(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 848 098**

(51) Int. CI.:

H04W 12/08 (2011.01)
H04W 8/18 (2009.01)
H04W 88/18 (2009.01)
H04W 12/04 (2011.01)
H04W 12/02 (2009.01)
H04L 29/06 (2006.01)
H04W 12/00 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.07.2015 PCT/KR2015/007215**

(87) Fecha y número de publicación internacional: **21.01.2016 WO16010312**

(96) Fecha de presentación y número de la solicitud europea: **10.07.2015 E 15821440 (3)**

(97) Fecha y número de publicación de la concesión europea: **06.01.2021 EP 3171622**

(54) Título: **Procedimiento y dispositivo para instalar perfil de eUICC**

(30) Prioridad:

17.07.2014 KR 20140090591

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.08.2021

(73) Titular/es:

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

(72) Inventor/es:

PARK, JONGHAN;
LEE, DUCKEY;
LEE, SANGSOO y
CHO, SONGYEAN

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Procedimiento y dispositivo para instalar perfil de eUICC

[Campo técnico]

La presente invención se refiere a un procedimiento y un dispositivo para instalar un perfil de una eUICC (Tarjeta de Circuito Integrado Universal incorporada) y, más particularmente, a un procedimiento y un dispositivo para instalar información de suscriptor de comunicaciones móviles (perfil) en un módulo de seguridad de manera remota reemplazando una UICC (Tarjeta de Circuito Integrado Universal) con la eUICC.

[Técnica antecedente]

Una UICC (Tarjeta de Circuito Integrado Universal) es una tarjeta inteligente que es insertada en un terminal de comunicaciones móviles y almacena información personal tal como información de autentificación de conexión de red, números de teléfono, y SMS de un suscriptor de comunicaciones móviles. La UICC habilita el uso seguro de la comunicación móvil al realizar la autentificación de suscriptor y generar una clave de seguridad de tráfico cuando se conecta a una red de comunicaciones móviles tal como GSM, WCDMA, y LTE.

Las aplicaciones de comunicación tales como un SIM, USIM, e ISIM se lanzan en la UICC de acuerdo con el tipo de la red de comunicaciones móviles conectada por un suscriptor. Adicionalmente, la UICC proporciona una función de seguridad de nivel superior para lanzar diversas aplicaciones tales como billetera electrónica, emisión de billetes, y pasaporte electrónico.

Las UICCs convencionales son fabricadas como una tarjeta dedicada para un proveedor de comunicaciones móviles específico de acuerdo con una solicitud del proveedor de comunicaciones móviles. Por consiguiente, la UICC es liberada preinstalando información de autentificación para conectarse a una red de un proveedor correspondiente (por ejemplo, IMSI y valor K de una aplicación de USIM). La UICC fabricada es suministrada a un proveedor de comunicaciones móviles correspondiente y se proporciona a un suscriptor, y si es necesario, la gestión de instalación, modificación, y eliminación de una aplicación en la UICC puede ser realizada usando una tecnología tal como una OTA (Por El Aire). El suscriptor puede usar los servicios de red y aplicaciones del proveedor de comunicaciones móviles correspondiente insertando la UICC en un terminal de comunicaciones móviles propiedad del suscriptor, y si el terminal es reemplazado por uno nuevo, el suscriptor puede usar la información de autentificación existente, números de teléfono para comunicación móvil, y agenda telefónica personal insertando la UICC en el nuevo terminal.

Las memorias descriptivas físicas y funciones lógicas de la UICC están definidas por una organización de estandarización del ETSI (Instituto Europeo de Estándares de Telecomunicaciones) que proporciona compatibilidad internacional. En vista de la memoria descriptiva física, un factor de forma de la UICC ha sido reducido gradualmente de un Mini SIM usado más ampliamente, a un Micro SIM usado desde hace diversos años, y además a un Nano SIM lanzado recientemente. Esto contribuye mucho a la miniaturización del terminal de comunicaciones móviles.

Recientemente, ha sido establecida una UICC más pequeña que el Nano SIM, sin embargo, puede ser difícil que sea estandarizada debido a que se trata de una pérdida de UICC. Puede ser difícil miniaturizar aún más la UICC debido a que se requiere un espacio para instalar una ranura para un terminal cuando se consideran las características de una UICC desmontable.

Adicionalmente, la UICC convencional no es adecuada para equipo de M2M (Máquina a Máquina) que realiza una conexión a una red de datos de comunicación móvil sin una operación directa de una persona en diversos entornos de instalación de un aparato doméstico inteligente, medidor eléctrico/de agua, y cámara CCTV.

Con el fin de resolver tal problema, se requiere el reemplazo de la UICC convencional, y se integra un módulo de seguridad que tiene una función similar a la de la UICC en un terminal de comunicaciones móviles en un proceso de producción.

El módulo de seguridad interno desarrollado de acuerdo con tal requisito es un módulo de seguridad instalado en un terminal, sin embargo, no puede lanzar información de autentificación de conexión de red de un proveedor de comunicaciones móviles específico tal como una IMSI y un valor K de un USIM mientras que fabrica el terminal. Por consiguiente, la información de autentificación del módulo de seguridad interno de terminal puede ser establecida por un usuario después de comprar un terminal lanzado con un módulo de seguridad interno correspondiente y convertirse en suscriptor de un proveedor de comunicaciones móviles específico.

En una red que soporta un terminal recientemente desarrollado que tiene un módulo de seguridad interno, si el terminal se conecta a una cierta red de comunicaciones móviles aprovisionando un perfil, un servidor que proporciona perfiles encripta el perfil usando una clave de sesión generada por autentificación mutua con el terminal en tiempo real y transmite el perfil encriptado al terminal. Un módulo de seguridad de hardware instalado en un servidor que proporciona perfiles para encriptar un perfil puede ser adecuado para encriptar un pequeño número de perfiles en tiempo real, sin embargo, si un gran número de terminales va a recibir perfiles para el terminal que tiene un módulo de seguridad interno, puede ser imposible proporcionar los perfiles debido a que todos los perfiles deben estar encriptados al mismo

tiempo. Por consiguiente, se pueden generar dificultades técnicas cuando se aprovisionan perfiles para un gran número de terminales que tienen un módulo de seguridad interno.

Adicionalmente, hay un problema de que no se pueden proporcionar perfiles correctos para algunos terminales si un estado de red externa de conectar el gran número de terminales que tienen un módulo de seguridad interno a un servidor de SM-DP (Preparación de Datos de Gestor de Suscripción) es pobre.

Por consiguiente, se requiere un procedimiento mejorado de tal manera que un perfil para un terminal que tenga un módulo de seguridad interno pueda ser aprovisionado sin sincronización con una red externa y los perfiles para un gran número de terminales puedan ser encriptados y almacenados con antelación.

El documento WO2013036010 se refiere a un sistema constituido por un operador de red móvil (MNO), un gestor de suscripción (SM), y una UICC incorporada (eUICC), en el que el sistema de MNO o el SM almacena un certificado de eUICC que puede verificar la identidad de la eUICC, transfiere el certificado de eUICC al sistema de MNO o al SM en un proceso de aprovisionamiento o cambio de MNO, verifica la identidad de una eUICC correspondiente usando el certificado de eUICC recibido, y encripta y transfiere un perfil a la eUICC solo si la verificación es exitosa de tal manera la eUICC puede ser verificada durante los procesos de aprovisionamiento o cambio de MNO.

[Divulgación de la invención]

[Problema técnico]

La presente invención está definida en el conjunto adjunto de reivindicaciones.

Con el fin de resolver los problemas anteriores, la presente invención proporciona un procedimiento y un dispositivo para aprovisionar un perfil sin sincronización con una red externa cuando se proporciona el perfil a un terminal.

Adicionalmente, la presente invención proporciona un procedimiento y un dispositivo para almacenar un gran número de perfiles y claves de contraseña para encriptar los perfiles con antelación de aprovisionar perfiles y proporcionar información de perfil encriptada a los terminales cuando se aprovisionan perfiles de los terminales.

[Solución al problema]

Con el fin de lograr el objeto anterior, un procedimiento para instalar un perfil de una eUICC (Tarjeta de Circuito Integrado Universal incorporada) de un dispositivo de red de acuerdo con la presente invención puede incluir las etapas de: adquirir al menos un perfil encriptado con una primera clave de contraseña y al menos una primera clave de contraseña encriptada con una segunda clave de contraseña; y transmitir el al menos un perfil encriptado y la al menos una primera clave de contraseña encriptada a al menos una eUICC cuando se inicia la instalación de perfil para la eUICC. La primera clave de contraseña es reencriptada por la primera clave de contraseña con una tercera clave de contraseña y transmitida a la al menos una eUICC y los perfiles encriptados son desencriptados por la primera clave de contraseña e instalados en la al menos una eUICC respectivamente.

Cada una de la primera clave de contraseña, segunda clave de contraseña, y tercera clave de contraseña puede estar configurada respectivamente con una pluralidad de claves. Por ejemplo, la primera clave de contraseña, segunda clave de contraseña, y tercera clave de contraseña pueden ser un conjunto de claves de contraseña que incluya información de clave. Adicionalmente, cada clave de contraseña puede ser una clave SCP 80, clave SCP 81, clave SCP 03, o clave asimétrica. Como ejemplos de la clave asimétrica en la autentificación basada en RSA, hay una clave pública incluida en un certificado de autentificación en un lenguaje plano y una clave personal generada pareada con la clave pública y almacenada de manera segura en una entidad propiedad del certificado de autentificación. En la siguiente descripción, encriptar usando un certificado de autentificación significa transmitir contenidos encriptando con una clave pública incluida en una entidad receptora del certificado de autentificación, y la entidad receptora puede realizar la desencriptación usando la clave personal almacenada internamente.

Adicionalmente, un procedimiento para instalar un perfil de una eUICC (Tarjeta de Circuito Integrado Universal incorporada) de una SM-DP (Preparación de Datos de Gestor de Suscripción) de acuerdo con la presente invención puede incluir la etapa de transmitir al menos uno de al menos un perfil encriptado y al menos una primera clave de contraseña para encriptar el al menos un perfil en un dispositivo de red. El al menos un perfil encriptado y la al menos una primera clave de contraseña son transmitidos a al menos una eUICC si se inicia la instalación de perfil para la eUICC, y la al menos una primera clave de contraseña es transmitida a la al menos una eUICC encriptando con una tercera clave de contraseña y el al menos un perfil encriptado es transmitido a la al menos una eUICC desencriptando con la al menos una primera clave de contraseña.

Adicionalmente, un dispositivo de red para instalar un perfil de una eUICC (Tarjeta de Circuito Integrado Universal incorporada) de acuerdo con la presente invención puede incluir: una unidad de comunicación configurada para realizar la comunicación de datos; un dispositivo de encriptación configurado para realizar la encriptación y desencriptación; y un dispositivo de almacenamiento configurado para adquirir al menos un perfil encriptado y al menos una primera contraseña para encriptar el al menos un perfil. La unidad de comunicación transmite el al menos un perfil encriptado y la al menos una primera clave de contraseña a al menos una eUICC cuando se inicia la instalación de

perfil para la eUICC, el dispositivo de encriptación transmite la al menos una primera clave de contraseña a la al menos una eUICC encriptando con una tercera clave de contraseña, y el al menos un perfil encriptado es instalado en la al menos una eUICC desencriptando con la al menos una primera clave de contraseña.

