puede transmitir también una solicitud de evento de solicitud de evento que incluye el ID de evento al servidor 915 de gestión de perfil. La operación 957 puede incluir desafío_eUICC generado e incluido en las operaciones 644 a 650 de las Figuras 6A y 6B.

En la operación 959, el servidor 915 de gestión de perfil puede generar un primer valor de firma del servidor de gestión de perfil. El primer valor de firma es una firma que incluye el desafío_eUICC. El primer valor de firma puede ser testigo de EM 1.

En la operación 961, el servidor 915 de gestión de perfil transfiere el mensaje de respuesta de evento, respuesta de evento, al terminal 925. El servidor 915 de gestión de perfil puede generar el primer valor de firma y desafío_SR y transferir el mensaje de respuesta de evento que incluye el primer valor de firma y el desafío_SR al terminal 925.

En la operación 963, el terminal 925 puede transferir el primer valor de firma SR_firma1 del servidor de gestión de perfil, un valor de tipo de evento que representa nueva información de dirección (por ejemplo, información de dirección de DPF) del servidor de transferencia de información de perfil, y un valor desafío_SR a la eUICC 930. El terminal 925 puede transferir la información a la eUICC 930 mientras que incluye la información en un mensaje de solicitud de verificación obtener solicitud de datos de autenticación.

Haciendo referencia a la Figura 9B, en la operación 965, el terminal 925 puede verificar la SR_firma1. La eUICC del terminal 925 puede verificar la SR_firma1. El procedimiento de verificación puede ser el mismo que o similar al procedimiento de firma de la operación 658 de las Figuras 6A y 6B.

La eUICC 930 puede generar la eUICC_firma1. La eUICC_firma1 es el valor de firma y puede ser uno firmado que incluye el valor desafío_SR.

En la operación 967, la eUICC 930 puede transferir un mensaje de respuesta de verificación, obtener respuesta de datos de autenticación, al terminal 925. La eUICC 930 a continuación devuelve al terminal 925, que incluye el valor de firma eUICC_firma1 o testigo de eUICC.

En la operación 969, el terminal 925 solicita la gestión de eUICC del servidor 915 de gestión de perfil, que incluye el valor de firma eUICC_firma1. Por ejemplo, el terminal 925 puede transmitir un mensaje de solicitud de gestión, solicitud de gestión de eUICC.

En la operación 971, el servidor 915 de gestión de perfil puede verificar el valor de firma eUICC_firma1. El procedimiento de verificación de una firma del servidor puede ser el mismo que o similar a la operación 664 de las Figuras 6A y 6B.

El servidor 915 de gestión de perfil puede generar la dirección de información de evento que cambia la DPF y la SR_firma2 en la que se firma el valor.

En la operación 973, el servidor 915 de gestión de perfil puede transmitir un mensaje de respuesta de gestión, respuesta de gestión de eUICC, al terminal 925. El mensaje de respuesta de gestión puede generar la información de evento que cambia la dirección de DPF y la SR_firma2 en la que se firma el valor.

En la operación 975, el terminal 925 puede realizar acuse de recibo adicionalmente de un consentimiento de usuario. El procedimiento puede ser la operación 975 antes de la operación 953, antes de la operación 963, y después de la operación 967. La operación 975 puede ser una operación opcional.

En la operación 977, el terminal 925 puede transferir la información recibida por el servidor 915 de gestión de perfil a la eUICC 930. El terminal puede transferir un mensaje de solicitud de gestión, solicitud de gestión de eUICC, que incluye la información recibida en la operación 973 del servidor 915 de gestión de perfil a la eUICC 930.

En la operación 979, la eUICC 930 puede verificar la información SR_firma2 incluida en la información recibida. Mediante la verificación, puede verificarse la firma que incluye los datos recibidos, los datos conocidos por la eUICC 930, y el ID de evento.

En la operación 981, si la verificación pasa, la eUICC 930 puede actualizar la información de DPF usando la información recibida y a continuación transferir el resultado procesado, resultado de evento, al terminal 925. La eUICC puede transmitir un mensaje de respuesta de gestión respuesta de gestión de eUICC que incluye el resultado procesado al terminal 925.

En la operación 983, el terminal 925 puede notificar al servidor 915 de gestión de perfil del correspondiente resultado. Por ejemplo, un mensaje notificar solicitud de resultado que incluye el resultado procesado puede transmitirse al servidor 915 de gestión de perfil.

En la operación 985, el servidor 915 de gestión de perfil puede transferir también el correspondiente resultado recibido del terminal 925 al BSS de MNO 910. Además, el servidor 915 de gestión de perfil puede recibir el mensaje de respuesta a la recepción del resultado procesado del BSS de MNO 910.

Después de que finaliza el procesamiento, en la operación 987, el servidor 915 de gestión de perfil puede borrar la solicitud de transferencia de información registrada en el servidor 920 de transferencia de información de perfil. Por ejemplo, el servidor 915 de gestión de perfil puede transmitir un mensaje de solicitud de borrado, borrar solicitud de evento. El servidor 920 de transferencia de información de perfil puede transmitir un mensaje de respuesta de borrado, respuesta de evento de borrado, al servidor 915 de gestión de perfil.

Como se ha descrito anteriormente, incluso aunque pase el procedimiento de autenticación mutua, se ha de observar que la eUICC puede recibir y procesar únicamente la solicitud a través del servidor de gestión de perfil específico o el servidor de control de perfil mediante el establecimiento de información de servidor adicional.

Además, el siguiente control de remoto adicional puede realizarse mediante un mecanismo similar a las Figuras 9A y 9B.

activar perfil remoto;
desactivar perfil remoto;
borrado de perfil remoto;
obtener registro de perfil;
actualizar registro de perfil;
obtener regla de política de eUICC;
actualizar regla de política de eUICC; y
resetear memoria de eUICC.

El control remoto puede realizarse por el mismo procedimiento de control que las Figuras 9A y 9B. En este caso, un tipo de evento del mensaje de respuesta de evento transmisión de la operación 961 puede cambiarse de acuerdo con una clase de controles remotos. En la operación 961, el tipo de evento que indica que se actualiza la información de DPF se describe como un ejemplo. Además, en la respuesta 973 de mensaje de solicitud de gestión, puede transferirse información adicional que coincide con el tipo de evento. La descripción de las Figuras 9A y 9B se refiere al control remoto de actualización de la información de DPF, y por lo tanto se incluye la información de DPF. En el caso del control que indica la actualización de regla de política entre los ejemplos de control, la regla de política puede incluirse en el caso de la respuesta 973 de mensaje de solicitud de gestión.

La activación del perfil remoto indica que el perfil instalado en la eUICC del terminal específico se activa de manera remota (en otras palabras, sistema de soporte empresarial de una operadora móvil). Si el perfil está activado en la eUICC, el terminal puede usar la información almacenada en el perfil para acceder a la red de la operadora móvil, recibiendo de esta manera un servicio.

La desactivación de perfil remoto indica que el perfil instalado en la eUICC del terminal específico se desactiva de manera remota. El terminal puede usar el correspondiente perfil justo antes o después de desactivar el perfil para bloquear un acceso a la red de comunicación móvil que ya se ha accedido. Si está desactivado el perfil específico del terminal, la eUICC puede activar automáticamente otros perfiles.

El borrado de perfil remoto puede indicar que el perfil específico se borra de manera remota. Cuando el borrado de perfil remoto intenta borrar el perfil activado actualmente, el terminal puede no procesar el borrado de perfil. Además, cuando el borrado de perfil remoto intenta borrar el perfil actualmente activado, el terminal desactiva en primer lugar el correspondiente perfil y a continuación procesa el correspondiente borrado del perfil.

Además, cuando el perfil que es un objeto del borrado de perfil remoto es un perfil único que puede acceder al servicio de comunicación móvil entre los perfiles instalados en la eUICC, el terminal puede no procesar el borrado de perfil.

La adquisición de la información de perfil es un control para permitir que el servidor remoto obtenga la información en todos o algunos de los perfiles instalados en la eUICC. La información puede incluir al menos uno del discriminador

de perfil que discrimina el perfil específico, el ICCID, el nombre de perfil, la información de proveedor, y el discriminador de eUICC.

La actualización de información de perfil es un control para permitir que el servidor remoto obtenga la información específica en todos o algunos de los perfiles instalados en la eUICC. La información puede incluir al menos uno del discriminador de perfil que discrimina el perfil específico, el ICCID, el nombre de perfil, la información de proveedor, y el discriminador de eUICC.

La adquisición de la regla de política de eUICC es un comando de control para permitir que el servidor obtenga la regla de política de eUICC establecida en la eUICC actual. El comando de control puede ser un discriminador que indica que el tipo de evento obtiene la regla de política de eUICC. La regla de política indica una política para la operación específica de la eUICC. Un ejemplo de la regla de política puede ser como sigue.

La instalación del perfil específico puede estar limitada.

El control remoto de perfil del servidor específico puede estar limitado.

La instalación del perfil del proveedor específico puede estar limitada.

El borrado de perfil específico puede estar limitado.

La activación o desactivación de perfil específico pueden estar limitadas.

La actualización de regla de política de eUICC puede usarse cuando se añaden o eliminan las reglas de política como se han enumerado anteriormente.

El reseteo de información de eUICC es un control remoto de eliminación de alguno o todos los perfiles instalados.

La Figura 10 es un diagrama de bloques que ilustra un servidor de suministro de perfil de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 10, un servidor 1000 de suministro de perfil puede incluir un transceptor 1010 para recibir una señal de otros nodos o transmitir una señal a otros nodos, un controlador 1030 para controlar una operación global del servidor de suministro de perfil, y un almacenamiento 1020 para almacenar un perfil e información relacionada con el perfil.

De acuerdo con la realización de la presente divulgación, el controlador 1030 puede realizar un control para recibir una solicitud de preparación de perfil de un sistema activador, transmitir información de perfil a un servidor de transferencia de información de perfil, basándose en la solicitud de preparación de perfil, recibir una solicitud de descarga de perfil de un aparato electrónico, y transmitir un perfil instalable en una UICC del aparato electrónico al aparato electrónico. La información de perfil puede usarse para solicitar la descarga de perfil del aparato electrónico.

La información de perfil puede incluir la información en la UICC del aparato electrónico y la información de dirección del servidor de suministro de perfil que proporciona el perfil para la UICC.

La solicitud de preparación de perfil puede incluir al menos una de un discriminador de UICC, información en el servidor de transferencia de información de perfil, un discriminador de perfil, una solicitud de tipo de perfil, una clave de instalación de perfil, información sobre el aparato electrónico, e información de UICC.

Además, el controlador 1030 puede realizar un control para recibir información aleatoria en la UICC del aparato electrónico, transmitir información de firma que corresponde a la información aleatoria y un certificado del servidor de suministro de perfil al aparato electrónico, recibir datos de generación de clave de encriptación del aparato electrónico si una verificación para la información de firma y el certificado tiene éxito, y transmitir un perfil encriptado con una clave de encriptación generada basándose en los datos de generación de clave de encriptación al aparato electrónico.

Además, de acuerdo con la realización de la presente divulgación, el controlador 1030 puede controlar una operación de transmisión de información de perfil, una operación de descarga de un perfil, un procedimiento de autenticación y verificación para descargar un perfil, una operación de intercambio de un perfil, una operación de cambio de información en el servidor de transferencia de información de perfil, o similares.

Además, la operación del servidor 1000 de suministro de perfil y el controlador 1030 no está limitada a la descripción de la Figura 10 y por lo tanto, puede realizarse la operación y función del servidor de suministro de perfil de acuerdo con la realización de la presente divulgación descrita con referencia a las Figuras 1 a 9B.

