(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 708 696**

(51) Int. CI.:

H04W 8/20 (2009.01)
H04W 12/08 (2009.01)
H04W 48/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.07.2012 PCT/KR2012/005377**

(87) Fecha y número de publicación internacional: **17.01.2013 WO13009044**

(96) Fecha de presentación y número de la solicitud europea: **06.07.2012 E 12811331 (3)**

(97) Fecha y número de publicación de la concesión europea: **07.11.2018 EP 2731381**

(54) Título: **Método para el cambio del operador de red móvil en una SIM integrada basado en un privilegio especial**

(30) Prioridad:

08.07.2011 KR 20110067779
21.10.2011 KR 20110107916

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.04.2019

(73) Titular/es:

KT CORPORATION (100.0%)
206 Jeongja-dong Bundang-gu
Seongnam-si, Gyeonggi-do 463-815, KR

(72) Inventor/es:

PARK, JAEMIN;
LEE, JINHYOUNG y
LEE, KWANGWUK

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método para el cambio del operador de red móvil en una SIM integrada basado en un privilegio especial

Campo anterior

La presente invención se refiere a un método de cambio de un operador de red móvil (MNO) en un módulo de identidad de abonado integrado (de aquí en adelante, denominado como un “eSIM” o “eUICC”) basado en un privilegio y un eSIM para el mismo.

Técnica antecedente

Una tarjeta de circuito integrado universal (UICC) es una pequeña tarjeta insertada en un terminal y usada como un módulo de autenticación del usuario. La UICC puede almacenar información personal sobre un usuario e información sobre un operador de la red móvil de un servicio móvil suscrito por el usuario. Por ejemplo, la UICC puede incluir una Identidad de Abonado Móvil Internacional (IMSI) para identificar un usuario. La UICC puede denominarse también como una tarjeta de Módulo de Identidad de Abonado (SIM) en el Sistema Global para Comunicaciones Móviles (GSM), y como un Módulo de Identidad de Abonado Universal (USIM) en el Acceso Múltiple por División de Código de Banda Ancha (WCDMA).

Cuando el usuario instala la UICC en un terminal de usuario, se consigue automáticamente la autenticación del usuario usando la información almacenada en la UICC, permitiendo al usuario usar convenientemente el terminal. Adicionalmente, cuando se sustituye el terminal, el usuario puede instalar la UICC separada del terminal en un nuevo terminal, cambiando de ese modo oportunamente el terminal.

Un terminal que requiera ser de pequeño tamaño, por ejemplo, un terminal para comunicaciones de máquina a máquina (M2M), es difícil de hacer pequeño cuando se fabrica con una estructura de UICC extraíble. Por ello, se ha introducido una UICC integrada (eUICC) que no es extraíble. La eUICC registra información sobre el usuario que usa la UICC en forma de Identidad de Abonado Móvil Internacional (IMSI).

Una UICC convencional es extraíble de un terminal, y por ello el usuario puede abrir el terminal independientemente de un tipo de terminal u operador móvil. Sin embargo, una IMSI puede asignarse a una eUICC bajo la premisa de que el terminal esté disponible bajo un operador de red móvil (MNO) particular a partir del momento de fabricación. Por ello, tanto los MNO como los fabricantes de terminales M2M para venta de terminales no pueden prestar mucha atención a los artículos en stock y puede tener lugar una elevación de precio. También, los usuarios pueden encontrar inconvenientes al no permitirse un cambio en los MNO de los terminales. Por ello, los usuarios requieren un método para liberar un terminal independientemente de los operadores móviles incluso para una eUICC.

Entretanto, la reciente introducción de una eUICC lleva a la necesidad de actualizar remotamente la información sobre los abonados a una pluralidad de operadores móviles para la UICC, y en consecuencia se analiza un gestor de abonados (SM) o gestor de perfiles (PM) para la gestión de la información sobre los abonados.

Sin embargo, debido a la diferencia física respecto a una SIM extraíble convencional, el entorno eSIM implica la gestión de datos de la SIM en forma de software, y en consecuencia están actualmente bajo análisis métodos basados en la tecnología GlobalPlatform. Sin embargo, un MNO pueden necesitar ir a proporcionar servicios basados en eSIM, en lugar de un tercero, debido a situaciones acerca de la propiedad de las claves y la iniciativa en actividades basadas en eSIM (comunicaciones y servicios opcionales) sobre GlobalPlatform, pero no se han hallado aún medidas concretas.