Adicionalmente, un servidor de SM-DP (Preparación de Datos de Gestor de Suscripción) para instalar un perfil de una eUICC (Tarjeta de Circuito Integrado Universal incorporada) de acuerdo con la presente invención puede incluir: una unidad de comunicación configurada para realizar la comunicación de datos; y una unidad de control configurada para controlar para transmitir al menos uno de al menos un perfil encriptado y al menos una primera clave de contraseña para encriptar el al menos un perfil a un dispositivo de red. El al menos un perfil encriptado y la al menos una primera clave de contraseña son transmitidos a al menos una eUICC cuando se inicia una instalación de perfil para la eUICC, y la al menos una primera clave de contraseña es transmitida a la al menos una eUICC encriptando con una tercera clave de contraseña, y el al menos un perfil encriptado es instalado en la al menos una eUICC desencriptando con la al menos una primera clave de contraseña.

[Efectos ventajosos de la invención]

De acuerdo con diversas realizaciones de la presente invención, se puede proporcionar un perfil encriptado sin una pérdida de rendimiento o de datos cuando se aprovisionan perfiles al mismo tiempo para un gran número de terminales que tienen un módulo de seguridad interno.

Adicionalmente, de acuerdo con diversas realizaciones de la presente invención, el aprovisionamiento de perfiles se puede realizar para un gran número de terminales incluso aunque un estado de red externa de conectar un servidor que proporciona perfiles y los terminales sea pobre.

[Breve descripción de los dibujos]

La figura 1 ilustra una estructura de una red que soporta una eUICC.
La figura 2 es un diagrama de flujo que ilustra un procedimiento para instalar un perfil de una eUICC.
La figura 3 ilustra una estructura de una red que soporta una eUICC de acuerdo con la presente invención.
La figura 4 es un diagrama de flujo que ilustra un procedimiento para instalar un perfil de una eUICC de acuerdo con una primera realización de la presente invención.
La figura 5 es un diagrama de flujo que ilustra un procedimiento para instalar un perfil de una eUICC de acuerdo con una segunda realización de la presente invención.
La figura 6 es un diagrama de flujo que ilustra un procedimiento para instalar un perfil de una eUICC de acuerdo con una tercera realización de la presente invención.
La figura 7 es un diagrama de bloques que ilustra estructuras de dispositivos de acuerdo con realizaciones de la presente invención.

[Modo de la invención]

La presente invención se refiere a un terminal equipado con un módulo de seguridad interno y se puede aplicar a terminales electrónicos generales tales como un teléfono inteligente, terminal portátil, terminal móvil, PDA (Asistente Digital Personal), terminal de PMP (Reproductor Multimedia Portátil), ordenador portátil, terminal Wibro, TV inteligente, y refrigerador inteligente, y además se aplica a todos los dispositivos o servicios que soportan un módulo de seguridad interno.

La presente invención proporciona un módulo de seguridad interno, servidor que proporciona perfiles, y dispositivo de red que soporta una instalación de perfil para el módulo de seguridad interno.

El módulo de seguridad interno se denomina eSE (Elemento Seguro incorporado), y un ejemplo típico puede ser una eUICC. Las siguientes realizaciones se divulgan principalmente para la eUICC, sin embargo, será claro para los expertos en la técnica que la presente invención puede ser aplicada a diversos tipos de módulo de seguridad interno incluyendo la eUICC. En la presente divulgación, el término "eUICC" puede ser usado de manera intercambiable con un eSIM (Módulo de Identidad de Suscriptor incorporado). La eUICC de acuerdo con diversas realizaciones de la presente invención puede ser instalada en un terminal o añadida al terminal en un tipo desmontable.

Un perfil instalado en un módulo de seguridad interno incluye información de datos tal como una o más aplicaciones, información de autentificación de suscriptor, directorio telefónico almacenado en una UICC. El perfil puede incluir un perfil operativo y un perfil de aprovisionamiento (o perfil de inicialización) de acuerdo con el uso. El perfil operativo está empaquetado en una forma de software, y puede significar información de suscriptor de un terminal servido por una empresa de comunicaciones móviles. El perfil de aprovisionamiento es requerido para conectarse a una cierta red de comunicaciones móviles en un país antes de que un usuario se suscriba a una cierta empresa de comunicaciones, y puede significar un perfil lanzado en una eUICC con antelación. El perfil de aprovisionamiento puede ser usado solo para proporcionar un entorno de conexión de red para descargar un perfil operativo de manera remota y puede incluir la información requerida para conectarse a una cierta red de comunicaciones móviles tal como una IMSI y un valor K.

Un servidor que proporciona perfiles se denomina SM-DP (Preparación de Datos de Gestor de Suscripción), y puede ser usado como significados de entidad fuera de tarjeta de dominio de perfil, servidor de encriptación de perfiles, servidor de generación de perfiles, aprovisionador de perfiles, o proveedor de perfiles.

Un dispositivo de red que soporta la instalación de un perfil en un módulo de seguridad interno puede ser configurado en una forma de servidor incluyendo al menos uno de un dispositivo de encriptación para encriptar o desencriptar un perfil y un dispositivo de almacenamiento para almacenar al menos un perfil. En caso de que el dispositivo de red esté configurado con solo uno del dispositivo de encriptación y el dispositivo de almacenamiento, el dispositivo de red puede ser un dispositivo de encriptación o un dispositivo de almacenamiento en sí mismo. Alternativamente, en caso de que el dispositivo de red esté configurado tanto con el dispositivo de encriptación como con el dispositivo de almacenamiento, el dispositivo de red puede operar como un dispositivo que incluye un dispositivo de encriptación y un dispositivo de almacenamiento o puede ser interpretado como un significado común de incluir un dispositivo de encriptación y un dispositivo de almacenamiento por separado.

El dispositivo de encriptación puede incluir un HSM (Módulo de Seguridad de Hardware) o puede denominarse HSM en sí mismo.

Adicionalmente, se pueden definir y usar diversos términos para una red que soporta una eUICC.

Por ejemplo, como término usado en la presente divulgación, SM-SR (Enrutamiento Seguro de Gestor de Suscripción) puede expresarse como un servidor de gestión de perfiles que toma la función de transmitir un perfil encriptado a una eUICC usando OTA. Adicionalmente, el SM-SR puede expresarse como una entidad fuera de tarjeta de gestor de perfiles de eUICC o un gestor de perfiles.

Adicionalmente, como término usado en la presente divulgación, EID (identificador de eUICC) es un identificador único para distinguir eUICCs instaladas en un terminal, y puede significar una ID de perfil si un perfil de aprovisionamiento está preinstalado en la eUICC, o puede significar una ID de terminal si el terminal y el chip de eUICC (o eSIM) no están separados. Adicionalmente, ID de E-UICC puede indicar un dominio seguro específico de un chip de eSIM.

Adicionalmente, como término usado en la presente divulgación, EIS (Conjunto de Información de eUICC) puede incluir un EID y un ICCID como información de eUICC almacenada en el SM-SR.

Adicionalmente, como término usado en la presente divulgación, EF (Archivo Elemental) puede significar un archivo que almacena información en un perfil de una eUICC que puede almacenar una IMSI y un MSISDN.

Adicionalmente, como término usado en la presente divulgación, MNO (Operador de Red Móvil) puede significar un proveedor de comunicaciones móviles o un sistema del proveedor de comunicaciones móviles.

Adicionalmente, como término usado en la presente divulgación, HSM (Módulo de Seguridad de Hardware) puede significar un módulo para encriptar o desencriptar una clave de contraseña con el fin de no exponer la clave de contraseña.

Los términos específicos que se usan de aquí en adelante se proporcionan para ayudar con el entendimiento la presente invención y pueden modificarse a diversas formas sin apartarse del ámbito técnico de la presente invención.

Los términos y palabras usados en la siguiente descripción y reivindicaciones no están limitados a significados bibliográficos, sino que, son usados simplemente por el inventor para habilitar un entendimiento claro y consecuente de la presente divulgación. Por consiguiente, debería ser evidente para los expertos en la técnica que la siguiente descripción de diversas realizaciones de la presente divulgación se proporciona solamente con propósito de ilustración y no con el propósito de limitar la presente divulgación como se define por las reivindicaciones adjuntas y sus equivalentes.

Debe entenderse que las formas singulares "un", "uno, una", y "el, la" incluyen referentes plurales a menos que el contexto dicte claramente otra cosa. Debe entenderse que los términos tales como "configurar" e "incluir" no siempre incluyen todos los componentes o etapas descritos en la presente divulgación.

De aquí en adelante, se describen en detalle realizaciones de la divulgación con referencia a los dibujos adjuntos. Los mismos símbolos de referencia son usados a lo largo de los dibujos para referirse a las partes iguales o similares. Pueden ser omitidas descripciones detalladas de funciones y estructuras bien conocidas incorporadas en la presente memoria para evitar ocultar la materia objeto de la divulgación. Adicionalmente, los términos descritos de aquí en adelante están definidos considerando funciones en la presente invención y pueden ser cambiados de acuerdo con la intención o práctica de un usuario o un operador. Por lo tanto, los términos deben ser definidos sobre la base del contenido general de la presente divulgación.

La figura 1 ilustra una estructura de una red que soporta una eUICC.

Con referencia a la figura 1, la red que soporta una eUICC puede estar configurada con un terminal 100, servidor 110 de SM, y un MNO 120. El servidor 110 de SM puede estar configurado con un SM-SR 111 y una SM-DP 112.

El terminal 100 incluye una eUICC 102 instalada como un módulo de seguridad interno. La eUICC puede tener un EID como un identificador único, y el EID puede estar indicado como un elemento físico o de software en el terminal 100.

El terminal 100 realiza la comunicación de datos conectándose a una red de comunicaciones móviles que corresponde a al menos un perfil almacenado en la eUICC 102 bajo el control de la unidad 101 de control. En particular, un perfil de aprovisionamiento usado para conectarse a una red temporalmente puede ser almacenado en la eUICC 102 de tal manera que el terminal 100 pueda descargar e instalar un perfil que va a ser usado.

El terminal 100 puede realizar la instalación de perfil activando un evento de instalación de perfil. Con más detalle, el terminal 100 transmite una solicitud para un perfil que incluye un EID al SM-SR 111, y recibe un perfil encriptado con una clave de sesión precompartida con la SM-DP 112 a través de un proceso de autentificación del SM-SR. 111. El terminal 100 se conecta a la red de comunicaciones móviles desencriptando el perfil con la clave de sesión.

En diversas realizaciones, el terminal 100 puede compartir una clave de sesión con la SM-DP 112 usando un procedimiento de autentificación digital. Por ejemplo, el terminal 100 puede recibir un certificado de autentificación digital que corresponde a su propia eUICC 112 desde la SM-DP 112 a través del SM-SR 111, generar una clave de sesión usando el certificado de autentificación digital recibido, y transmitir a la SM-DP 112 encriptando la clave de sesión. La SM-DP 112 puede desencriptar la clave de sesión recibida usando el certificado de autentificación digital y transmitir un perfil para la eUICC 112 que corresponde al certificado de autentificación digital al terminal 100 encriptando con la clave de sesión. En caso de usar el procedimiento de autentificación digital, la SM-DP 112 puede encriptar un perfil usando una clave pública generada con el certificado de autentificación digital, y el terminal 100 puede desencriptar el perfil usando una clave secreta (clave privada) generada con el certificado de autentificación digital. El procedimiento de uso de un certificado de autentificación digital ha sido descrito anteriormente como un ejemplo de uso compartido de una clave de sesión, sin embargo, la presente invención no está limitada a esto y puede usar diversos procedimientos de uso compartido de unos algoritmos de autentificación entre la SM-DP 112 y el terminal 100.