De acuerdo con la realización de la presente divulgación, el servidor de suministro de perfil puede incluir el servidor de gestión de perfil o el servidor de control de perfil o realizar las funciones de los mismos. La configuración del servidor de suministro de perfil y el servidor de gestión de perfil puede corresponder a la configuración del servidor de suministro de perfil.

La Figura 11 es un diagrama de bloques que ilustra un servidor de transferencia de información de perfil de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 11, un servidor 1100 de transferencia de información de perfil puede incluir un transceptor 1110 para recibir una señal de otros nodos o transmitir una señal a otros nodos, un controlador 1130 para controlar una operación global del servidor 1100 de transferencia de información de perfil, y un almacenamiento 1120 para registrar y almacenar información de perfil.

De acuerdo con la realización de la presente divulgación, el controlador 1130 puede realizar un control para recibir la información de perfil del servidor de suministro de perfil, registrar la información de perfil, y transferir la información de perfil al aparato electrónico que corresponde a la información de perfil.

En este caso, la información de perfil puede usarse para permitir que el aparato electrónico descargue un perfil instalable en una UICC del aparato electrónico del servidor de suministro de perfil.

La información de perfil puede incluir la información en la UICC del aparato electrónico y la información de dirección del servidor de suministro de perfil que proporciona el perfil para la UICC.

Además, el controlador 1130 puede realizar un control para realizar una de una operación de transferencia de la información de perfil que corresponde a una solicitud de descarga de perfil del aparato electrónico y una operación de transferencia de la información de perfil usando notificación de envío, si la información de identificación del aparato electrónico se registra en el servidor de transferencia de información de perfil con antelación y a continuación se recibe la información de perfil en el aparato electrónico por el servidor de transferencia de información de perfil.

Además, de acuerdo con la realización de la presente divulgación, el controlador 1130 puede controlar una operación de registro de transmisión de información de perfil, una operación de envío, una operación de descarga de un perfil, un procedimiento de autenticación y verificación para descargar un perfil, una operación de intercambio de un perfil, una operación de cambio de información en el servidor de transferencia de información de perfil, o similares.

Además, la operación del servidor 1100 de transferencia de información de perfil y el controlador 1130 no está limitada a la descripción de la Figura 11 y por lo tanto, puede realizarse la operación y función del servidor de transferencia de información de perfil de acuerdo con la realización de la presente divulgación descrita con referencia a las Figuras 1 a 9B.

La Figura 12 es un diagrama que ilustra un aparato electrónico de acuerdo con una realización de la presente divulgación.

Haciendo referencia a la Figura 12, un aparato 1200 electrónico puede incluir un transceptor 1210 para recibir una señal de otros nodos y transmitir una señal a otros nodos y un controlador 1230 para controlar una operación global del aparato 1200 electrónico. Además, el aparato 1200 electrónico puede incluir una UICC 1220 para descargar el perfil del servidor de suministro de perfil e instalar el perfil descargado. La UICC puede ser la eUICC. El controlador 1230 puede controlar una operación de la UICC 1220. El aparato electrónico 1220 puede ser el terminal. Una UICC 1220 puede incluir un procesador o un controlador para instalar un perfil o puede tener aplicaciones instaladas en la misma.

De acuerdo con la realización de la presente divulgación, el controlador 1230 puede realizar un control para recibir información de perfil de un servidor de transferencia de información de perfil, transmitir una solicitud de perfil a un servidor de suministro de perfil identificado basándose en la información de perfil, y recibir un perfil instalable en la UICC del aparato electrónico del servidor de suministro de perfil.

En este caso, la información de perfil puede incluir la información en la UICC del aparato electrónico y la información de dirección del servidor de suministro de perfil que proporciona el perfil para la UICC.

Además, el controlador 1230 puede realizar un control para recibir la información de perfil usando una de una operación de recepción de la información de perfil que corresponde a una solicitud de descarga de perfil del aparato electrónico y una operación de recepción de la información de perfil usando notificación de envío, si la información de identificación del aparato electrónico se registra en el servidor de transferencia de información de perfil con antelación y a continuación la información de perfil en el aparato electrónico se recibe por el servidor de transferencia de información de perfil.

Además, el controlador 1230 puede realizar un control para transmitir información aleatoria en la UICC del aparato electrónico al servidor de suministro de perfil, recibir información de firma que corresponde a la información aleatoria y un certificado del servidor de suministro de perfil, verificar el servidor de suministro de perfil basándose en la información de firma y la firma, transferir datos de generación de clave de encriptación al servidor de suministro de perfil, si la verificación tiene éxito, y recibir un perfil encriptado con una clave de encriptación generada basándose en los datos de generación de clave de encriptación.

Además, de acuerdo con la realización de la presente divulgación, el controlador 1230 puede controlar un registro y

solicitar operación de recepción de información de perfil, una operación para descargar un perfil, un procedimiento de autenticación y verificación para descargar un perfil, una operación de intercambio de un perfil, una operación de cambio de información en el servidor de transferencia de información de perfil, o similares.

La operación y función del aparato 1200 electrónico no está limitada a la descripción de la Figura 12. El aparato 1200 electrónico y el controlador 1230 pueden controlar la operación del aparato electrónico y el terminal (o eUICC del terminal) de acuerdo con la realización de la presente divulgación descrita con referencia a las Figuras 1 a 9B. Además, el procesador de la UICC puede controlar la operación de la eUICC o la UICC de acuerdo con la realización de la presente divulgación descrita con referencia a las Figuras 1 a 12.

El controlador 1230 puede controlar la operación del procesador de la eUICC 1220 y puede implementarse para realizar la operación del procesador.

En las realizaciones detalladas de la presente divulgación, los componentes incluidos en la presente divulgación se representan por un número singular o un número plural de acuerdo con la realización detallada como se ha descrito anteriormente. Sin embargo, las expresiones del número singular o el número plural se seleccionan para cumplir las situaciones propuestas por conveniencia de explicación y la presente divulgación no está limitada a un único componente o a los diversos componentes e incluso aunque los componentes se representen en plural, el componente puede estar configurado en un número singular o incluso aunque los componentes se representen en un número singular, el componente puede estar configurado en plural.

De acuerdo con las realizaciones de la presente divulgación, es posible proporcionar el aparato y procedimiento para descargar e instalar un perfil en una comunicación para una conexión de comunicación. Además, es posible proporcionar el aparato para transmitir un perfil para activar el aparato anterior para descargar el perfil y el aparato para transmitir información de perfil y el procedimiento de operación del mismo.

De acuerdo con las realizaciones de la presente divulgación, es posible instalar automáticamente el perfil que usa el servicio de comunicación en el terminal de comunicación móvil en el sistema de comunicación inalámbrica.

Los procedimientos de acuerdo con diversas realizaciones pueden realizarse en un formato de comando de programa (o instrucción) que puede ejecutarse usando diversos medios informáticos, para registrarse en un medio legible por ordenador no transitorio. En el presente documento, el medio legible por ordenador puede incluir independientemente un comando de programa (o instrucción), fichero de datos, estructura de datos, y así sucesivamente, o puede incluir una combinación de los mismos. Por ejemplo, el medio legible por ordenador puede almacenarse en un dispositivo de almacenamiento volátil o no volátil tal como una ROM, una memoria tal como una RAM, un chip de memoria, o un circuito integrado, o un medio de almacenamiento que puede grabarse óptica o magnéticamente y leerse por una máquina (por ejemplo, un ordenador) tal como un disco compacto (CD), un DVD, un disco magnético, o una cinta magnética, independientemente de la posibilidad de borrado o posibilidad de re-grabación. Se entenderá por un experto en la materia que una memoria que puede incluirse en un terminal móvil es un medio de almacenamiento que puede leerse por una máquina para almacenar programas o un programa que incluye instrucciones de acuerdo con diversas realizaciones. El comando de programa grabado en el medio legible por ordenador puede estar diseñado y construido específicamente para la presente divulgación o puede ser conocido para y usable por un experto en la materia en un campo del software informático.

Aunque se ha mostrado y descrito la presente divulgación con referencia a diversas realizaciones de la misma, se entenderá por los expertos en la materia que pueden hacerse en la misma diversos cambios en forma y detalle sin alejarse del alcance de la presente divulgación según se define por las reivindicaciones adjuntas y sus equivalentes.

REIVINDICACIONES

1. Un procedimiento de instalación de un perfil por un aparato electrónico en un sistema de comunicación inalámbrica, comprendiendo el procedimiento:

transmitir, a un primer servidor, un primer mensaje para solicitar información asociada con un perfil (260);
recibir, del primer servidor, un segundo mensaje que incluye información asociada con una dirección de un segundo servidor y un identificador para un evento (275);
transmitir, al segundo servidor, un tercer mensaje para solicitar un perfil basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento (280);
recibir, del segundo servidor, el perfil (285); e
instalar el perfil en una tarjeta de circuito integrado universal, UICC, del aparato (290) electrónico.

2. El procedimiento de la reivindicación 1, en el que una dirección del primer servidor está preconfigurada para el aparato electrónico.

3. El procedimiento de la reivindicación 1, en el que la recepción del perfil (285) comprende:

transmitir información aleatoria en la UICC del aparato electrónico al segundo servidor;
recibir información de firma que corresponde a la información aleatoria y un certificado del segundo servidor;
verificar el segundo servidor basándose en la información de firma y el certificado;
transmitir, si la verificación tiene éxito, datos de generación de clave de encriptación al segundo servidor; y
recibir el perfil encriptado con una clave de encriptación generada basándose en los datos de generación de clave de encriptación.

4. Un aparato (1200) electrónico para instalar un perfil en un sistema de comunicación inalámbrica, comprendiendo el aparato electrónico:

un transceptor (1210); y
un controlador (1230) acoplado con el transceptor y configurado para controlar para:

transmitir, a un primer servidor, un primer mensaje para solicitar información asociada con un perfil,
recibir, del primer servidor, un segundo mensaje que incluye información asociada con una dirección de un segundo servidor y un identificador para un evento,
transmitir, al segundo servidor, un tercer mensaje para solicitar un perfil basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento,
recibir, del segundo servidor, el perfil, e
instalar el perfil en una tarjeta de circuito integrado universal, UICC (1220), del aparato electrónico.

5. El aparato (1200) electrónico de la reivindicación 4, en el que una dirección del primer servidor está preconfigurada para el aparato electrónico.

6. El aparato (1200) electrónico de la reivindicación 4, en el que el controlador (1230) está configurado adicionalmente para:

transmitir información aleatoria en la UICC (1220) del aparato electrónico al segundo servidor, recibir información de firma que corresponde a la información aleatoria y un certificado del segundo servidor,
verificar el segundo servidor basándose en la información de firma y el certificado,
transmitir datos de generación de clave de encriptación al segundo servidor si la verificación tiene éxito, y recibir un perfil encriptado con una clave de encriptación generada basándose en los datos de generación de clave de encriptación.

7. Un procedimiento por un primer servidor en un sistema de comunicación inalámbrica, comprendiendo el procedimiento:

recibir, de un segundo servidor, un primer mensaje que incluye información en un perfil para un aparato (270) electrónico;
recibir, del aparato electrónico, un segundo mensaje para solicitar información asociada con un perfil; y
transmitir, al aparato electrónico, un tercer mensaje que incluye información asociada con una dirección del segundo servidor y un identificador para un evento,
en el que un mensaje para solicitar un perfil se transmite del aparato electrónico al segundo servidor basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento, y en el que el perfil se transmite del segundo servidor al aparato electrónico y se instala en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

8. El procedimiento de la reivindicación 7, en el que la información en el perfil incluye un identificador de una tarjeta de circuito integrado universal, UICC, del aparato electrónico, la información asociada con la dirección del segundo servidor y el identificador para el evento.

9. El procedimiento de la reivindicación 8, el procedimiento comprende adicionalmente:

registrar la información en el perfil incluido en el primer mensaje; e
identificar el aparato electrónico usando el identificador de la UICC del aparato electrónico, cuando se recibe el segundo mensaje.