El documento US 2009/0191857A divulga parámetros de actualización de SIM Universal mediante el envío de una clave de autorización a la uSIM desde un MNO donador, para cambiar el MNO.

El documento de la Asociación GSM: “Embedded SIM Task Force Requirements and Use Cases 1.0”, Non-confidential White Paper, 21 de febrero de 2011 (2011-02-21), XP055180476 divulga la provisión de perfiles SIM de modo que un perfil sustituye a otro.

La invención está en el método de la reivindicación 1.

Breve descripción de los dibujos

La figura 1 ilustra una arquitectura completa de servicios que incluye un eSIM o una eUICC de acuerdo con la presente invención.
La figura 2 ilustra una arquitectura de tarjeta basada en GlobalPlatform de acuerdo con la presente invención.
La figura 3 ilustra una estructura interna de un eSIM y la relación entre el eSIM y los MNO externos de acuerdo con una realización de ejemplo de la presente invención.
La figura 4 es un diagrama de flujo que ilustra un proceso de provisión usando un eSIM de acuerdo con una

realización de ejemplo de la presente invención.
La figura 5 es un diagrama de flujo que ilustra un proceso de cambio de MNO usando un eSIM de acuerdo con otra realización de ejemplo de la presente invención.
La figura 6 es un diagrama de flujo que ilustra un proceso de cambio de MNO usando un eSIM de acuerdo con otra realización de ejemplo de la presente invención, en la que un MNO abierto inicialmente no es un MNO donador o receptor.
La figura 7 es un diagrama de flujo que ilustra un proceso de vuelta a un MNO abierto inicialmente usando un eSIM de acuerdo con una realización de ejemplo de la presente invención.

Modo de llevar a cabo la invención

Las realizaciones y/o ejemplos de la descripción que sigue que no están cubiertos por las reivindicaciones adjuntas se considera que no son parte de la presente invención.

De aquí en adelante en el presente documento se describirán algunas realizaciones de ejemplo con referencia a los dibujos adjuntos. Números de referencia iguales en los dibujos se refieren a elementos iguales a todo lo largo de ellos. En la descripción que sigue, cuando se determina que descripciones detalladas acerca de funciones o estructuras bien conocidas relacionadas hacen no clara la invención, se omitirán en el presente documento las descripciones detalladas.

Un terminal de máquina a máquina (M2M) activamente analizado en la Asociación para el Sistema Global de Comunicaciones Móviles (GSM) (GSMA) se requiere que sea característicamente pequeño. Sin embargo, cuando se usa una Tarjeta de Circuito Integrado Universal (UICC) convencional, se necesita un módulo separado sobre el que se monta la UICC y este se inserta en el terminal M2M. Así, cuando el terminal M2M se fabrica con una estructura de UICC extraíble, es difícil hacer un M2M pequeño.

Por ello, se considera una UICC integrada (eUICC), que no es extraíble. En este caso, la eUICC montada sobre el terminal M2M almacena necesariamente información sobre un operador de la red móvil (MNO) usando la UICC en una forma de identidad de abonado móvil internacional (IMSI).

Sin embargo, dado que puede asignarse el IMSI al terminal en la eUICC sobre la base de que el terminal está disponible bajo un MNO particular a partir de su fabricación, tanto los MNO como los fabricantes de terminales M2M para la venta de terminales M2M o UICC no pueden prestar mucha atención a los artículos en stock y puede tener lugar una elevación de precios, lo que bloquea la difusión de los terminales M2M.

De ese modo, a diferencia del módulo de identidad abonado (SIM) extraíble universal, una eUICC o eSIM integralmente montado sobre un terminal implica muchos problemas acerca de la autorización para abrir una cuenta, en la iniciativa en actividad de servicios opcionales y en la seguridad de la información de abonado debido a diferencias en la estructura física. Con este fin, una organización de normalización internacional tal como la GSMA y el Instituto Europeo de Normas de Telecomunicaciones (ETSI) están desarrollando actividades de normalización con respecto a los elementos necesarios e incluyendo una estructura superior junto con las compañías relacionales tales como operadores, fabricantes, y fabricantes de SIM. Durante los análisis sobre el eSIM, la asociación de normalización se centra sobre la gestión de la suscripción (SM), que se refiere a una entidad o función/papel para realizar una gestión general del eSIM, por ejemplo, enviando información del operador (también denominada como credenciales del operador, credenciales de MNO, perfil, perfil de eUICC o paquete de perfil) al eSIM y manejar el proceso de cambio en la suscripción o de cambio de MNO.