El SM-SR 111 gestiona información de perfil para una pluralidad de terminales. El SM-SR 111 puede transmitir un SMS para descargar un perfil a un MSISDN de la eUICC 102 activando un evento de instalación de perfil. En diversas realizaciones, el SM-SR 111 puede realizar una función de transmisión de una clave de sesión encriptada o un perfil encriptado entre la SM-DP 112 y el terminal 100. El SM-SR 111 puede intercambiar datos con el terminal 100 usando una tecnología OTA verificada. A saber, el SM-SR 111 puede transmitir datos al terminal usando una Clave OTA. El SM-SR 111 puede realizar funciones de gestión de perfiles de activación, desactivación, y eliminación de un perfil después de completar la desencriptación e instalación del perfil en la eUICC 102.

La SM-DP 112 genera un perfil para la eUICC 102 instalada en el terminal 100 y encripta el perfil usando una clave de sesión. Si se recibe una solicitud para instalar un perfil de una cierta eUICC 102, la SM-DP 112 puede transmitir el perfil encriptando con una clave de sesión precompartida con la eUICC 102 correspondiente. Alternativamente, si se recibe una clave de sesión verificada del terminal 100, la SM-DP 112 transmite un perfil encriptado con la clave de sesión correspondiente al terminal 100. La SM-DP 112 puede operar directamente por un MNO 120 o por otras empresas que tengan una perfecta relación de confianza con el MNO 120. De acuerdo con una relación comercial o contractual, la SM-DP 112 puede proporcionar un servicio para uno o más MNOs 120.

Puede existir al menos un MNO 120 en una red. El MNO 120 proporciona un servicio de comunicación para el terminal 100. El MNO 120 puede gestionar la SM-DP 112 y ayudar a una instalación de perfil del terminal usando la SM-DP 112 si un usuario del terminal 100 solicita una suscripción a un servicio. Al menos un MNO 120 puede gestionar SM-DPs 112 separadas de manera individual. Alternativamente, una SM-DP 112 puede proporcionar un servicio para una pluralidad de MNOs 120 de acuerdo con una relación contractual de confianza.

De aquí en adelante, se describirá un procedimiento para instalar un perfil para la eUICC en la red ilustrada por la figura 1.

La figura 2 es un diagrama de flujo que ilustra un procedimiento para instalar un perfil de una eUICC. Aunque no se muestra un flujo de datos del SM-SR 220 2 entre la SM-DP 230 y la eUICC 210 en la figura 2, el SM-SR 220 puede transmitir la información total o parcial para configurar un perfil y una clave de sesión encriptada por la SM-DP 230 a la eUICC 210, o transmitir la información total o parcial para configurar una clave de sesión encriptada por la eUICC 210 a la SM-DP 230.

Con referencia a la figura 2, la eUICC 210 y la SM-DP 230 generan autentificación de eUICC individual y claves de sesión en la etapa 201.

Con más detalle, la SM-DP 230 genera claves de sesión a través de autentificación para cada eUICC 210 distinguida por un EID y genera un perfil usando la clave de sesión generada. La eUICC 210 puede obtener una clave de sesión a través de un proceso de autentificación en tiempo real y desencriptar el perfil encriptado transmitido desde la SM-DP 230 usando la clave de sesión obtenida.

La SM-DP 230 encripta los perfiles para cada eUICC 210 individualmente con las claves de sesión correspondientes en la etapa 203, y transmite los perfiles a las eUICCs 210 en la etapa 205. La eUICC 210 desencripta e instala el perfil

usando la clave de sesión generada en tiempo real a través del proceso de autentificación. Debido a que cada clave de sesión corresponde a cada eUICC 210 una por una, un perfil encriptado por una clave de sesión específica puede ser desencriptado solo por una eUICC 210 específica que corresponde a la clave de sesión.

El proceso anterior se realiza para cada eUICC individualmente cuando la eUICC 210 inicia realmente una instalación de perfil. La SM-DP 230 puede estar equipada con un módulo de encriptación separado para encriptar un perfil, sin embargo, la SM-DP 230 no puede realizar la instalación de perfil correctamente si un gran número de eUICCs solicita la instalación de perfil al mismo tiempo debido a que lleva tiempo para el módulo de encriptación encriptar un perfil. Adicionalmente, si la instalación de perfil se detiene debido a una desconexión de red mientras que se realiza la instalación de perfil individualmente, el perfil no puede ser instalado correctamente para todas las eUICCs 210.

Por consiguiente, puede ser usado un procedimiento eficiente para instalar un perfil almacenando perfiles preencriptados en la SM-DP 230 para un gran número de terminales con antelación de instalar un perfil en la eUICC 210 y transmitir el perfil preencriptado a los terminales cuando se inicia realmente una instalación de perfil. Adicionalmente, se requiere un procedimiento para descargar un perfil de manera independiente de la SM-DP 230 ubicada en una red externa cuando se instala el perfil en la eUICC 210.

De aquí en adelante, se describirá un procedimiento para instalar un perfil que puede proporcionar las características técnicas anteriores de acuerdo con la presente invención.

La figura 3 ilustra una estructura de una red que soporta una eUICC de acuerdo con la presente invención.

Con referencia a la figura 3, la red que soporta una eUICC de acuerdo con la presente invención puede estar configurada con un dispositivo 330 de red que soporta una instalación de perfil de una eUICC.

El dispositivo 330 de red puede estar configurado con al menos uno de un dispositivo 331 de encriptación para encriptar o desencriptar un perfil y un dispositivo 332 de almacenamiento para almacenar al menos un perfil.

El dispositivo 331 de encriptación puede incluir un HSM o puede denominarse HSM en sí mismo, y puede realizar la encriptación y desencriptación de un perfil sin exponer una clave de contraseña.

El dispositivo 332 de almacenamiento almacena al menos un perfil. El dispositivo 332 de almacenamiento puede incluir al menos un medio de un disco duro, RAM (Memoria de Acceso Aleatorio), SRAM (Memoria de Acceso Aleatorio Estático), ROM (Memoria de Solo Lectura), EEPROM (Memoria de Solo Lectura Programable y Borrable Eléctricamente), PROM (Memoria de Solo Lectura Programable), memoria magnética, disco magnético, y disco óptico.

En caso de que el dispositivo 330 de red incluya uno del dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento, el dispositivo 330 de red puede ser el dispositivo 331 de encriptación o el propio dispositivo 332 de almacenamiento. Alternativamente, en caso de que el dispositivo 330 de red incluya tanto el dispositivo 331 de encriptación como el dispositivo 332 de almacenamiento, el dispositivo 330 de red puede operar como un dispositivo que incluye el dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento, o puede ser interpretado como un concepto común de incluir el dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento configurados por separado.

Adicionalmente, el dispositivo 330 de red puede estar configurado con una unidad 333 de comunicación. La unidad 330 de comunicación transmite y recibe datos. Cuando el dispositivo 330 de red opera como un dispositivo que incluye el dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento, la unidad 333 de comunicación puede estar equipada en el dispositivo 330 de red. Por otro lado, cuando el dispositivo 330 de red es interpretado como un concepto común de incluir el dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento configurados por separado, la unidad 333 de comunicación puede ser instalada en cada uno del dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento. En este caso, el dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento pueden intercambiar datos a través de la unidad 333 de comunicación.

El dispositivo 330 de red puede estar configurado en una forma de servidor. Cuando el dispositivo 330 de red opera como un dispositivo que incluye el dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento, el dispositivo 330 de red puede incluir un dispositivo de control separado para controlar el dispositivo 331 de encriptación y el dispositivo 332 de almacenamiento de manera central.

Han sido descritos anteriormente ejemplos de entidades incluidas en una red que soporta una eUICC de acuerdo con la presente invención, sin embargo, se pueden incluir además diversas entidades requeridas para proporcionar e instalar un perfil para una eUICC, y los dispositivos que tienen las mismas o similares funciones pueden estar configurados omitiendo o integrando algunos de ellos. En este caso, las entidades que configuran una red pueden ser modificadas de acuerdo con el ámbito técnico de la presente invención, y si las entidades que configuran la red operan dentro del ámbito técnico de la presente invención, será claro para los expertos en la técnica que las realizaciones correspondientes todavía caen dentro del ámbito de derechos definidos por las reivindicaciones adjuntas.

De aquí en adelante, se describirá con más detalle el procedimiento para instalar un perfil para una eUICC de manera práctica en una red de acuerdo con las realizaciones anteriores de la presente invención.

La figura 4 es un diagrama de flujo que ilustra un procedimiento para instalar un perfil de una eUICC de acuerdo con una primera realización de la presente invención.

Con referencia a la figura 4, en la primera realización de la presente invención, la SM-DP 410 genera un perfil encriptado con una primera clave de contraseña y la primera clave de contraseña encriptada con una segunda clave de contraseña pareada en la etapa 401.

La SM-DP 410 genera perfiles para una pluralidad de eUICCs 430. La SM-DP 410 puede generar una IMSI y un valor K de una clave secreta como información para configurar los perfiles de cada eUICC 430.

La SM-DP 410 encripta cada perfil con una primera clave de contraseña que corresponde a cada perfil. La primera clave de contraseña es una clave aleatoria generada por un HSM instalado en la SM-DP 410, y puede ser una clave simétrica, clave asimétrica, o clave de sesión SCP 03. La primera clave de contraseña es independiente de la eUICC 430 (es decir, no se mapea a un EID), y corresponde a cada perfil uno por uno. Por consiguiente, un perfil encriptado con la primera clave de contraseña no es para una eUICC 430 específica, y puede ser generado en una forma en volumen. La SM-DP 410 puede generar y almacenar un gran número de perfiles encriptados con la primera clave de contraseña en una forma en volumen. La SM-DP 410 encripta y almacena la primera clave de contraseña con una segunda clave de contraseña. La segunda clave de contraseña puede ser una clave simétrica o una clave asimétrica como una clave maestra. Adicionalmente, la segunda clave de contraseña puede ser usada para la autentificación mutua entre la SM-DP 410 y un dispositivo de red usando una clave precompartida.

La SM-DP 410 transmite el perfil encriptado con la primera clave de contraseña y la primera clave de contraseña encriptada con la segunda contraseña pareada al dispositivo 421 de almacenamiento en la etapa 403. El dispositivo 421 de almacenamiento almacena el perfil encriptado con la primera clave de contraseña y la primera clave de contraseña encriptada con la segunda contraseña pareada en la etapa 405 antes de iniciar una instalación de perfil.

Si la instalación de perfil de la eUICC 430 inicia realmente en un cierto momento, un dispositivo 422 de encriptación desencripta la primera clave de contraseña encriptada con la segunda clave de contraseña y encripta la primera clave de contraseña de nuevo con una tercera clave de contraseña en la etapa 407.