10. Un primer servidor (1100) en un sistema de comunicación inalámbrica, comprendiendo el primer servidor:

un transceptor (1110); y
un controlador (1130) acoplado con el transceptor y configurado para controlar para:

recibir, de un segundo servidor, un primer mensaje que incluye información en un perfil para un aparato electrónico,
recibir, del aparato electrónico, un segundo mensaje para solicitar información asociada con un perfil, y
transmitir, al aparato electrónico, un tercer mensaje que incluye información asociada con una dirección del segundo servidor y un identificador para un evento,

en el que un mensaje para solicitar un perfil se transmite del aparato electrónico al segundo servidor basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento, y en el que el perfil se transmite del segundo servidor al aparato electrónico y se instala en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

11. El primer servidor (1100) de la reivindicación 10, en el que la información en el perfil incluye un identificador de una tarjeta de circuito integrado universal, UICC, del aparato electrónico, la información asociada con la dirección del segundo servidor y el identificador para el evento.

12. El primer servidor (1100) de la reivindicación 11, en el que el controlador (1130) está configurado adicionalmente para:

registrar la información en el perfil incluido en el primer mensaje; e
identificar el aparato electrónico usando el identificador de la UICC del aparato electrónico, cuando se recibe el segundo mensaje.

13. Un procedimiento por un segundo servidor en un sistema de comunicación inalámbrica, comprendiendo el procedimiento:

transmitir, a un primer servidor, un primer mensaje que incluye información asociada con una dirección del segundo servidor y un identificador para un evento del aparato (270) electrónico;
recibir, del aparato electrónico, un segundo mensaje para solicitar un perfil basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento (280); y transmitir, al aparato electrónico, el perfil a instalarse en una tarjeta de circuito integrado universal, UICC, del aparato (285) electrónico.

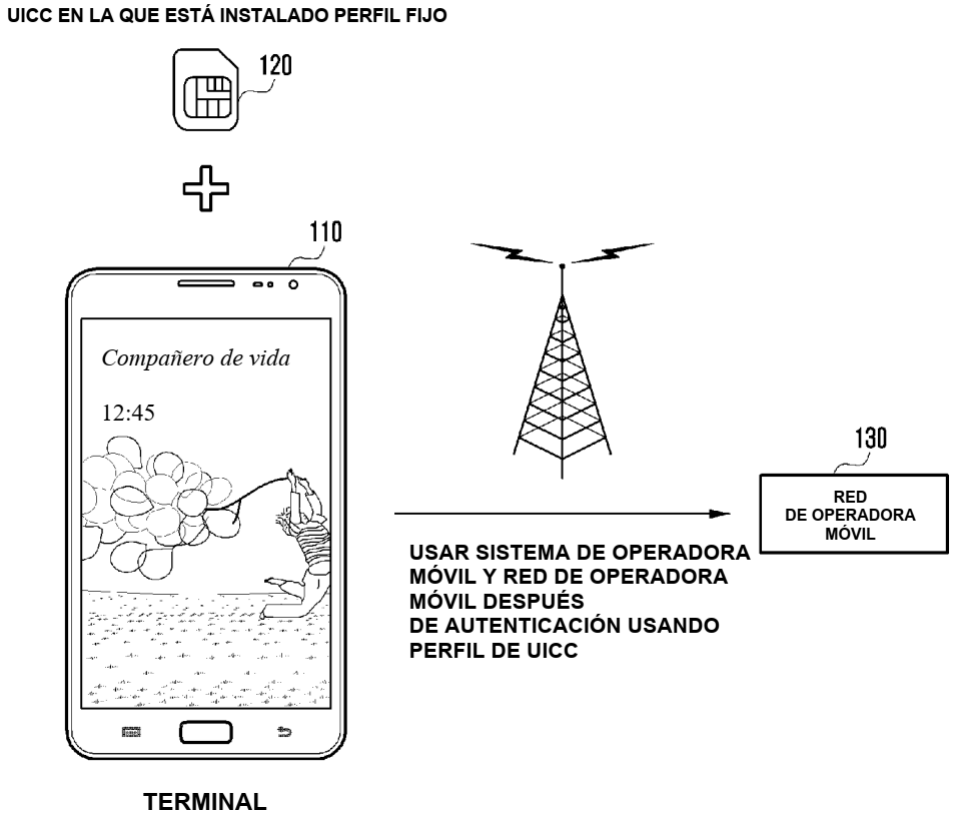
14. Un segundo servidor (1000) en un sistema de comunicación inalámbrica, comprendiendo el segundo servidor:

un transceptor (1010); y
un controlador (1030) acoplado con el transceptor y configurado para controlar para:

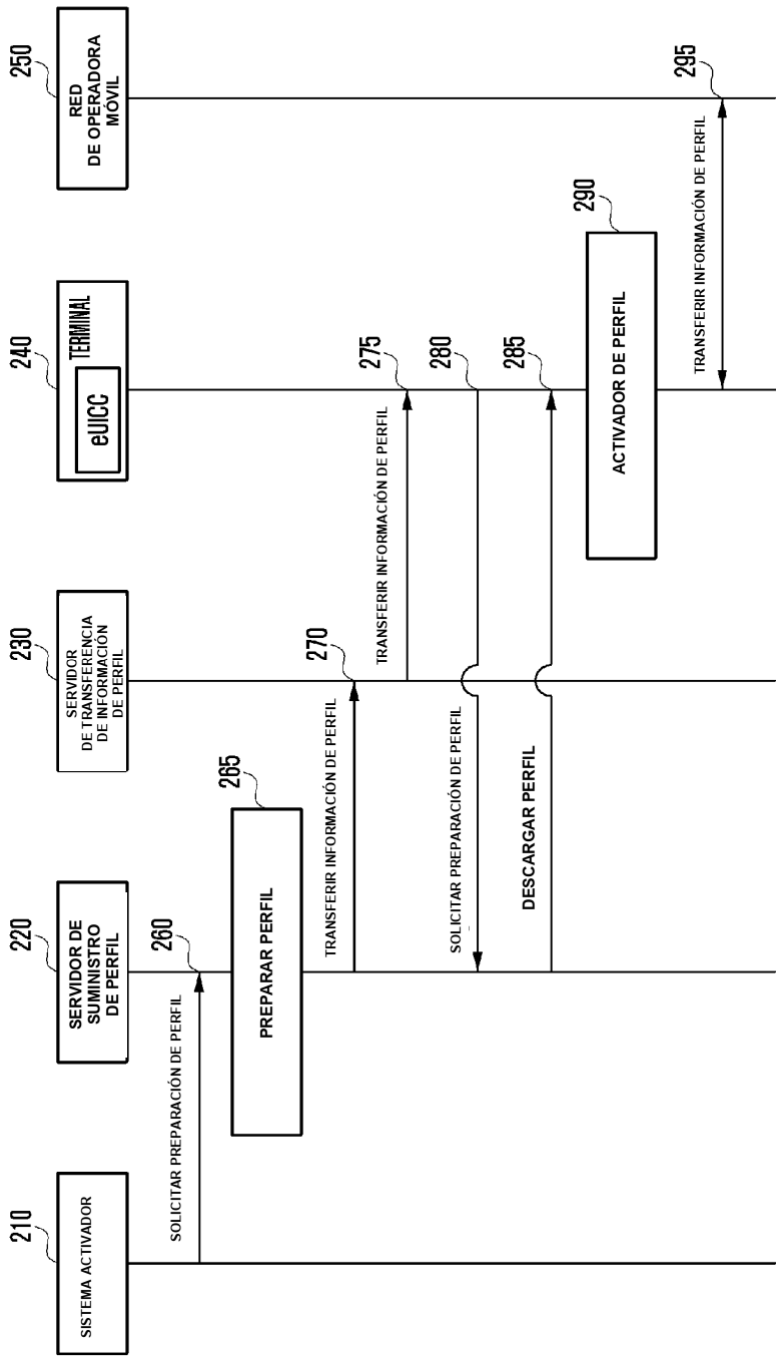
transmitir, a un primer servidor, un primer mensaje que incluye información asociada con una dirección del segundo servidor y un identificador para un evento del aparato electrónico,
recibir, del aparato electrónico, un segundo mensaje para solicitar un perfil basándose en la información asociada con la dirección del segundo servidor, correspondiendo el perfil al identificador para el evento, y
transmitir, al aparato electrónico, el perfil a instalarse en una tarjeta de circuito integrado universal, UICC, del aparato electrónico.

15. En cualquiera de las reivindicaciones 13 o 14, en las que el primer mensaje se entrega al aparato electrónico por el primer servidor e incluye un identificador de la UICC del aparato electrónico, y
en el que una dirección del primer servidor está preconfigurada para el aparato electrónico.

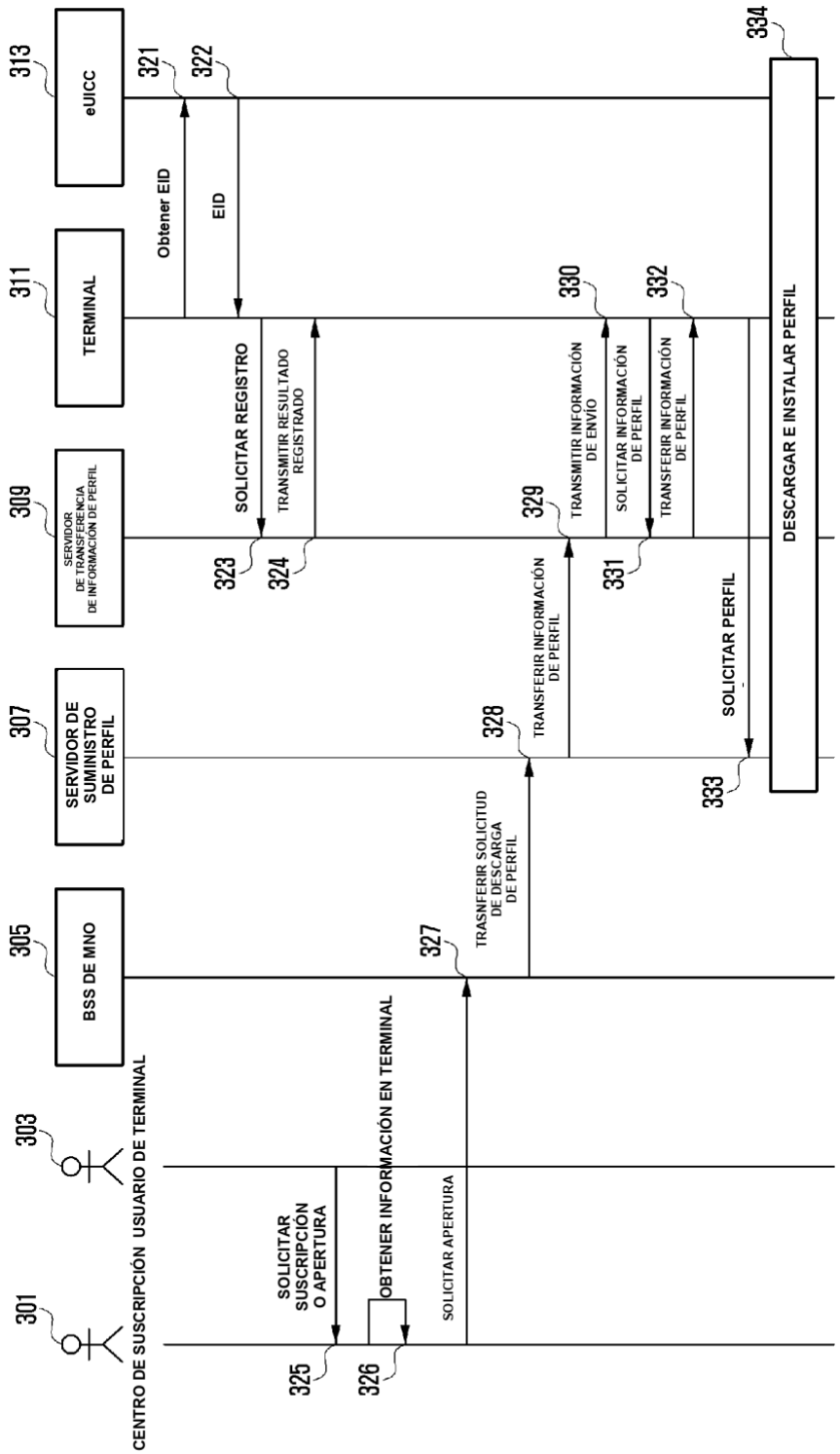
[Fig. 1]