La tercera clave de contraseña es una clave electrónica emitida por eUICCs 430 individuales, y puede ser una clave simétrica o una clave asimétrica. La tercera clave de contraseña es generada por un procedimiento de autentificación digital, y puede estar configurada con una clave pública y una clave secreta generadas pareadas de acuerdo con un procedimiento de autentificación precompartido. La tercera clave de contraseña corresponde a una eUICC 430 una por una, y una tercera clave de contraseña correspondiente solo puede ser desencriptada por una eUICC 430 específica.

El dispositivo 422 de encriptación y la eUICC 430 pueden compartir la tercera clave de contraseña en un procedimiento de uso compartido fuera de línea o un procedimiento de comunicación de red antes o después de iniciar una instalación de perfil. En una realización, el dispositivo 422 de encriptación y la eUICC 430 pueden compartir la tercera clave de contraseña en un procedimiento de uso compartido de un certificado de autentificación digital. A saber, el dispositivo 422 de encriptación y la eUICC 430 tienen el mismo certificado de autentificación digital, y de esa manera pueden realizar autentificación mutua (encriptación y desencriptación de datos) usando una clave pública y una clave secreta generadas pareadas a partir de un certificado de autentificación digital correspondiente.

El dispositivo 422 de encriptación transmite la primera clave de contraseña encriptada con la tercera clave de contraseña a la eUICC 430 en la etapa 409. La eUICC 430 almacena la primera clave de contraseña desencriptando con la tercera clave de contraseña precompartida en la etapa 411.

Subsecuentemente, la eUICC 430 recibe un perfil encriptado con una segunda clave de contraseña del dispositivo 421 de almacenamiento en la etapa 413.

En diversas realizaciones, el dispositivo 420 de red puede transmitir la información total o parcial requerida para configurar un perfil encriptado y una primera clave de contraseña a la eUICC 430.

La eUICC 430 instala un perfil correspondiente después de desencriptar el perfil encriptado con la primera clave de contraseña en la etapa 415.

De acuerdo con la primera realización, la SM-DP 410 puede generar un gran número de perfiles encriptados antes de instalar un perfil de una eUICC 430 sin una limitación de tiempo. Adicionalmente, la SM-DP 410 encripta un perfil y una primera clave de contraseña usada para la encriptación del perfil con una clave de contraseña precompartida con el dispositivo 420 de red, y los almacena en el dispositivo 420 de red con antelación. Por lo tanto, puede ser transmitido un perfil a la eUICC 430 sin una sincronización directa con la SM-DP 410 cuando se instala el perfil.

La figura 5 es un diagrama de flujo que ilustra un procedimiento para instalar un perfil de una eUICC de acuerdo con una segunda realización de la presente invención.

Con referencia a la figura 5, en la segunda realización de la presente invención, una SM-DP 510 genera un perfil encriptado con una segunda clave de contraseña en la etapa 501. Aquí, la SM-DP 510 puede ser un servidor que proporciona perfiles de un fabricante de SIM.

La SM-DP 510 genera perfiles para una pluralidad de eUICCs 540. La SM-DP 510 puede generar una IMSI y un valor K de una clave secreta como información para configurar perfiles de cada eUICC 540.

La SM-DP 510 encripta cada perfil con una segunda clave de contraseña. La segunda clave de contraseña es una clave maestra que puede ser una clave simétrica o una clave asimétrica. Adicionalmente, la segunda clave de contraseña puede ser precompartida entre la SM-DP 510 y el dispositivo 520 de red. La segunda clave de contraseña es independiente de la eUICC 540, y puede corresponder a cada perfil uno por uno, o puede ser idéntica para todo el perfil. El perfil encriptado con la segunda clave de contraseña puede ser generado de manera aleatoria sin fijar a una eUICC 540 específica.

La SM-DP 510 transmite el perfil encriptado con la segunda clave de contraseña a un dispositivo 520 de red en la etapa 503. El dispositivo 520 de red desencripta el perfil encriptado con la segunda clave de contraseña en la etapa 505.

Subsecuentemente, el dispositivo 520 de red genera una primera clave de contraseña directamente en la etapa 507. La primera clave de contraseña es generada aleatoriamente por un dispositivo de encriptación instalado en el dispositivo 520 de red, y puede ser una clave simétrica, clave asimétrica, o clave de sesión SCP 03.

El dispositivo 520 de red genera un perfil encriptado con la primera clave de contraseña reencriptando el perfil con la primera clave de contraseña en la etapa 509.

En una realización, el dispositivo 520 de red puede generar un perfil encriptado en una forma de APDU (Unidad de Datos de Protocolo de Aplicación) remota. La APDU remota es una especie de estándar (ETSI TS 102.226) para transmitir un comando encriptado entre un servidor remoto y una eUICC, y se genera cuando se transmiten datos al dividir con una unidad de búfer de conjunto. El dispositivo 520 de red puede generar la APDU remota reencriptando un perfil con la primera clave de contraseña.

El dispositivo 520 de red transmite la primera clave de contraseña y el perfil encriptado con la primera clave de contraseña a una SM-DP 530 en la etapa 511. Aquí, la SM-DP 530 puede ser un servidor que proporciona perfiles de un SIM o un servidor que proporciona perfiles que opera por separado por un fabricante de terminales. La SM-DP 530 puede almacenar un gran número de primeras claves de contraseña y perfiles encriptados con las primeras claves de contraseña antes de iniciar una instalación de perfil.

Si una instalación de perfil de una eUICC 540 inicia realmente en un cierto momento, la SM-DP 530 encripta la primera clave de contraseña con una tercera clave de contraseña en la etapa 513. La tercera clave de contraseña es una clave electrónica emitida por la eUICC 540 y puede ser una clave simétrica o una clave asimétrica. La tercera clave de contraseña se proporciona mediante un procedimiento de autentificación digital, y se pueden generar una clave pública y una clave secreta pareadas de acuerdo con un procedimiento de autentificación precompartido. La tercera clave de contraseña corresponde a cada eUICC 540 una por una, y de esa manera solo puede ser desencriptada por una eUICC específica que corresponde a la tercera clave de contraseña.

La SM-DP 530 y la eUICC 540 pueden compartir la tercera clave de contraseña en un procedimiento de uso compartido fuera de línea o en un procedimiento de comunicación de red antes o después de iniciar una instalación de perfil. En una realización, la SM-DP 530 y la eUICC 540 pueden precompartir la tercera clave de contraseña en un procedimiento de uso compartido de un certificado de autentificación digital. A saber, el dispositivo 530 de encriptación y la eUICC 540 tienen el mismo certificado de autentificación digital, y de esa manera pueden realizar una autentificación mutua (encriptación y desencriptación de datos) usando una clave pública y una clave secreta generadas pareadas a partir del certificado de autentificación digital correspondiente.

La SM-DP 530 transmite la primera clave de contraseña encriptada con la tercera clave de contraseña a la eUICC 540 en la etapa 515. En una realización, la SM-DP 530 puede transmitir la primera clave de contraseña a la eUICC 540 de acuerdo con un Escenario #1 de CCCM. El Escenario #1 es uno de tecnologías de memoria descriptiva de plataforma global para encriptar y transmitir una clave de sesión, y se puede realizar transmitiendo una primera clave de contraseña a través de una comunicación directa entre la SM-DP 530 y la eUICC 540 que corresponde a una solicitud para una primera clave de contraseña (o transmisión de una primera clave de contraseña) y responder a la primera clave de contraseña.

La eUICC 540 almacena la primera clave de contraseña desencriptando la primera clave de contraseña con una tercera clave de contraseña precompartida en la etapa 517.

Subsecuentemente, la eUICC 540 realiza una instalación de perfil en base a una APDU remota de la SM-DP 530 en la etapa 519. La eUICC 540 recibe una APDU remota generada encriptando con una primera clave de contraseña de la SM-DP 530, y obtiene un perfil desencriptando la APDU remota con la primera clave de contraseña. Por consiguiente, la eUICC 540 puede instalar el perfil obtenido.

De acuerdo con la segunda realización, la SM-DP 510 puede prealmacenar un gran número de perfiles encriptados generados por un dispositivo de red con antelación de iniciar una instalación de perfil de una eUICC 540 sin una limitación de tiempo. Adicionalmente, la SM-DP 540 habilita una instalación de perfil con menos influencia en un estado de red aprovisionando un perfil encriptado y una primera clave de contraseña usada para la encriptación en base a la APDU remota.

En comparación con la primera realización, la segunda realización puede ser distinguida de la primera realización en el hecho de que el cuerpo principal de generar una primera clave de contraseña y desencriptar un perfil con la primera clave de contraseña se cambia de una SM-DP a un dispositivo de red. Adicionalmente, la segunda realización puede ser distinguida de la primera realización en el hecho de que el cuerpo principal de transmitir un perfil encriptado se cambia de un dispositivo de red a una SM-DP. Por consiguiente, la segunda realización tiene una diferencia de la primera realización en el hecho de que se usa un Escenario #1 de CCCM cuando se transmite una primera clave de contraseña encriptada con una tercera clave de contraseña y se realiza una instalación de perfil en base a una APDU remota.

La figura 6 es un diagrama de flujo que ilustra un procedimiento para instalar un perfil de una eUICC de acuerdo con una tercera realización de la presente invención.

Con referencia a la figura 6, en la tercera realización de la presente invención, la SM-DP 610 genera un perfil encriptado con una primera clave de contraseña en la etapa 601.

La SM-DP 610 genera perfiles para una pluralidad de eUICCs 630. La SM-DP 610 puede generar una IMSI y un valor K de una clave secreta de cada eUICC 630 como información para configurar los perfiles de cada eUICC 630.

La SM-DP 610 encripta cada perfil con una primera clave de contraseña que corresponde a cada perfil. La primera clave de contraseña es generada aleatoriamente por un HSM instalado en la SM-DP 610, y puede ser una clave simétrica, clave asimétrica, o clave de sesión SCP 03. La primera clave de contraseña es independiente de la eUICC 630 y corresponde a cada perfil uno por uno. Por consiguiente, un perfil encriptado con la primera clave de contraseña no es para una eUICC 650 específica y se genera de una forma en volumen. La SM-DP 610 puede generar y almacenar un gran número de perfiles encriptados con la primera clave de contraseña de una forma en volumen.

La SM-DP 610 transmite el perfil encriptado con la contraseña a un dispositivo 620 de red en la etapa 603. El dispositivo 620 de red almacena el perfil encriptado con la primera contraseña en la etapa 605 con antelación de iniciar una instalación de perfil.

Si una instalación de perfil de una eUICC 630 inicia realmente en un cierto momento, el dispositivo 620 de red determina al menos una eUICC que va a ser instalada con un perfil en la etapa 607. El dispositivo 620 de red puede identificar una eUICC 640 activada por un evento de instalación de perfil de acuerdo con una condición predeterminada o una solicitud de la eUICC 630 o un MNO, y determinar al menos una eUICC que va a ser instalada con un perfil en base al resultado de identificación.

El dispositivo 620 de red transmite información (lista) relacionada con al menos una eUICC que va a ser instalada con un perfil a la SM-DP 610 en la etapa 609. La información relacionada con al menos una eUICC que va a ser instalada con un perfil puede incluir un identificador (EID) de una eUICC correspondiente, identificador de un perfil que va a ser instalado en la eUICC correspondiente, y certificado de autentificación de la eUICC correspondiente.