UICC EN LA QUE ESTÁ INSTALADO PERFIL FIJO
120
110
Compañero de vida
12:45
TERMINAL
130
RED
DE OPERADORA
MÓVIL
USAR SISTEMA DE OPERADORA
MÓVIL Y RED DE OPERADORA
MÓVIL DESPUÉS
DE AUTENTICACIÓN USANDO
PERFIL DE UICC

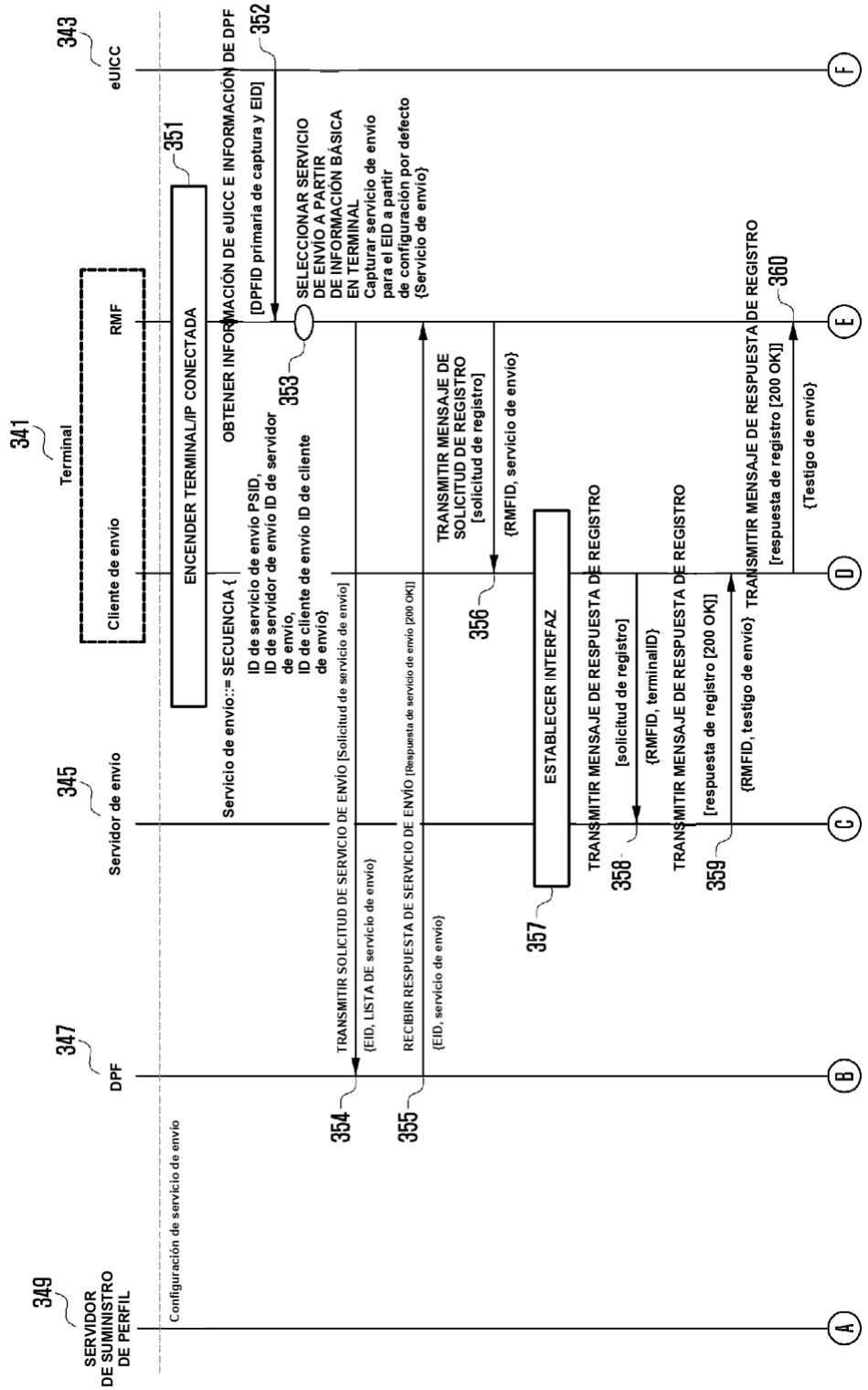
[Fig. 2]


250
RED DE OPERADORA MOVIL
240
TERMINAL
eUICC
230
SERVIDOR DE TRANSFERENCIA DE INFORMACIÓN DE PERFIL
220
SERVIDOR DE SUMINISTRO DE PERFIL
210
SISTEMA ACTIVADOR
295
TRANSFERIR INFORMACIÓN DE PERFIL
290
ACTIVADOR DE PERFIL
275
TRANSFERIR INFORMACIÓN DE PERFIL
280
SOLICITAR PREPARACIÓN DE PERFIL
285
DESCARGAR PERFIL
270
TRANSFERIR INFORMACIÓN DE PERFIL
265
PREPARAR PERFIL
260
SOLICITAR PREPARACIÓN DE PERFIL

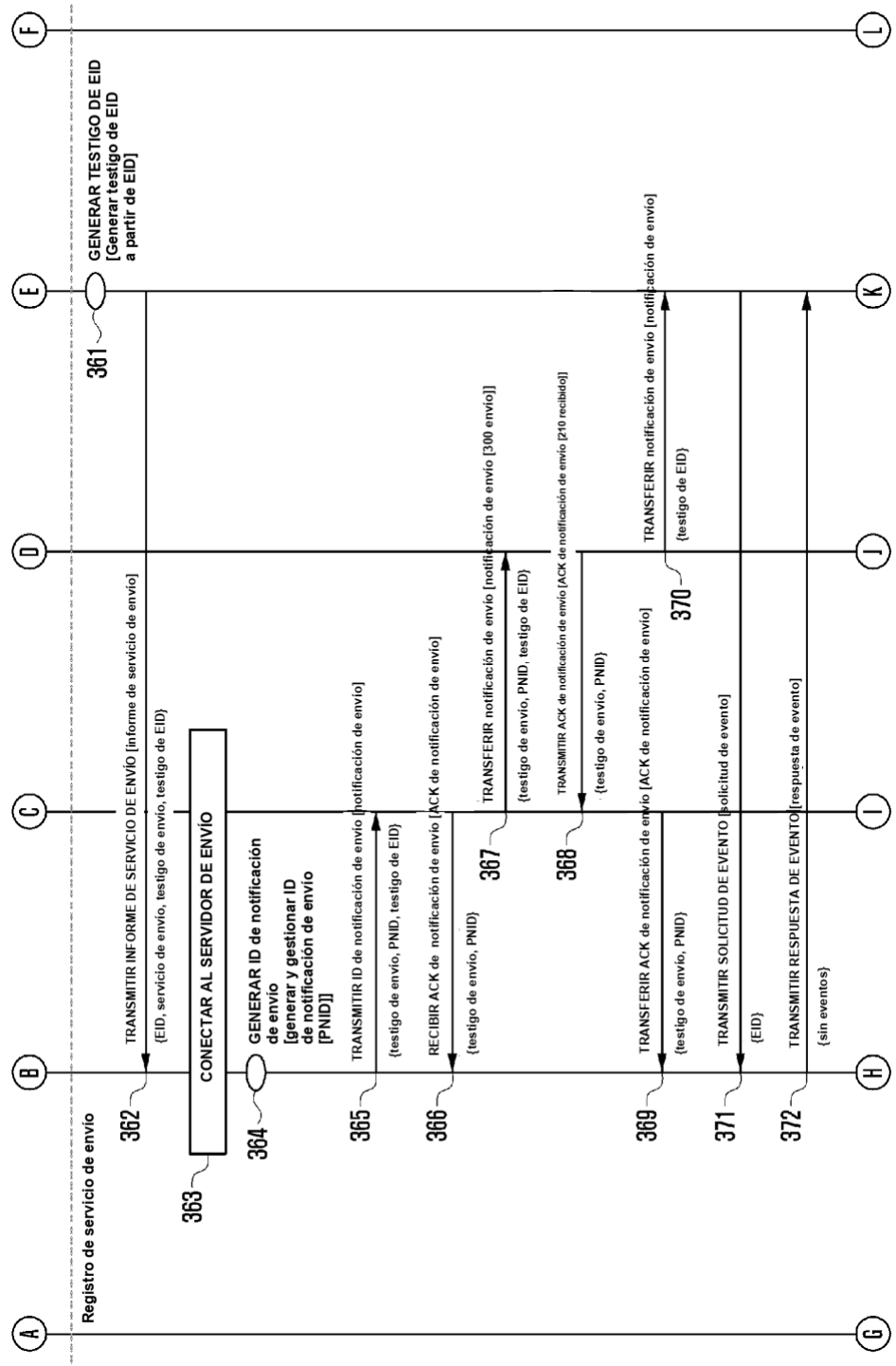
[Fig. 3a]


313
eUICC
321
322
334
Obtener EID
EID
311
TERMINAL
330
332
309
SERVIDOR DE TRANSFERENCIA DE INFORMACIÓN DE PERFIL
SOLICITAR REGISTRO
TRANSMITIR RESULTADO REGISTRADO
329
TRANSMITIR INFORMACIÓN DE ENVÍO
SOLICITAR INFORMACIÓN DE PERFIL
TRANSFERIR INFORMACIÓN DE PERFIL
DESCARGAR E INSTALAR PERFIL
323
324
331
307
SERVIDOR DE SUMINISTRO DE PERFIL
328
TRANSFERIR INFORMACIÓN DE PERFIL
SOLICITAR PERFIL
333
305
BSS DE MNO
327
TRASNFERIR SOLICITUD DE DESCARGA DE PERFIL
303
SOLICITAR SUSCRIPCIÓN O APERTURA
OBTENER INFORMACIÓN EN TERMINAL
SOLICITAR APERTURA
301
CENTRO DE SUSCRIPCIÓN
USUARIO DE TERMINAL
325
326

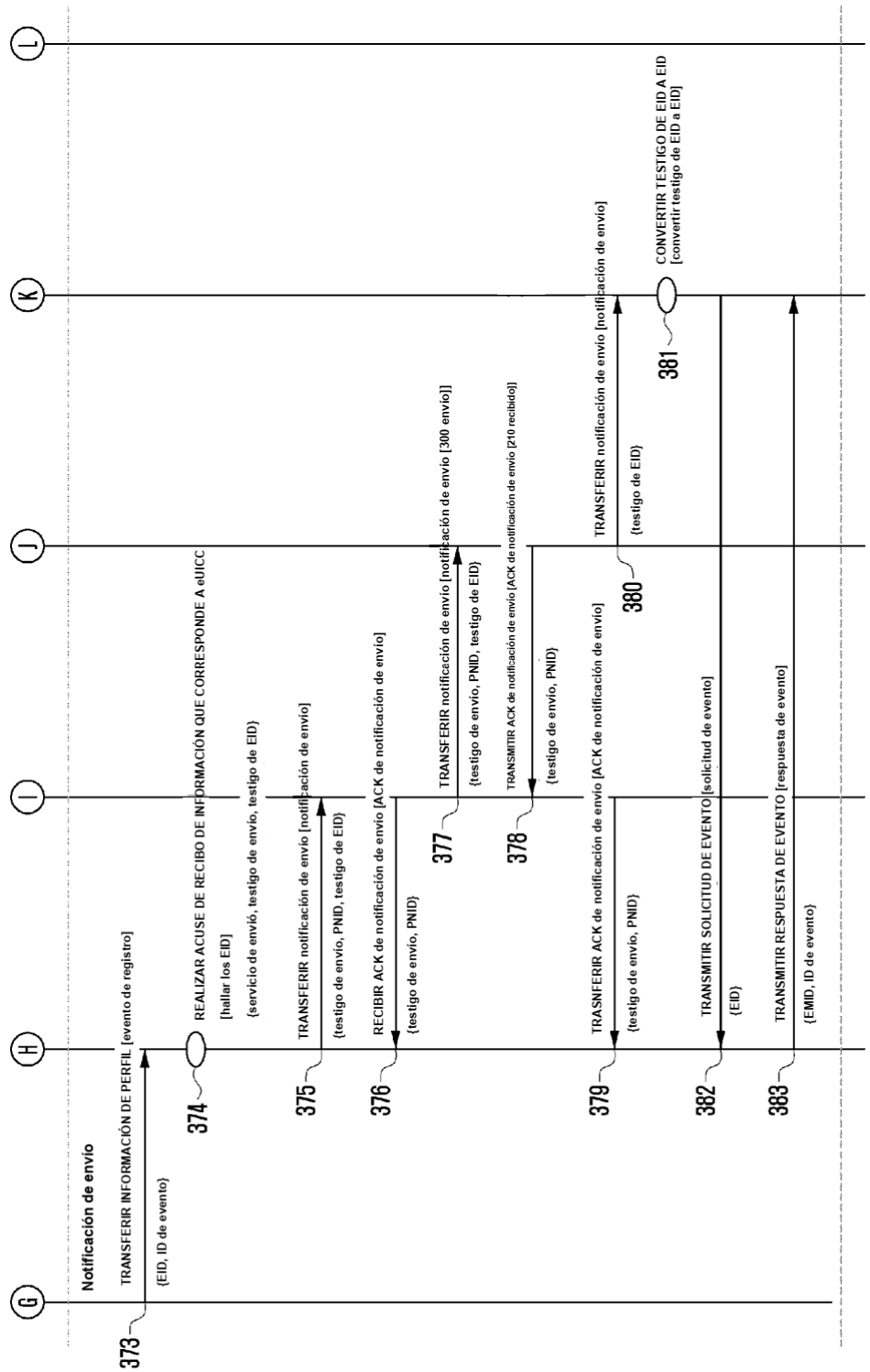
[Fig. 3b]


343
eUICC
352
[DPFID primaria de captura y EID]
351
ENCENDER TERMINAL/IP CONECTADA
OBTENER INFORMACIÓN DE eUICC E INFORMACIÓN DE DPF
SELECCIONAR SERVICIO DE ENVÍO A PARTIR DE INFORMACIÓN BÁSICA EN TERMINAL
Capturar servicio de envío para el EID a partir de configuración por defecto {Servicio de envío}
341
Terminal
Cliente de envío
RMF
Servicio de envío::= SECUENCIA {
ID de servicio de envío PSID,
ID de servidor de envío ID de servidor de envío,
ID de cliente de envío ID de cliente de envío}
353
345
Servidor de envío
TRANSMITIR SOLICITUD DE SERVICIO DE ENVÍO [Solicitud de servicio de envío]
{EID, LISTA DE servicio de envío}
RECIBIR RESPUESTA DE SERVICIO DE ENVÍO [Respuesta de servicio de envío [200 OK]]
{EID, servicio de envío}
TRANSMITIR MENSAJE DE SOLICITUD DE REGISTRO [solicitud de registro]
{RMFID, servicio de envío}
356
ESTABLECER INTERFAZ
357
TRANSMITIR MENSAJE DE RESPUESTA DE REGISTRO [solicitud de registro]
358
{RMFID, terminalID}
TRANSMITIR MENSAJE DE RESPUESTA DE REGISTRO [respuesta de registro [200 OK]]
359
{RMFID, testigo de envío}
TRANSMITIR MENSAJE DE RESPUESTA DE REGISTRO [respuesta de registro [200 OK]]
360
{Testigo de envío}
347
DPF
354
355
349
SERVIDOR DE SUMINISTRO DE PERFIL
Configuración de servicio de envío
A
B
C
D
E
F

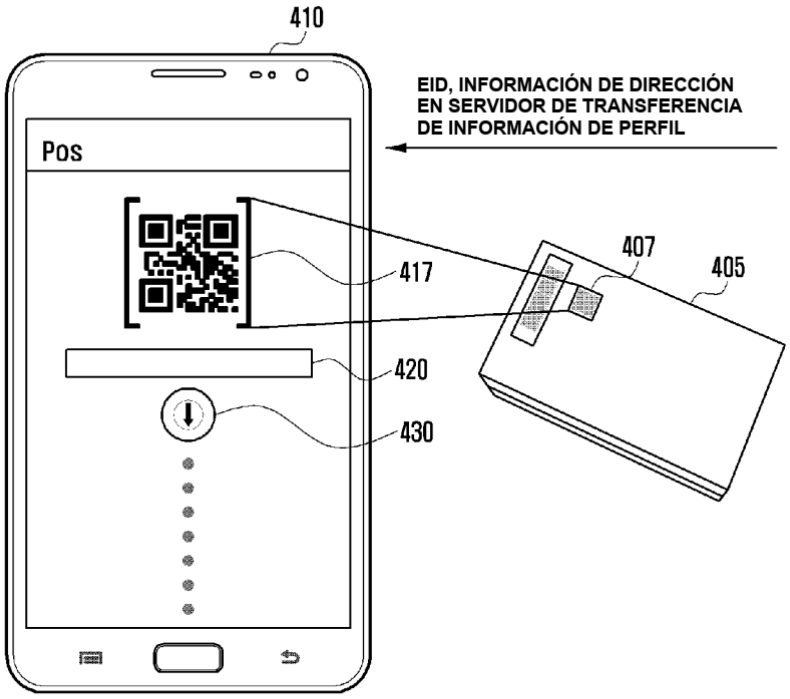
[Fig. 3c]


A
B
C
D
E
F
G
H
I
J
K
L
Registro de servicio de envío
GENERAR TESTIGO DE EID
[Generar testigo de EID
a partir de EID]
361
TRANSMITIR INFORME DE SERVICIO DE ENVÍO [informe de servicio de envío]
{EID, servicio de envío, testigo de envío, testigo de EID}
362
CONECTAR AL SERVIDOR DE ENVÍO
363
GENERAR ID de notificación
de envío
[generar y gestionar ID
de notificación de envío
[PNID]]
364
TRANSMITIR ID de notificación de envío [notificación de envío]
{testigo de envío, PNID, testigo de EID}
365
RECIBIR ACK de notificación de envío [ACK de notificación de envío]
{testigo de envío, PNID}
366
TRANSFERIR notificación de envío [notificación de envío [300 envío]]
{testigo de envío, PNID, testigo de EID}
367
TRANSMITIR ACK de notificación de envío [ACK de notificación de envío [210 recibido]]
{testigo de envío, PNID}
368
TRANSFERIR ACK de notificación de envío [ACK de notificación de envío]
{testigo de envío, PNID}
369
TRANSFERIR notificación de envío [notificación de envío]
{testigo de EID}
370
TRANSMITIR SOLICITUD DE EVENTO [solicitud de evento]
{EID}
371
TRANSMITIR RESPUESTA DE EVENTO [respuesta de evento]
{sin eventos}
372

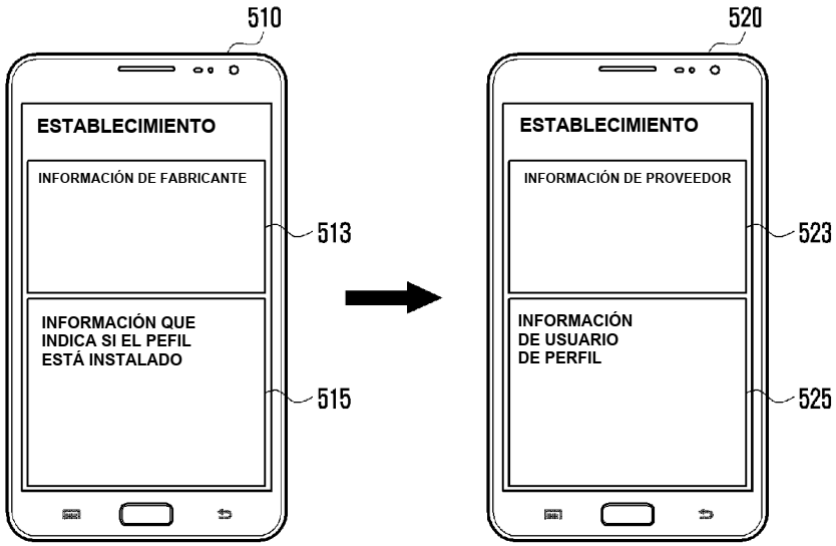
[Fig. 3d]


G
H
I
J
K
L
Notificación de envío
373
TRANSFERIR INFORMACIÓN DE PERFIL [evento de registro]
{EID, ID de evento}
374
REALIZAR ACUSE DE RECIBO DE INFORMACIÓN QUE CORRESPONDE A eUICC
[hallar los EID]
{servicio de envío, testigo de envío, testigo de EID}
375
TRANSFERIR notificación de envío [notificación de envío]
{testigo de envío, PNID, testigo de EID}
376
RECIBIR ACK de notificación de envío [ACK de notificación de envío]
{testigo de envío, PNID}
377
TRANSFERIR notificación de envío [notificación de envío [300 envío]]
{testigo de envío, PNID, testigo de EID}
378
TRANSMITIR ACK de notificación de envío [ACK de notificación de envío [210 recibido]
{testigo de envío, PNID}
379
TRASNFERIR ACK de notificación de envío [ACK de notificación de envío]
{testigo de envío, PNID}
380
TRANSFERIR notificación de envío [notificación de envío]
{testigo de EID}
381
CONVERTIR TESTIGO DE EID A EID
[convertir testigo de EID a EID]
382
TRANSMITIR SOLICITUD DE EVENTO [solicitud de evento]
{EID}
383
TRANSMITIR RESPUESTA DE EVENTO [respuesta de evento]
{EMID, ID de evento}