Si la información relacionada con al menos una eUICC se recibe de la eUICC, la SM-DP 610 encripta la primera clave de contraseña con una tercera clave de contraseña en la etapa 611. La tercera clave de contraseña es una clave electrónica emitida por una eUICC 630, y puede ser una clave simétrica o una clave asimétrica. La tercera clave de contraseña se proporciona en un procedimiento de autentificación digital, y puede estar configurada con una clave pública y una clave secreta generadas pareadas de acuerdo con un procedimiento de autentificación precompartido. La tercera clave de contraseña corresponde a una eUICC 630 una por una, y de esa manera puede ser usada para desencriptación solamente en una eUICC específica que corresponde a una tercera clave de contraseña.

La SM-DP 610 y la eUICC 630 pueden compartir la tercera clave de contraseña en un procedimiento de uso compartido fuera de línea o en un procedimiento de comunicación de red antes o después de iniciar una instalación de perfil. En una realización, la SM-DP 610 y la eUICC 630 pueden precompartir la tercera clave de contraseña en un procedimiento de uso compartido de un certificado de autentificación digital. A saber, el dispositivo 610 de encriptación y la eUICC 630 tienen el mismo certificado de autentificación digital, y de esa manera pueden realizar autentificación mutua (encriptación y desencriptación de datos) usando una clave pública y una clave secreta generadas pareadas a partir del certificado de autentificación digital correspondiente. En diversas realizaciones, la primera clave de contraseña encriptada con la tercera clave de contraseña puede ser transmitida desde la SM-DP 610 a la eUICC 630 directamente.

La SM-DP 610 transmite la primera clave de contraseña encriptada con la tercera clave de contraseña al dispositivo 620 de red en la etapa 613. El dispositivo 620 de red transmite una segunda clave de contraseña encriptada a la eUICC 630 en la etapa 615. Adicionalmente, el dispositivo 620 de red transmite un perfil encriptado con la primera clave de contraseña a la eUICC 630 en la etapa 617.

La eUICC 630 obtiene la primera clave de contraseña desencriptando la primera clave de contraseña encriptada con la tercera clave de contraseña en la etapa 619, e instala un perfil correspondiente después de desencriptar el perfil con la primera clave de contraseña obtenida en la etapa 621.

De acuerdo con la tercera realización, el dispositivo 620 de red puede prealmacenar un gran número de perfiles encriptados generados por la SM-DP 610 sin una limitación de tiempo con antelación de iniciar una instalación de perfil de la eUICC 630.

En comparación con la primera realización, la tercera realización es distinguida de la primera realización en el hecho de que la transmisión de una primera clave de contraseña encriptada se realiza solamente para una eUICC solicitada por el dispositivo de red después de iniciar una instalación de perfil.

De aquí en adelante, se describirá una configuración de un dispositivo que opera de acuerdo con las realizaciones de la presente invención.

La figura 7 es un diagrama de bloques que ilustra estructuras de dispositivos de acuerdo con realizaciones de la presente invención.

Con referencia a la figura 7, una SM-DP 700 de acuerdo con una realización de la presente invención puede estar configurada con una unidad 701 de comunicación, unidad 702 de control, y unidad 703 de encriptación.

La unidad 701 de comunicación puede transmitir y recibir datos hacia/desde otros dispositivos. La unidad 701 de comunicación puede transmitir y recibir una clave encriptada y un perfil encriptado. Para esto, la unidad 701 de comunicación puede incluir al menos un módulo de comunicación y una antena.

La unidad 702 de control puede controlar cada componente de la SM-DP 700 para instalar un perfil de acuerdo con la presente invención. Las operaciones detalladas de la unidad 702 de control son las mismas que la descripción anterior.

La unidad 703 de encriptación realiza la encriptación o desencriptación de una clave o un perfil de acuerdo con el control de la unidad 702 de control. La unidad 703 de encriptación puede ser instalada en la unidad 702 de control o proporcionada en una forma de código de software accionada por la unidad 702 de control.

Con referencia a la figura 7, un dispositivo 710 de red de acuerdo con una realización de la presente invención puede estar configurado con un dispositivo 711 de comunicación, dispositivo 712 de encriptación, y dispositivo 713 de almacenamiento.

El dispositivo 711 de comunicación puede transmitir o recibir datos hacia/desde otros dispositivos. El dispositivo 711 de comunicación puede transmitir o recibir una clave encriptada o un perfil encriptado. Para esto, el dispositivo 711 de comunicación puede incluir al menos un módulo de comunicación y una antena.

En diversas realizaciones, si el dispositivo 710 de red opera como un dispositivo que incluye el dispositivo 712 de encriptación y el dispositivo 713 de almacenamiento, el dispositivo 711 de comunicación puede ser instalado en el dispositivo 710 de red. Alternativamente, si el dispositivo 710 de red es interpretado como un concepto común de incluir el dispositivo 712 de encriptación y el dispositivo 713 de almacenamiento configurados por separado, el dispositivo 711 de comunicación puede ser instalado en el dispositivo 712 de encriptación y el dispositivo 713 de almacenamiento de manera individual. En este caso, el dispositivo 712 de encriptación y el dispositivo 713 de almacenamiento pueden transmitir y recibir datos entre sí a través del dispositivo 711 de comunicación.

El dispositivo 712 de encriptación puede incluir un HSM o denominado HSM en sí mismo, y puede realizar la encriptación y desencriptación sin exponer una clave de contraseña.

El dispositivo 713 de almacenamiento almacena al menos un perfil. El dispositivo 713 de almacenamiento puede incluir al menos un medio de un disco duro, RAM (Memoria de Acceso Aleatorio), SRAM (Memoria de Acceso Aleatorio Estático), ROM (Memoria de Solo Lectura), EEPROM (Memoria de Solo Lectura Programable y Borrable Eléctricamente), PROM (Memoria de Solo Lectura Programable), memoria magnética, disco magnético, y disco óptico.

El dispositivo 710 de red puede estar configurado en una forma de servidor. En caso de que el dispositivo 710 de red opere como un dispositivo que incluye un dispositivo 712 de encriptación y un dispositivo 713 de almacenamiento, el dispositivo 710 de red puede incluir un dispositivo de control separado para controlar el dispositivo 712 de encriptación y el dispositivo 713 de almacenamiento de manera central.

Con referencia a la figura 7, un terminal 720 de acuerdo con una realización de la presente invención puede estar configurado con una unidad 721 de comunicación, unidad 722 de control, y eUICC 723.

La unidad 721 de comunicación puede transmitir o recibir hacia/desde otros dispositivos. La unidad 721 de comunicación puede recibir una clave encriptada y un perfil encriptado. Para esto, la unidad 721 de comunicación puede incluir al menos un módulo de comunicación y una antena.

La unidad 722 de control puede controlar cada componente del terminal 720 para instalar un perfil de acuerdo con la presente invención. Las operaciones detalladas de la unidad 722 de control son las mismas que la descripción anterior.

Una eUICC 723 es un chip de UICC instalado en el terminal 720, y realiza funciones de almacenamiento, gestión, y eliminación de al menos un perfil. El perfil incluye información de datos tales como una o más aplicaciones, información de autentificación de suscriptor, y agenda telefónica.

Las realizaciones anteriores de la presente invención ilustradas por los dibujos adjuntos han sido sugeridas para un entendimiento más fácil de la presente invención y no limitan el ámbito de la presente invención. Adicionalmente, será entendido por los expertos en la técnica que se pueden hacer diversos cambios en forma y detalles en la misma sin apartarse del ámbito de la presente divulgación como se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento de instalación de un perfil de una Tarjeta de Circuito Integrado Universal incorporada, eUICC, realizado por un dispositivo (330, 420, 710) de red, comprendiendo el procedimiento:

adquirir, de un servidor (410, 510, 700) de Preparación de Datos de Gestor de Suscripción, SM-DP, al menos un perfil encriptado con una primera clave de contraseña y una primera clave de contraseña encriptada que está encriptada con una segunda clave de contraseña; desencriptar la primera clave de contraseña encriptada encriptada con la segunda clave de contraseña y reencriptar la primera clave de contraseña con una tercera clave de contraseña; y
transmitir, a al menos una eUICC, el al menos un perfil encriptado y la primera clave de contraseña encriptada que está reencriptada con una tercera clave de contraseña en base al inicio de una instalación de perfil para la al menos una eUICC,
en el que el al menos un perfil encriptado es desencriptado por la primera clave de contraseña e instalado en la al menos una eUICC, respectivamente.

2. El procedimiento de la reivindicación 1, en el que la adquisición comprende:
recibir el al menos un perfil encriptado con la primera clave de contraseña y la primera clave de contraseña encriptada que está encriptada con la segunda clave de contraseña del servidor (410, 510, 700) de Preparación de Datos de Gestor de Suscripción, SM-DP, y en el que la transmisión comprende:

desencriptar la primera clave de contraseña encriptada que está encriptada con la segunda clave de contraseña;
reencriptar la primera clave de contraseña desencriptada con la tercera clave de contraseña; y
transmitir la primera clave de contraseña encriptada que está encriptada con la tercera clave de contraseña y el al menos un perfil encriptado con la primera clave de contraseña a la al menos una eUICC.

3. El procedimiento de la reivindicación 2,
en el que la transmisión comprende:

transmitir una lista de eUICC para instalar perfiles a la SM-DP;
recibir la primera clave de contraseña encriptada con la tercera clave de contraseña de la SM-DP; y
transmitir la primera clave de contraseña encriptada que está encriptada con la tercera clave de contraseña y el al menos un perfil encriptado con la primera clave de contraseña a la al menos una eUICC incluida en la lista de eUCC.

4. El procedimiento de la reivindicación 1, en el que la primera clave de contraseña es una clave aleatoria generada para encriptar al menos un perfil que corresponde a al menos un perfil, y
en el que la tercera clave de contraseña es una clave de sesión generada para encriptar la primera clave de contraseña que corresponde a la al menos una eUICC.

5. Un procedimiento para habilitar la instalación de un perfil de una Tarjeta de Circuito Integrado Universal incorporada, eUICC, realizada por un servidor (410, 510, 700) de Preparación de Datos de Gestor de Suscripción, SM-DP, comprendiendo el procedimiento: generar (401) y transmitir (403), a un dispositivo (330, 420, 710) de red, al menos un perfil encriptado con una primera clave de contraseña y una primera clave de contraseña encriptada que está encriptada con una segunda clave de contraseña.

6. El procedimiento de la reivindicación 5, en el que la primera clave de contraseña es una clave aleatoria generada para encriptar al menos un perfil que corresponde a al menos un perfil.

7. Un dispositivo (330, 420, 710) de red para instalar un perfil de una Tarjeta de Circuito Integrado Universal incorporada, eUICC, comprendiendo el dispositivo de red:

una unidad (333, 711) de comunicación; y
un dispositivo (331, 332, 712, 713) de control configurado para controlar para:

adquirir, de un servidor (410, 510, 700) de Preparación de Datos de Gestor de Suscripción, SM-DP, al menos un perfil encriptado con una primera clave de contraseña y una primera clave de contraseña encriptada que está encriptada con una segunda clave de contraseña,
desencriptar la primera clave de contraseña encriptada encriptada con la segunda clave de contraseña y reencriptar la primera clave de contraseña con una tercera clave de contraseña; y
transmitir, a al menos una eUICC, el al menos un perfil encriptado y la primera clave de contraseña encriptada que está reencriptada con una tercera clave de contraseña en base al inicio de una instalación de perfil para la al menos una eUICC,

en el que el al menos un perfil encriptado es instalado en la al menos una eUICC desencriptando con la primera clave de contraseña.