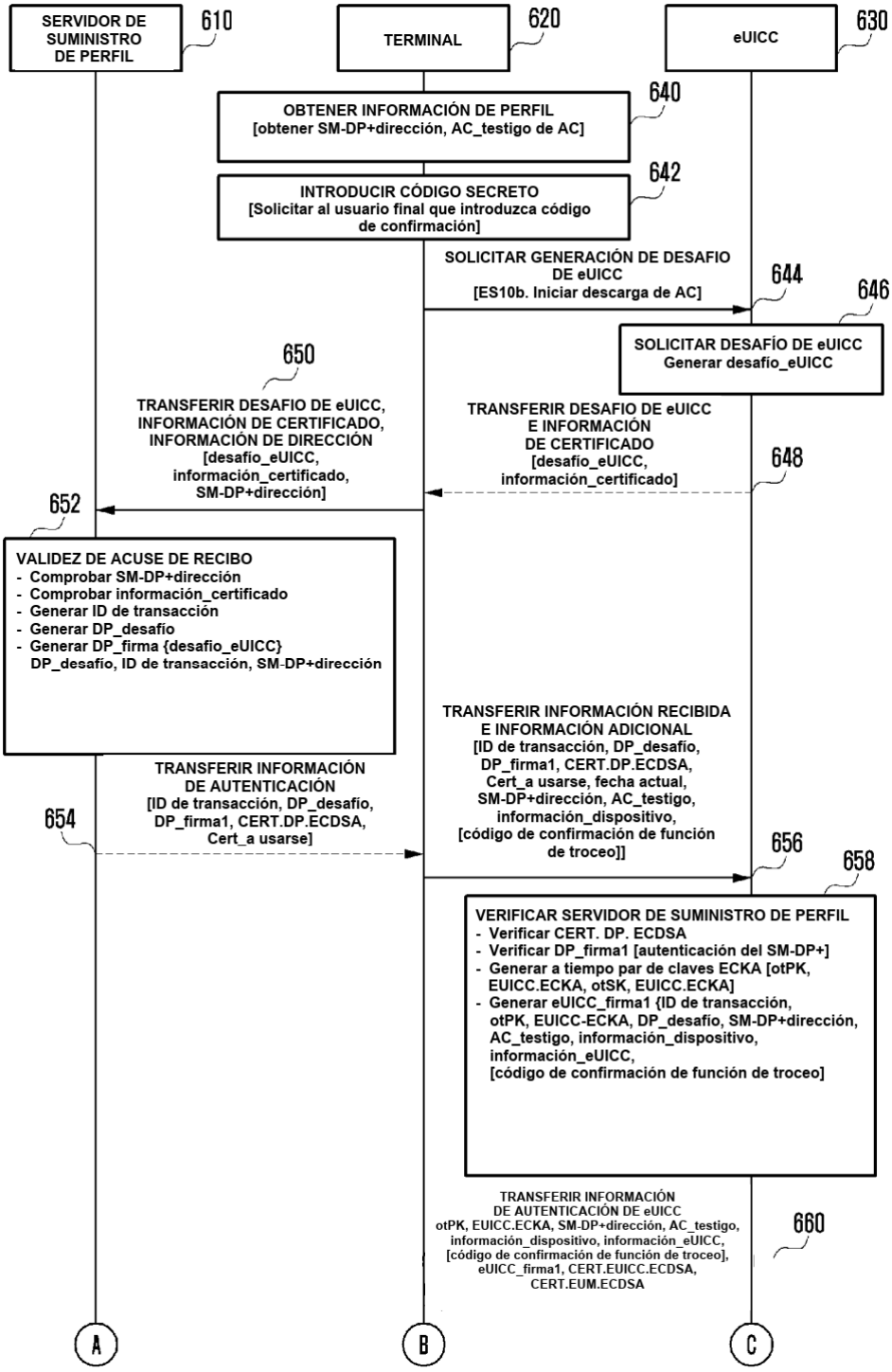
[Fig. 4]


410
EID, INFORMACIÓN DE DIRECCIÓN
EN SERVIDOR DE TRANSFERENCIA
DE INFORMACIÓN DE PERFIL
Pos
417
407
405
420
430

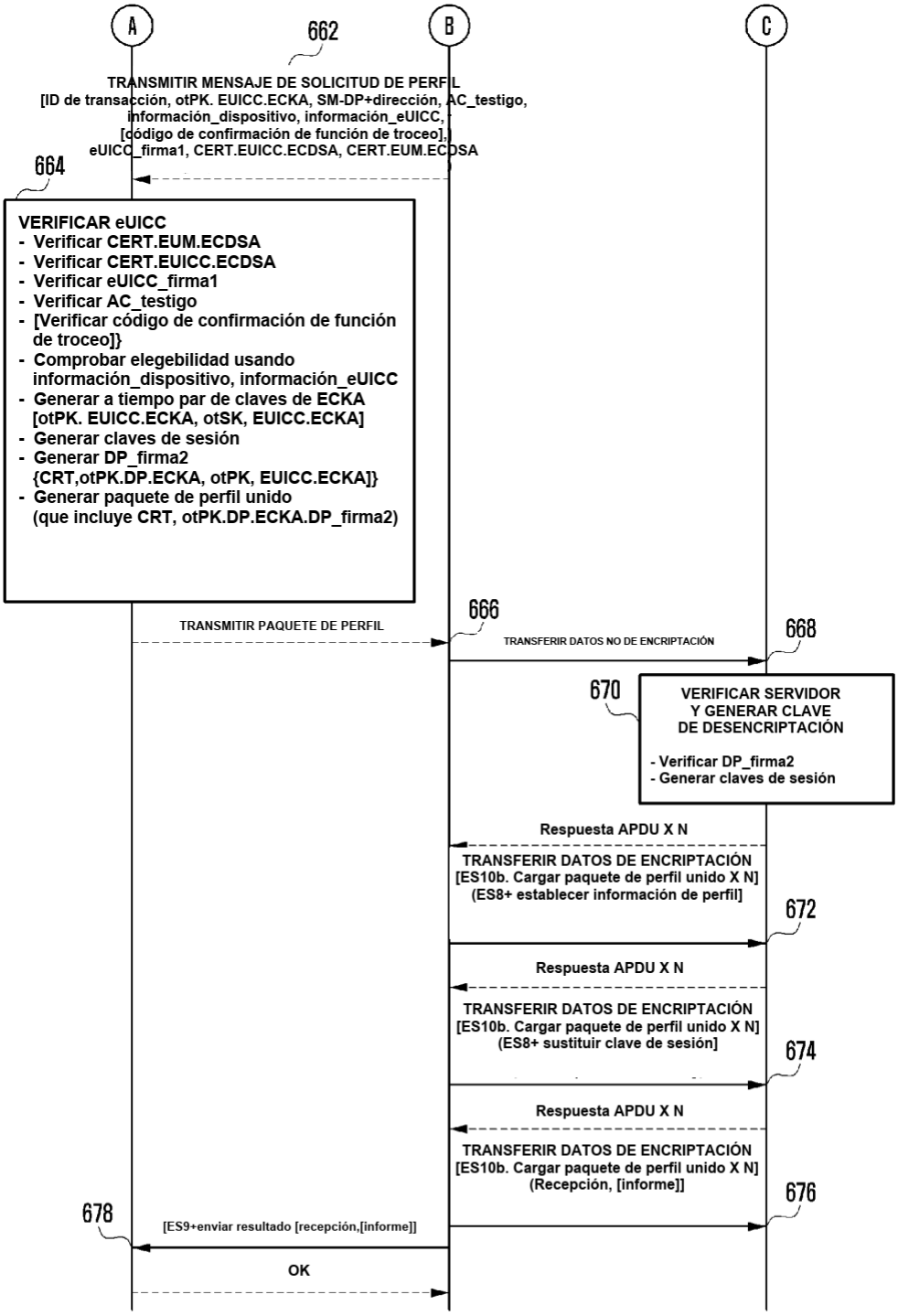
[Fig. 5]


510
ESTABLECIMIENTO
INFORMACIÓN DE FABRICANTE
513
INFORMACIÓN QUE
INDICA SI EL PEFIL
ESTÁ INSTALADO
515
520
ESTABLECIMIENTO
INFORMACIÓN DE PROVEEDOR
523
INFORMACIÓN
DE USUARIO
DE PERFIL
525

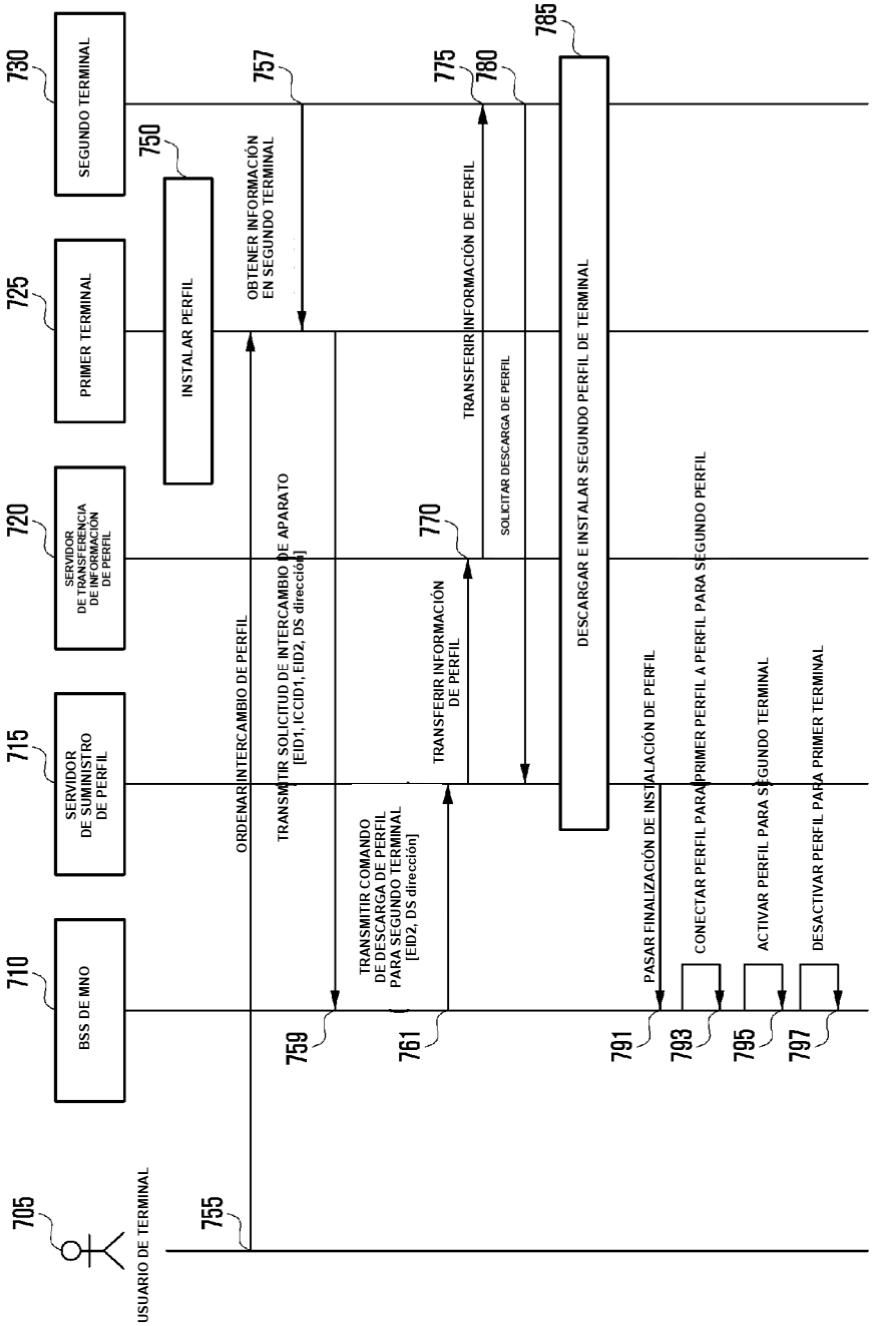
[Fig. 6a]