8. El dispositivo de red de la reivindicación 7, en el que el dispositivo de control está configurado para controlar para:

recibir el al menos un perfil encriptado con la primera clave de contraseña y la primera clave de contraseña encriptada que está encriptada con la segunda clave de contraseña del servidor (410, 510, 700) de Preparación de Datos de Gestor de Suscripción, SM-DP,
desencriptar la primera clave de contraseña encriptada que está encriptada con la segunda clave de contraseña,
reencriptar la primera clave de contraseña desencriptada con la tercera clave de contraseña; y
transmitir la primera clave de contraseña encriptada que está encriptada con la tercera clave de contraseña y el al menos un perfil encriptado con la primera clave de contraseña a la al menos una eUICC.

9. El dispositivo de red de la reivindicación 8, en el que el dispositivo de control está configurado para controlar para:

transmitir una lista de eUICC para instalar perfiles a la SM-DP,
recibir la primera clave de contraseña encriptada con la tercera clave de contraseña de la SM-DP, y
transmitir la primera clave de contraseña encriptada que está encriptada con la tercera clave de contraseña y el al menos un perfil encriptado con la primera clave de contraseña a la al menos una eUICC incluida en la lista de eUICC.

10. El dispositivo de red de la reivindicación 7, en el que la primera clave de contraseña es una clave aleatoria generada para encriptar al menos un perfil que corresponde a al menos un perfil, y
en el que la tercera clave de contraseña es una clave de sesión generada para encriptar la primera clave de contraseña que corresponde a la al menos una eUICC.

11. Un servidor (410, 510, 700) de Preparación de Datos de Gestor de Suscripción, SM-DP, para habilitar la instalación de un perfil de una Tarjeta de Circuito Integrado Universal incorporada, eUICC, comprendiendo el servidor de SM-DP:

una unidad de comunicación; y
una unidad de control configurada para controlar para: generar (401) y transmitir (403), a un dispositivo (330, 420, 710) de red al menos un perfil encriptado con una primera clave de contraseña y una primera clave de contraseña encriptada que está encriptada con una segunda clave de contraseña.

12. El servidor de SM-DP de la reivindicación 11, en el que la primera clave de contraseña es una clave aleatoria generada para encriptar al menos un perfil que corresponde a al menos un perfil.

FIG. 1

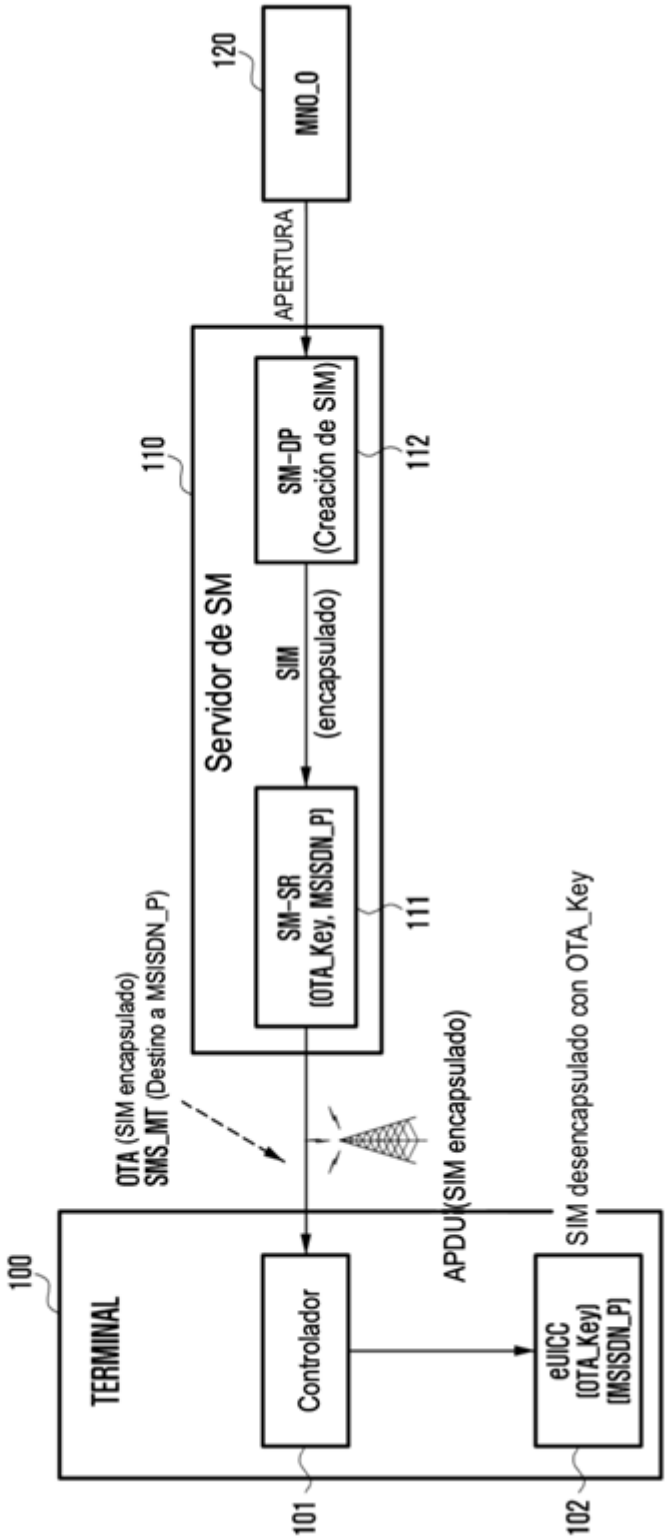

120
MNO_O
APERTURA
110
Servidor de SM
SM-DP
(Creación de SIM)
112
SIM
(encapsulado)
SM-SR
[OTA_Key, MSISDN_P]
111
OTA (SIM encapsulado)
SMS_MT (Destino a MSISDN_P)
APDU(SIM encapsulado)
SIM desencapsulado con OTA_Key
100
TERMINAL
Controlador
eUICC
[OTA_Key]
[MSISDN_P]
101
102

FIG. 2

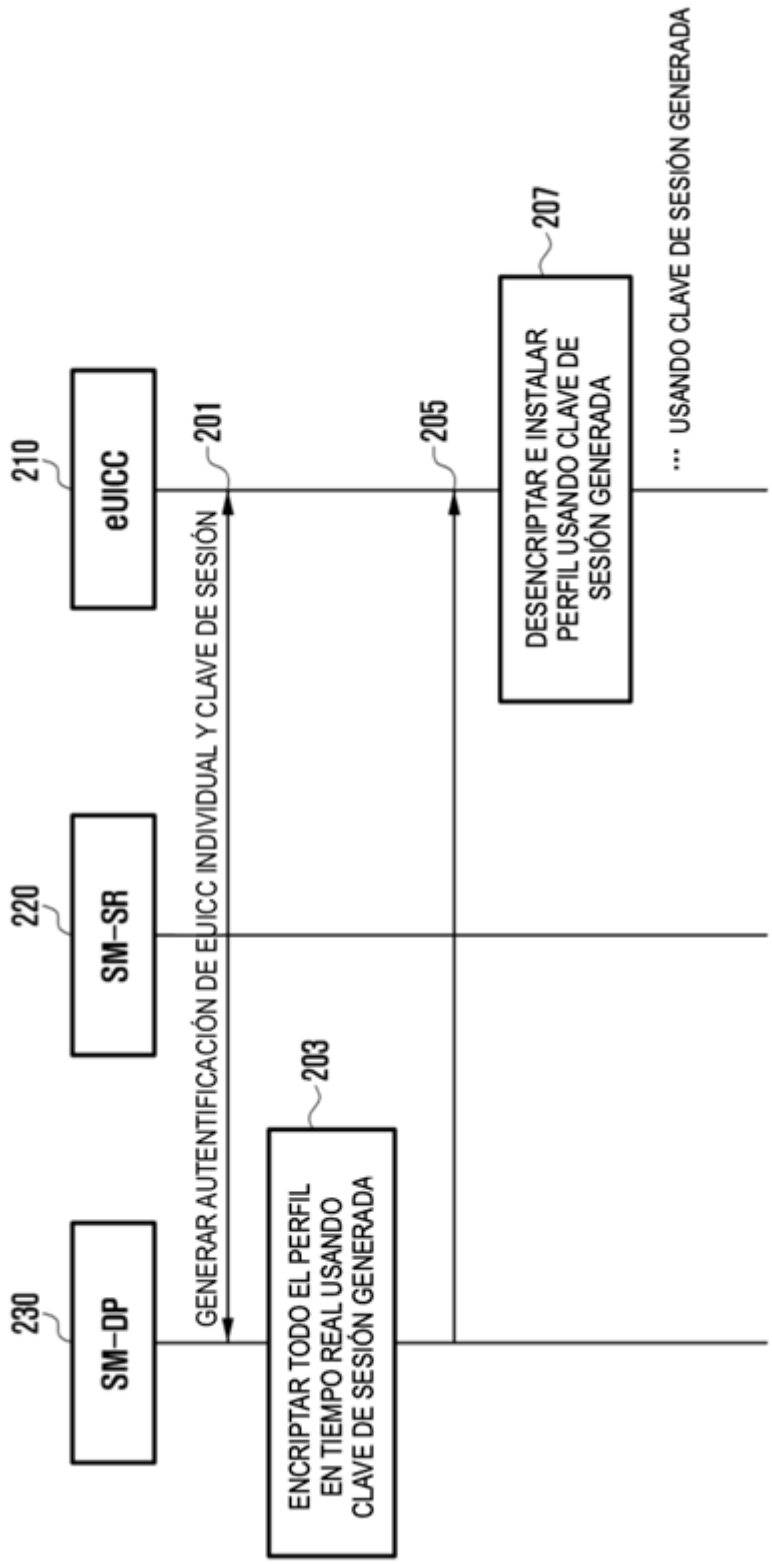

210
eUICC
201
205
207
... USANDO CLAVE DE SESIÓN GENERADA
DESENCRIPTAR E INSTALAR PERFIL USANDO CLAVE DE SESIÓN GENERADA
220
SM-SR
GENERAR AUTENTIFICACIÓN DE EUICC INDIVIDUAL Y CLAVE DE SESIÓN
203
230
SM-DP
ENCRIPTAR TODO EL PERFIL EN TIEMPO REAL USANDO CLAVE DE SESIÓN GENERADA

FIG. 3

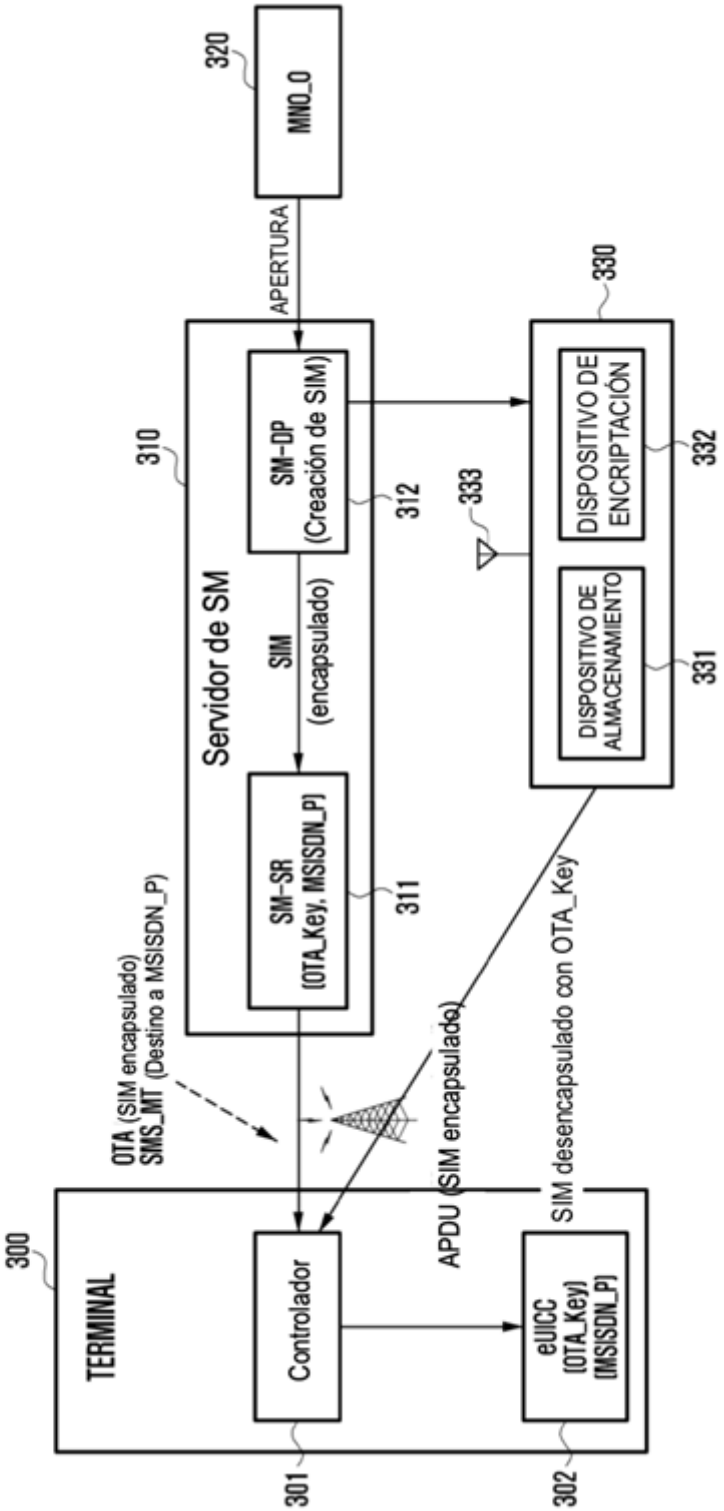

320
MNO_0
APERTURA
330
310
SM-DP
(Creación de SIM)
312
333
DISPOSITIVO DE
ENCRIPTACIÓN
332
Servidor de SM
SIM
(encapsulado)
DISPOSITIVO DE
ALMACENAMIENTO
331
SM-SR
(OTA_Key, MSISDN_P)
311
OTA (SIM encapsulado)
SMS_MT (Destino a MSISDN_P)
APDU (SIM encapsulado)
SIM desencapsulado con OTA_Key
300
TERMINAL
Controlador
eUICC
(OTA_Key)
(MSISDN_P)
301
302

FIG. 4

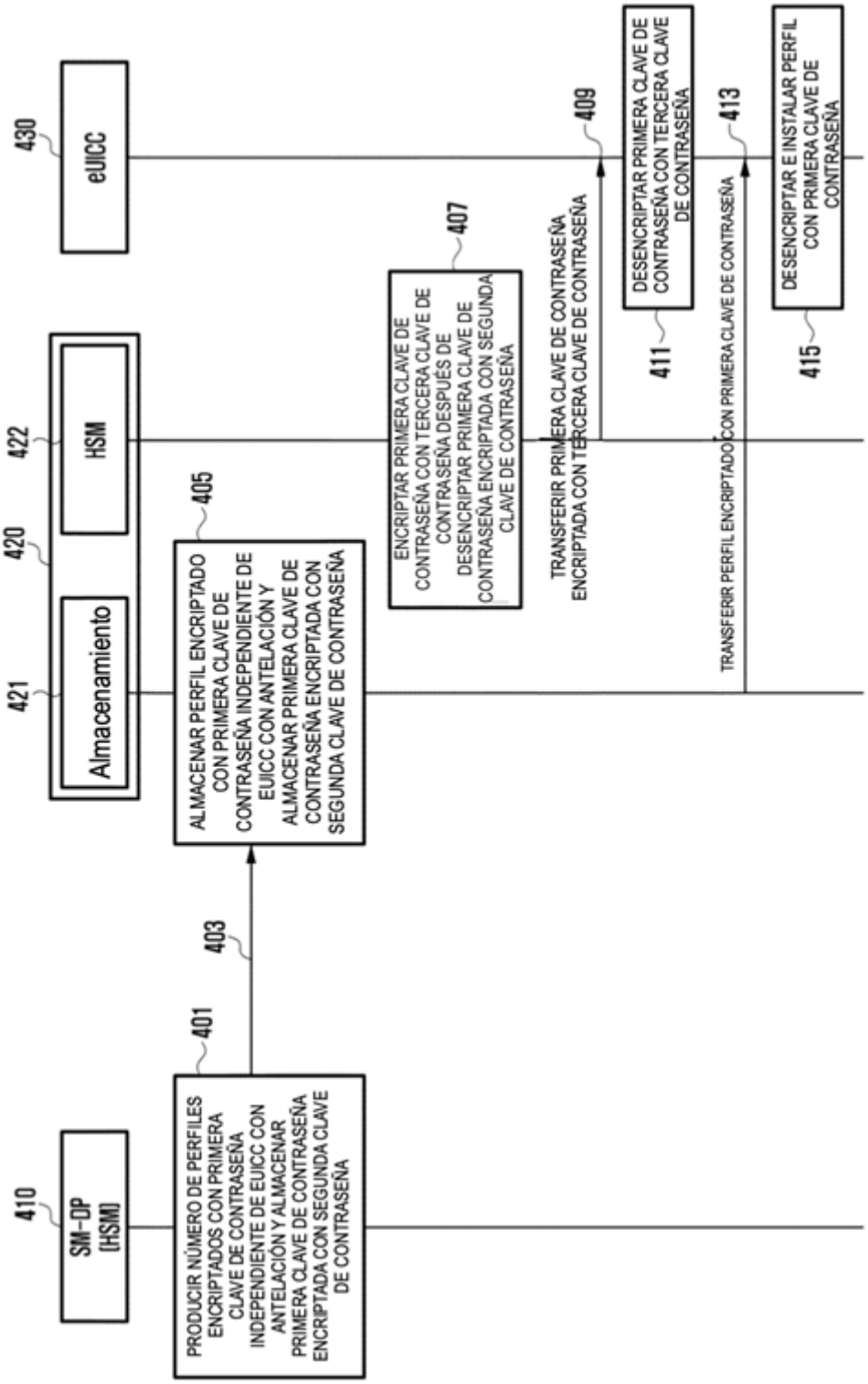

410
SM-DP (HSM)
PRODUCIR NÚMERO DE PERFILES ENCRIPTADOS CON PRIMERA CLAVE DE CONTRASEÑA INDEPENDIENTE DE EUICC CON ANTELACIÓN Y ALMACENAR PRIMERA CLAVE DE CONTRASEÑA ENCRIPTADA CON SEGUNDA CLAVE DE CONTRASEÑA
401
403
420
421
Almacenamiento
422
HSM
ALMACENAR PERFIL ENCRIPTADO CON PRIMERA CLAVE DE CONTRASEÑA INDEPENDIENTE DE EUICC CON ANTELACIÓN Y ALMACENAR PRIMERA CLAVE DE CONTRASEÑA ENCRIPTADA CON SEGUNDA CLAVE DE CONTRASEÑA
405
ENCRIPTAR PRIMERA CLAVE DE CONTRASEÑA CON TERCERA CLAVE DE CONTRASEÑA DESPUÉS DE DESENCRIPTAR PRIMERA CLAVE DE CONTRASEÑA ENCRIPTADA CON SEGUNDA CLAVE DE CONTRASEÑA
407
TRANSFERIR PRIMERA CLAVE DE CONTRASEÑA ENCRIPTADA CON TERCERA CLAVE DE CONTRASEÑA
409
430
eUICC
DESENCRIPTAR PRIMERA CLAVE DE CONTRASEÑA CON TERCERA CLAVE DE CONTRASEÑA
411
TRANSFERIR PERFIL ENCRIPTADO CON PRIMERA CLAVE DE CONTRASEÑA
413
DESENCRIPTAR E INSTALAR PERFIL CON PRIMERA CLAVE DE CONTRASEÑA
415