SERVIDOR DE SUMINISTRO DE PERFIL
610
TERMINAL
620
eUICC
630
OBTENER INFORMACIÓN DE PERFIL
[obtener SM-DP+dirección, AC_testigo de AC]
640
INTRODUCIR CÓDIGO SECRETO
[Solicitar al usuario final que introduzca código de confirmación]
642
SOLICITAR GENERACIÓN DE DESAFIO DE eUICC
[ES10b. Iniciar descarga de AC]
644
646
SOLICITAR DESAFÍO DE eUICC
Generar desafío_eUICC
650
TRANSFERIR DESAFIO DE eUICC, INFORMACIÓN DE CERTIFICADO, INFORMACIÓN DE DIRECCIÓN
[desafío_eUICC, información_certificado, SM-DP+dirección]
TRANSFERIR DESAFIO DE eUICC E INFORMACIÓN DE CERTIFICADO
[desafío_eUICC, información_certificado]
648
652
VALIDEZ DE ACUSE DE RECIBO
- Comprobar SM-DP+dirección
- Comprobar información_certificado
- Generar ID de transacción
- Generar DP_desafío
- Generar DP_firma {desafío_eUICC}
DP_desafío, ID de transacción, SM-DP+dirección
TRANSFERIR INFORMACIÓN RECIBIDA E INFORMACIÓN ADICIONAL
[ID de transacción, DP_desafío, DP_firma1, CERT.DP.ECDSA, Cert_a usarse, fecha actual, SM-DP+dirección, AC_testigo, información_dispositivo, [código de confirmación de función de troceo]]
TRANSFERIR INFORMACIÓN DE AUTENTICACIÓN
[ID de transacción, DP_desafío, DP_firma1, CERT.DP.ECDSA, Cert_a usarse]
654
656
658
VERIFICAR SERVIDOR DE SUMINISTRO DE PERFIL
- Verificar CERT. DP. ECDSA
- Verificar DP_firma1 [autenticación del SM-DP+]
- Generar a tiempo par de claves ECKA [otPK, EUICC.ECKA, otSK, EUICC.ECKA]
- Generar eUICC_firma1 {ID de transacción, otPK, EUICC-ECKA, DP_desafío, SM-DP+dirección, AC_testigo, información_dispositivo, información_eUICC, [código de confirmación de función de troceo]
TRANSFERIR INFORMACIÓN DE AUTENTICACIÓN DE eUICC
otPK, EUICC.ECKA, SM-DP+dirección, AC_testigo, información_dispositivo, información_eUICC, [código de confirmación de función de troceo], eUICC_firma1, CERT.EUICC.ECDSA, CERT.EUM.ECDSA
660
A
B
C

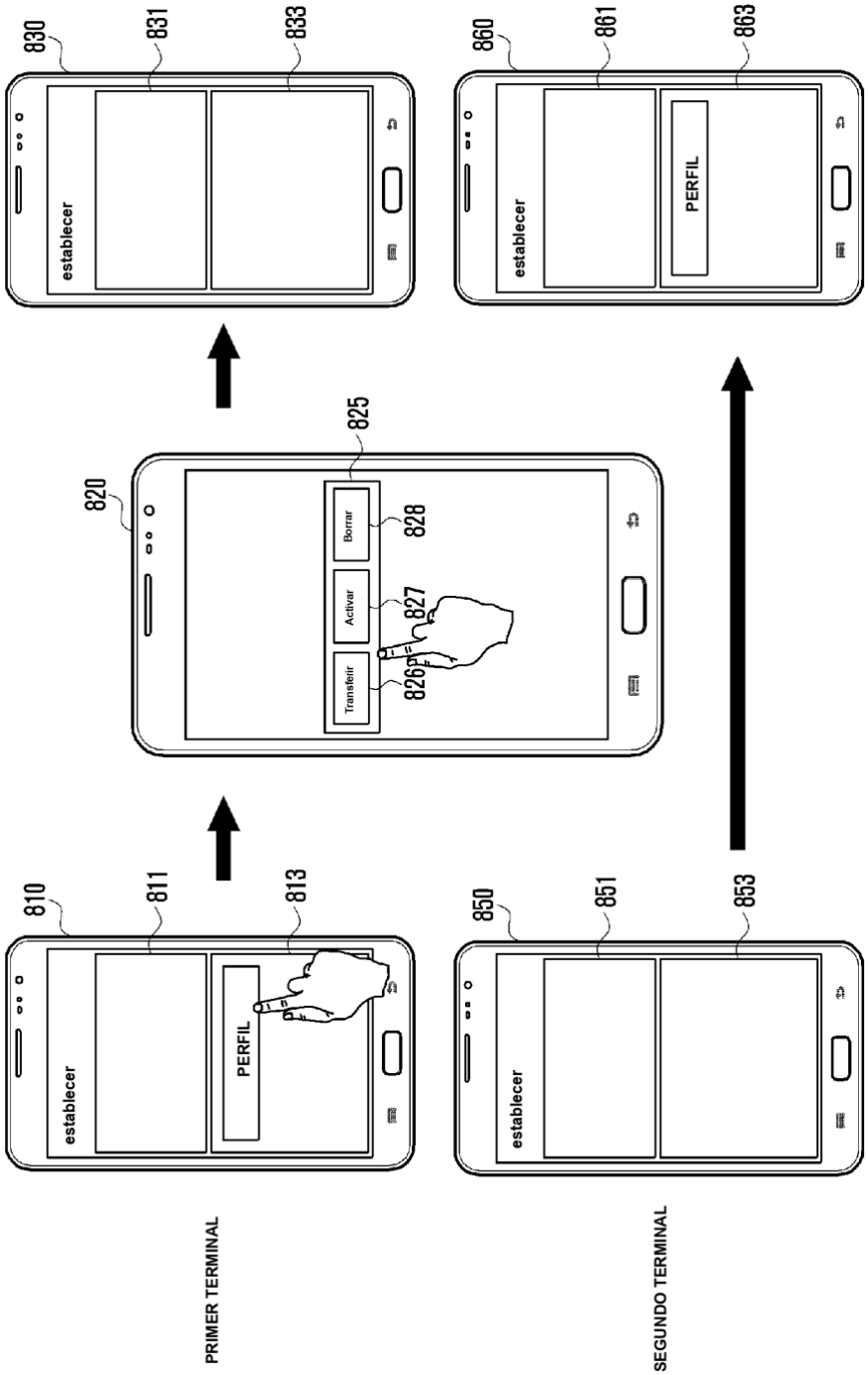
[Fig. 6b]


A
B
C
662
TRANSMITIR MENSAJE DE SOLICITUD DE PERFIL
[ID de transacción, otPK. EUICC.ECKA, SM-DP+dirección, AC_testigo,
información_dispositivo, información_eUICC,
[código de confirmación de función de troceo],]
eUICC_firma1, CERT.EUICC.ECDSA, CERT.EUM.ECDSA
664
VERIFICAR eUICC
- Verificar CERT.EUM.ECDSA
- Verificar CERT.EUICC.ECDSA
- Verificar eUICC_firma1
- Verificar AC_testigo
- [Verificar código de confirmación de función de troceo]}
- Comprobar elegebilidad usando información_dispositivo, información_eUICC
- Generar a tiempo par de claves de ECKA [otPK. EUICC.ECKA, otSK, EUICC.ECKA]
- Generar claves de sesión
- Generar DP_firma2 {CRT,otPK.DP.ECKA, otPK, EUICC.ECKA]}
- Generar paquete de perfil unido (que incluye CRT, otPK.DP.ECKA.DP_firma2)
TRANSMITIR PAQUETE DE PERFIL
666
TRANSFERIR DATOS NO DE ENCRIPTACIÓN
668
670
VERIFICAR SERVIDOR Y GENERAR CLAVE DE DESENCRIPTACIÓN
- Verificar DP_firma2
- Generar claves de sesión
Respuesta APDU X N
TRANSFERIR DATOS DE ENCRIPTACIÓN
[ES10b. Cargar paquete de perfil unido X N]
(ES8+ establecer información de perfil]
672
Respuesta APDU X N
TRANSFERIR DATOS DE ENCRIPTACIÓN
[ES10b. Cargar paquete de perfil unido X N]
(ES8+ sustituir clave de sesión]
674
Respuesta APDU X N
TRANSFERIR DATOS DE ENCRIPTACIÓN
[ES10b. Cargar paquete de perfil unido X N]
(Recepción, [informe]]
676
678
[ES9+enviar resultado [recepción,[informe]]
OK

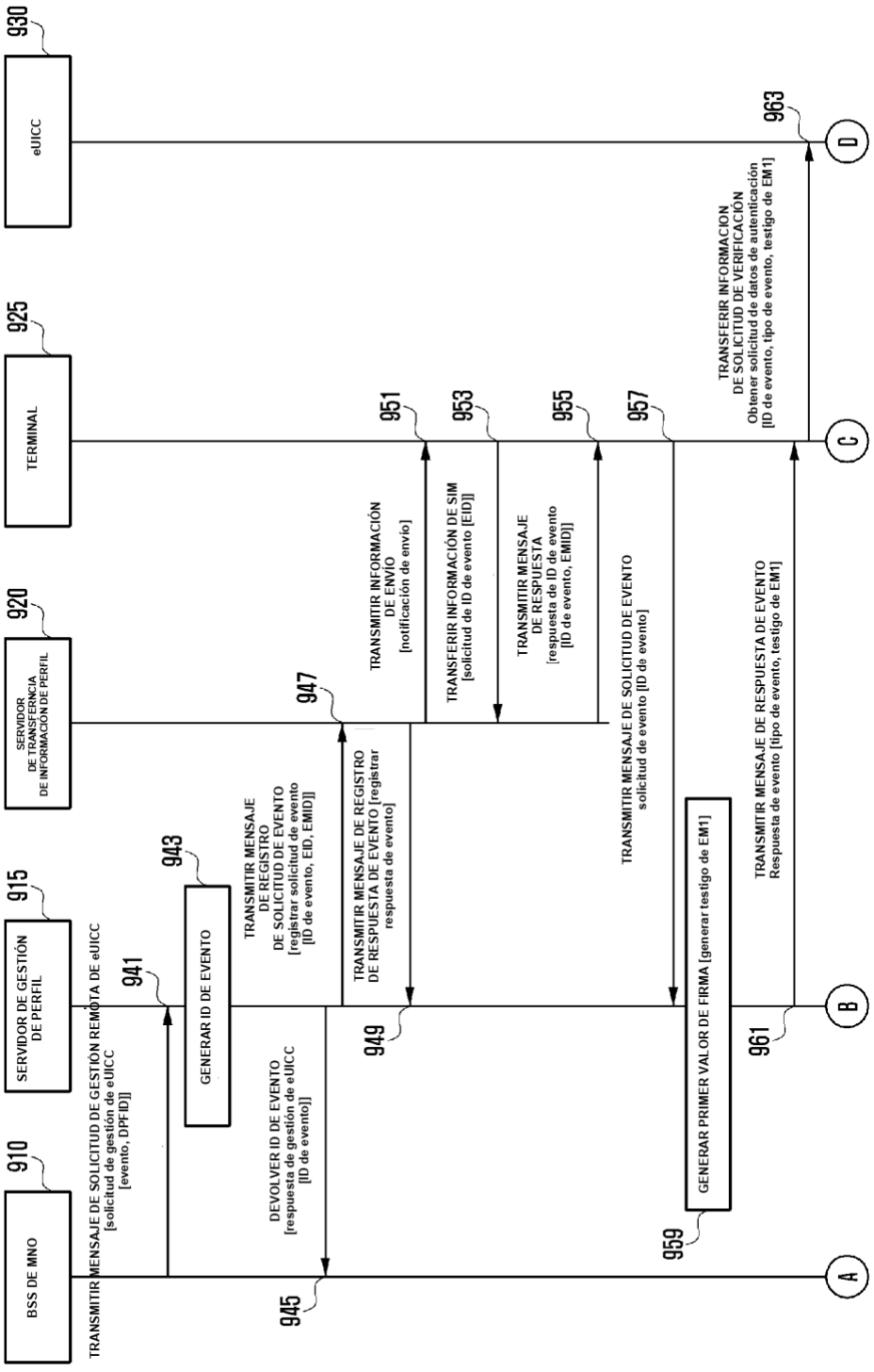
[Fig. 7]