FIG. 5

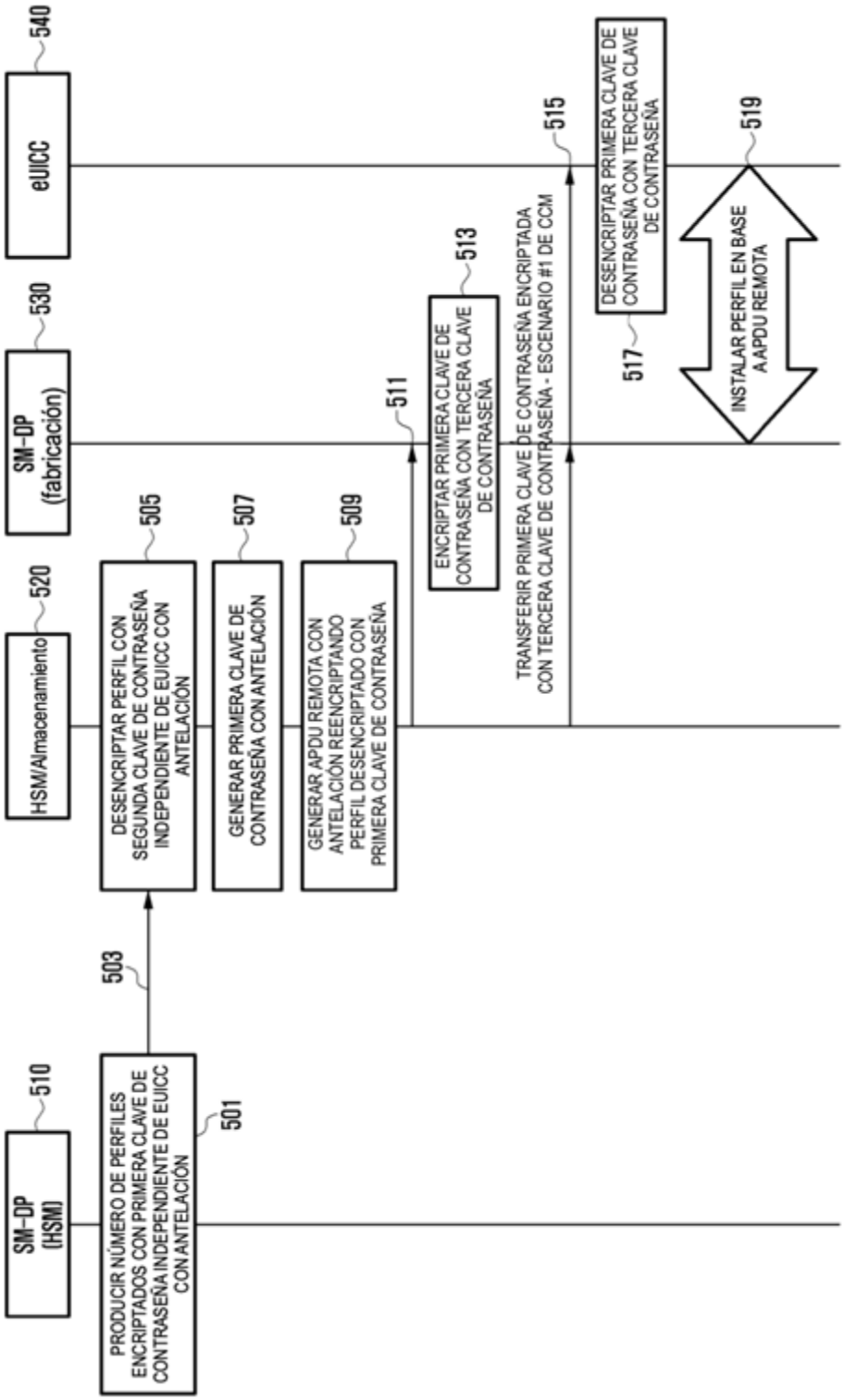

SM-DP (HSM)
510
PRODUCIR NÚMERO DE PERFILES ENCRIPTADOS CON PRIMERA CLAVE DE CONTRASEÑA INDEPENDIENTE DE EUICC CON ANTELACIÓN
501
503
HSM/Almacenamiento
520
DESENCRIPTAR PERFIL CON SEGUNDA CLAVE DE CONTRASEÑA INDEPENDIENTE DE EUICC CON ANTELACIÓN
505
GENERAR PRIMERA CLAVE DE CONTRASEÑA CON ANTELACIÓN
507
GENERAR APDU REMOTA CON ANTELACIÓN REENCRIPTANDO PERFIL DESENCRIPTADO CON PRIMERA CLAVE DE CONTRASEÑA
509
SM-DP (fabricación)
530
511
ENCRIPTAR PRIMERA CLAVE DE CONTRASEÑA CON TERCERA CLAVE DE CONTRASEÑA
513
TRANSFERIR PRIMERA CLAVE DE CONTRASEÑA ENCRIPTADA CON TERCERA CLAVE DE CONTRASEÑA - ESCENARIO #1 DE CCM
515
eUICC
540
DESENCRIPTAR PRIMERA CLAVE DE CONTRASEÑA CON TERCERA CLAVE DE CONTRASEÑA
517
INSTALAR PERFIL EN BASE A APDU REMOTA
519

FIG. 6

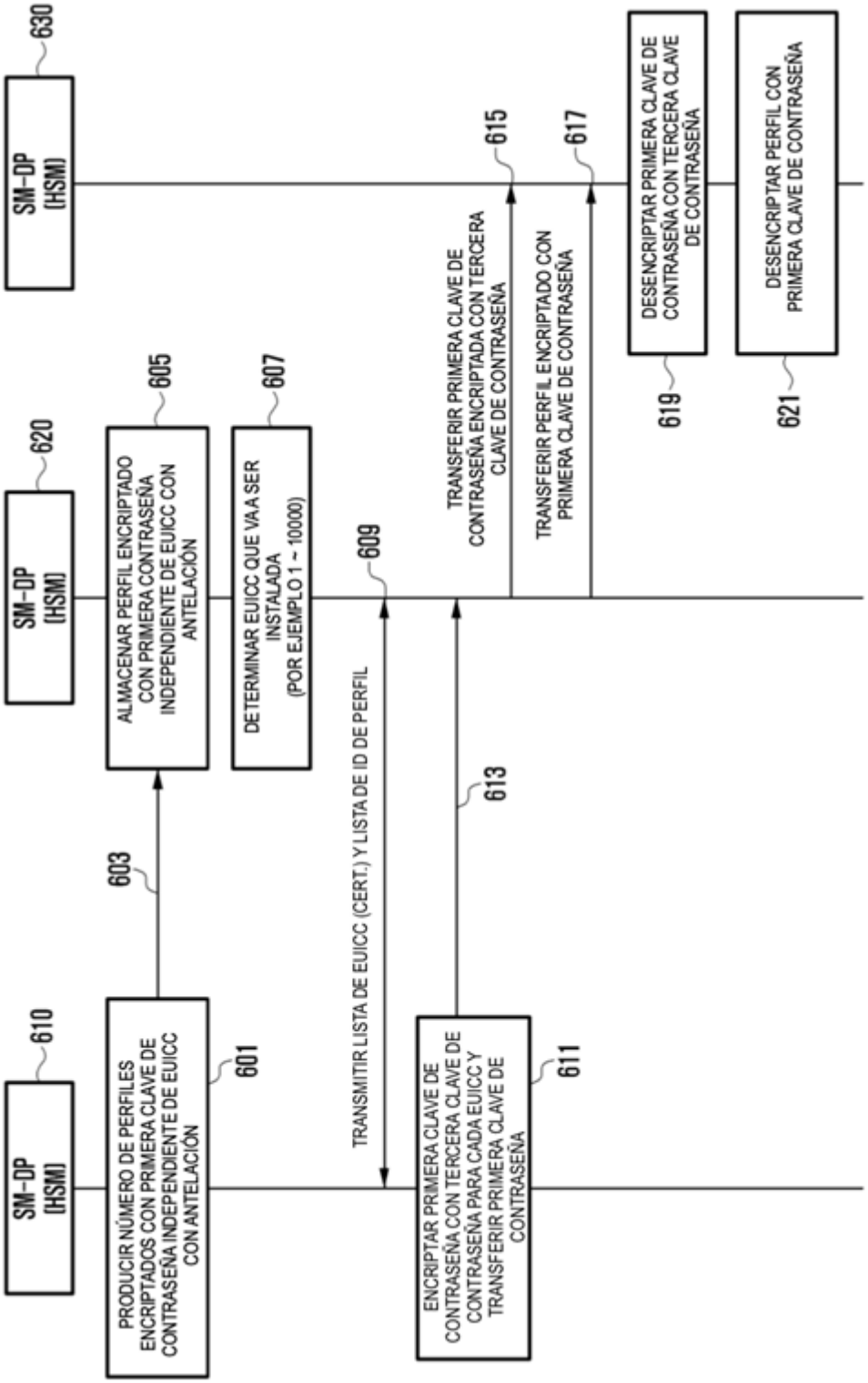
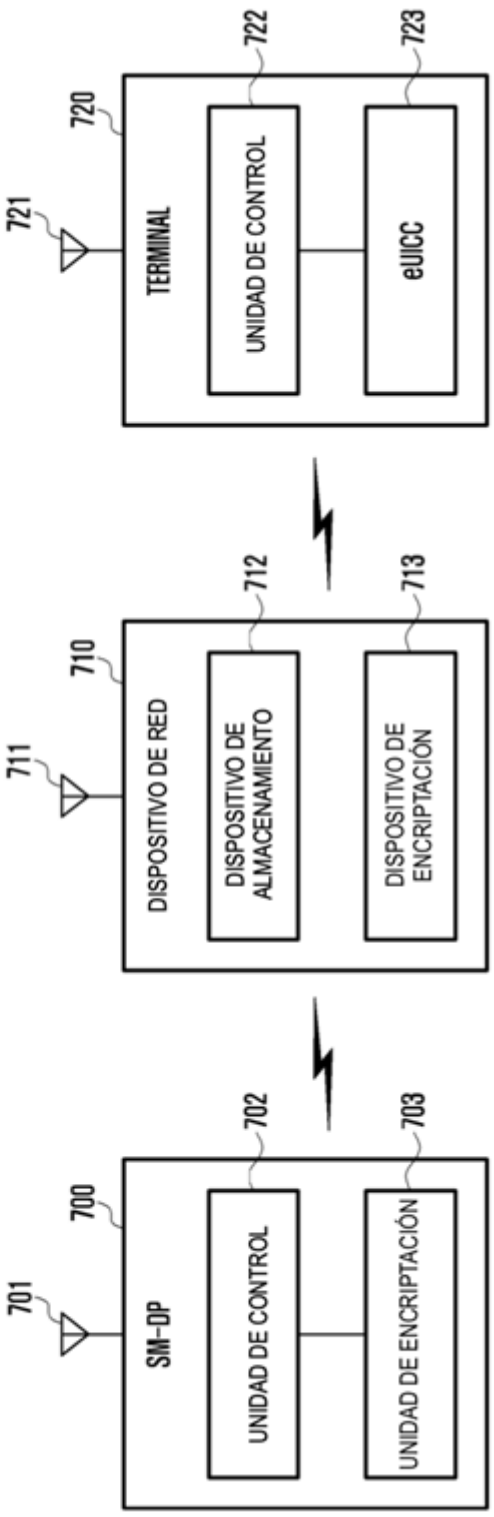

SM-DP (HSM)
610
PRODUCIR NÚMERO DE PERFILES ENCRIPTADOS CON PRIMERA CLAVE DE CONTRASEÑA INDEPENDIENTE DE EUICC CON ANTELACIÓN
601
603
SM-DP (HSM)
620
ALMACENAR PERFIL ENCRIPTADO CON PRIMERA CONTRASEÑA INDEPENDIENTE DE EUICC CON ANTELACIÓN
605
DETERMINAR EUICC QUE VAA SER INSTALADA (POR EJEMPLO 1 ~ 10000)
607
609
TRANSMITIR LISTA DE EUICC (CERT.) Y LISTA DE ID DE PERFIL
ENCRIPTAR PRIMERA CLAVE DE CONTRASEÑA CON TERCERA CLAVE DE CONTRASEÑA PARA CADA EUICC Y TRANSFERIR PRIMERA CLAVE DE CONTRASEÑA
611
613
SM-DP (HSM)
630
TRANSFERIR PRIMERA CLAVE DE CONTRASEÑA ENCRIPTADA CON TERCERA CLAVE DE CONTRASEÑA
615
TRANSFERIR PERFIL ENCRIPTADO CON PRIMERA CLAVE DE CONTRASEÑA
617
DESENCRIPTAR PRIMERA CLAVE DE CONTRASEÑA CON TERCERA CLAVE DE CONTRASEÑA
619
DESENCRIPTAR PERFIL CON PRIMERA CLAVE DE CONTRASEÑA
621

FIG. 7


701
700
SM-DP
UNIDAD DE CONTROL
702
UNIDAD DE ENCRIPTACIÓN
703
711
710
DISPOSITIVO DE RED
DISPOSITIVO DE ALMACENAMIENTO
712
DISPOSITIVO DE ENCRIPTACIÓN
713
721
720
TERMINAL
UNIDAD DE CONTROL
722
eUICC
723