730
SEGUNDO TERMINAL
725
PRIMER TERMINAL
720
SERVIDOR DE TRANSFERENCIA DE INFORMACIÓN DE PERFIL
715
SERVIDOR DE SUMINISTRO DE PERFIL
710
BSS DE MNO
705
USUARIO DE TERMINAL
750
INSTALAR PERFIL
757
OBTENER INFORMACIÓN EN SEGUNDO TERMINAL
775
780
TRANSFERIR INFORMACIÓN DE PERFIL
785
DESCARGAR E INSTALAR SEGUNDO PERFIL DE TERMINAL
SOLICITAR DESCARGA DE PERFIL
ORDENAR INTERCAMBIO DE PERFIL
TRANSMITIR SOLICITUD DE INTERCAMBIO DE APARATO [EID1, ICCID1, EID2, DS dirección]
770
TRANSFERIR INFORMACIÓN DE PERFIL
TRANSMITIR COMANDO DE DESCARGA DE PERFIL PARA SEGUNDO TERMINAL [EID2, DS dirección]
PASAR FINALIZACIÓN DE INSTALACIÓN DE PERFIL
CONECTAR PERFIL PARA PRIMER PERFIL A PERFIL PARA SEGUNDO PERFIL
ACTIVAR PERFIL PARA SEGUNDO TERMINAL
DESACTIVAR PERFIL PARA PRIMER TERMINAL
755
759
761
791
793
795
797

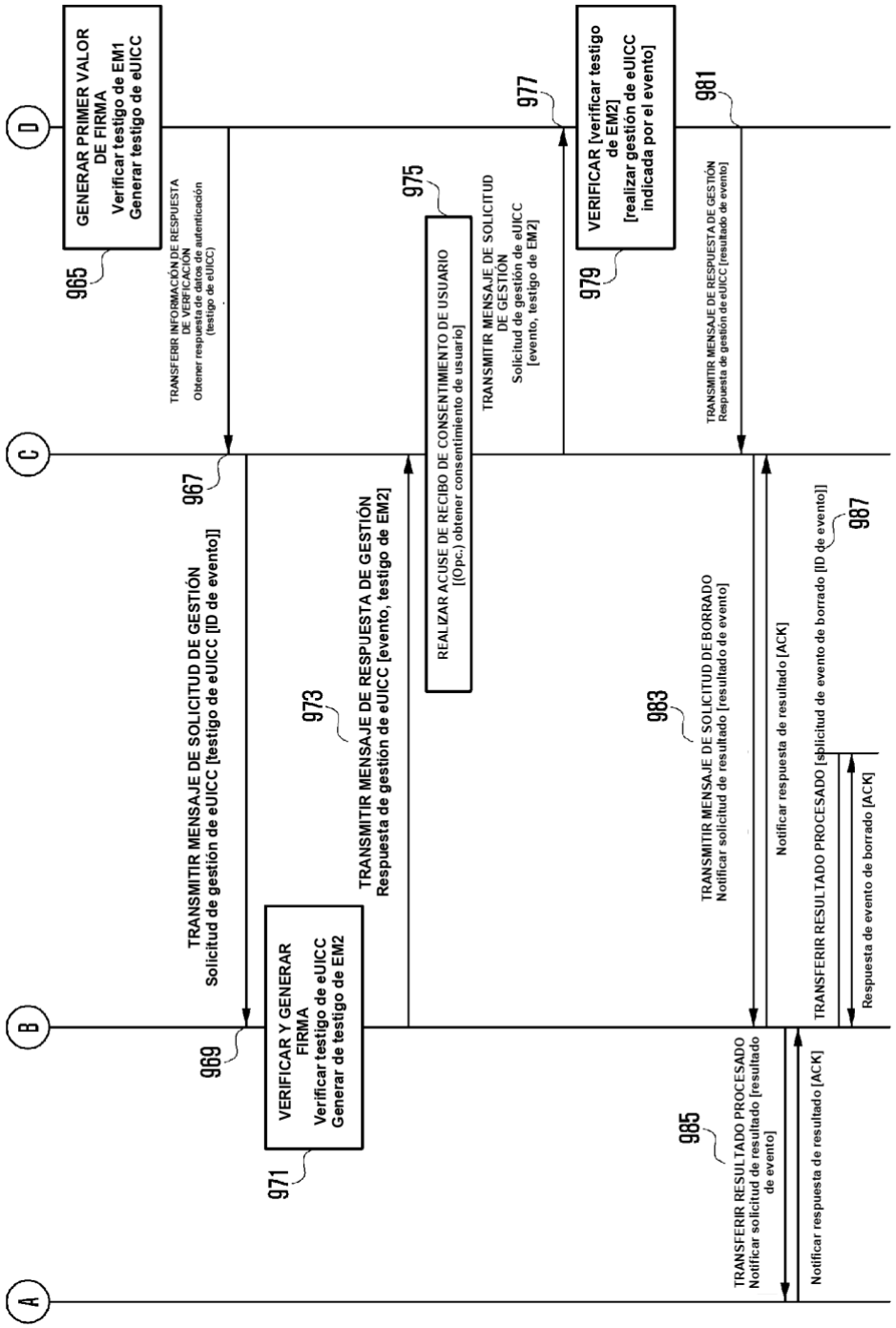
[Fig. 8]


830
831
833
establecer
860
861
863
establecer
PERFIL
825
820
828
Borrar
827
Activar
826
Transferir
810
811
813
establecer
PERFIL
850
851
853
establecer
PRIMER TERMINAL
SEGUNDO TERMINAL

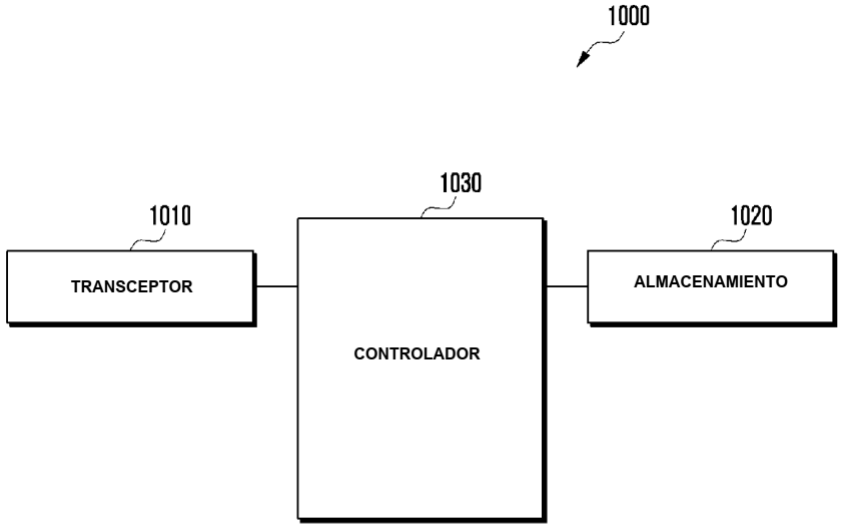
[Fig. 9a]


930
eUICC
925
TERMINAL
920
SERVIDOR DE TRANSFERNCIA DE INFORMACIÓN DE PERFIL
915
SERVIDOR DE GESTIÓN DE PERFIL
910
BSS DE MNO
TRANSMITIR MENSAJE DE SOLICITUD DE GESTIÓN REMOTA DE eUICC [solicitud de gestión de eUICC [evento, DPFID]]
941
GENERAR ID DE EVENTO
943
TRANSMITIR MENSAJE DE REGISTRO DE SOLICITUD DE EVENTO [registrar solicitud de evento [ID de evento, EID, EMID]]
947
TRANSMITIR MENSAJE DE REGISTRO DE RESPUESTA DE EVENTO [registrar respuesta de evento]
949
DEVOLVER ID DE EVENTO [respuesta de gestión de eUICC [ID de evento]]
945
TRANSMITIR INFORMACIÓN DE ENVÍO [notificación de envío]
951
TRANSFERIR INFORMACIÓN DE SIM [solicitud de ID de evento [EID]]
953
TRANSMITIR MENSAJE DE RESPUESTA [respuesta de ID de evento [ID de evento, EMID]]
955
TRANSMITIR MENSAJE DE SOLICITUD DE EVENTO solicitud de evento [ID de evento]
957
GENERAR PRIMER VALOR DE FIRMA [generar testigo de EM1]
959
TRANSMITIR MENSAJE DE RESPUESTA DE EVENTO Respuesta de evento [tipo de evento, testigo de EM1]
961
TRANSFERIR INFORMACION DE SOLICITUD DE VERIFICACIÓN Obtener solicitud de datos de autenticación [ID de evento, tipo de evento, testigo de EM1]
963
A
B
C
D

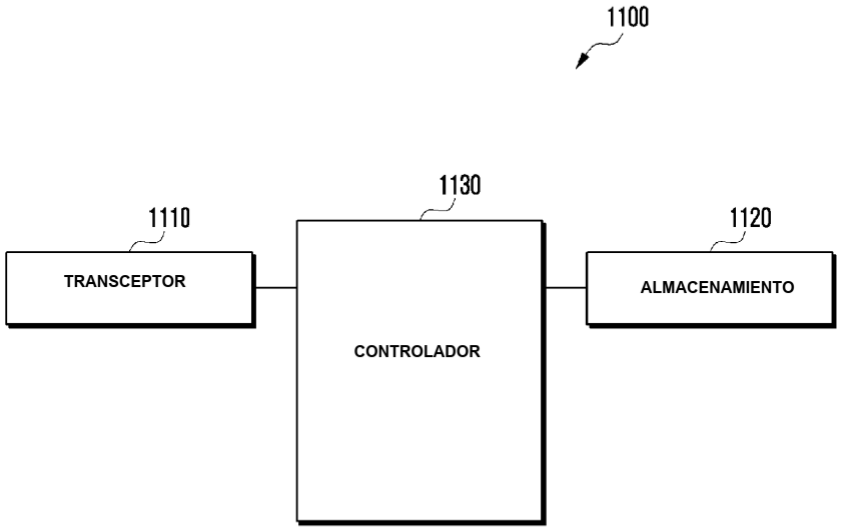
[Fig. 9b]


A
B
C
D
GENERAR PRIMER VALOR DE FIRMA
Verificar testigo de EM1
Generar testigo de eUICC
965
TRANSFERIR INFORMACIÓN DE RESPUESTA DE VERIFICACIÓN
Obtener respuesta de datos de autenticación (testigo de eUICC)
967
TRANSMITIR MENSAJE DE SOLICITUD DE GESTIÓN
Solicitud de gestión de eUICC [testigo de eUICC [ID de evento]]
969
VERIFICAR Y GENERAR FIRMA
Verificar testigo de eUICC
Generar de testigo de EM2
971
973
TRANSMITIR MENSAJE DE RESPUESTA DE GESTIÓN
Respuesta de gestión de eUICC [evento, testigo de EM2]
975
REALIZAR ACUSE DE RECIBO DE CONSENTIMIENTO DE USUARIO
[(Opc.) obtener consentimiento de usuario]
977
TRANSMITIR MENSAJE DE SOLICITUD DE GESTIÓN
Solicitud de gestión de eUICC [evento, testigo de EM2]
979
VERIFICAR [verificar testigo de EM2] [realizar gestión de eUICC indicada por el evento]
981
TRANSMITIR MENSAJE DE RESPUESTA DE GESTIÓN
Respuesta de gestión de eUICC [resultado de evento]
983
TRANSMITIR MENSAJE DE SOLICITUD DE BORRADO
Notificar solicitud de resultado [resultado de evento]
985
TRANSFERIR RESULTADO PROCESADO
Notificar solicitud de resultado [resultado de evento]
Notificar respuesta de resultado [ACK]
Notificar respuesta de resultado [ACK]
TRANSFERIR RESULTADO PROCESADO [solicitud de evento de borrado [ID de evento]]
987
Respuesta de evento de borrado [ACK]

[Fig. 10]



[Fig. 11]



[Fig. 12]