Recientemente, la GSMA sugiere una estructura en la que las funciones de la SM se dividen en una preparación de datos de SM (SM-DP) responsable de generar información de operador y en un enrutado seguro de SM (SM-SR) para llevar directamente información del operador al eSIM, y un método para codificar y transmitir un perfil, ambos de los cuales carecen de tecnicismos.

En esta especificación, el eSIM y la eUICC se usan para referirse a conceptos equivalentes.

Un eSIM es un nuevo concepto de tecnología SIM, que se fabrica mediante la fijación de un chip de circuito integrado (IC) a una tarjeta de circuito de un terminal y la entrega de datos SIM (información de apertura de servicio e información de servicio opcional) en una forma de software a través del aire (OTA) o a través de un método fuera de línea (conexión basada en la tecnología de un PC y un USB) en la fabricación del terminal. El chip de IC usado para el eSIM soporta en general un procesador de criptografía basada en hardware (CCP) para promocionar la generación de una clave pública basada en hardware, y una plataforma SIM (por ejemplo, Plataforma de Tarjeta Java) proporciona una interfaz de programación de aplicaciones (API) para la utilización de la clave pública basada en una aplicación (por ejemplo, applet). La Plataforma de Tarjeta Java es una plataforma que permite a una tarjeta inteligente tener múltiples aplicaciones y proporcionar servicios.

Por razones de espacio de memoria limitado y de seguridad, no todo el mundo tiene permitido montar una aplicación sobre la SIM, y por ello no solo se necesita una plataforma para el montaje de una aplicación sino también una

plataforma de gestión del servicio SIM responsable del montaje y gestión de una aplicación sobre el SIM. La plataforma de gestión del servicio SIM envía datos a un área de memoria del SIM a través de autenticación y seguridad usando una clave de gestión, y usa especificaciones de la GlobalPlatform, Gestión Remota de Archivos (RFM) y Gestión Remota de Aplicaciones (RAM) de la ETSI TS 102.226.

Un SM como uno de los elementos importantes en un entorno eSIM sirve para enviar remotamente datos de comunicación y servicios opcionales a través de una clave de gestión, tal como una clave UICC OTA y una clave GP ISD.

El GAMA puede dividir las funciones del SM en SM-DP y SM-SR. El SM-DP sirve para construir con seguridad no solamente un perfil de aplicación o información de operador sino un IMSI, K, OPc, aplicaciones de servicios opcionales y datos de servicios opcionales en un paquete de credenciales, mientras que el SM-SR sirve para descargar con seguridad el paquete de credenciales generado en el SM-DP para el eSIM a través de tecnología de gestión remota de la SIM tal como OTA o protocolo de comunicación seguro GP (SCP).

La figura 1 ilustra un sistema de comunicación eSIM que incluye un SM.

Una arquitectura del sistema de comunicación del eSIM que usa el SM puede incluir una pluralidad de sistemas MNO, al menos un sistema SM, un sistema de fabricante de eUICC, un sistema fabricante de un dispositivo que incluye la eUICC, y un eUICC. En la figura 1, una línea de puntos indica un círculo de confianza y dos líneas continuas indican enlaces seguros.

En la figura 1, se introduce una estructura de “círculo de confianza” para solapar relaciones entre objetos o entidades similares, estableciendo así una relación de confianza de extremo a extremo entre un MNO y un eSIM. Esto es, el MNO1 construye una relación de confianza con el SM1, el SM1 con el SM4, y SM4 con el eSIM, estableciendo de ese modo finalmente una relación de confianza entre el MNO y el eSIM.

El sistema de comunicación del eSIM que usa el SM adopta una función definida como un SM, y una función principal del SM prepara y transmite un paquete o perfil que incluye una credencial del MNO para la eUICC. La función SM puede proporcionarse directamente por el MNO, o el MNO puede realizar un contrato con una tercera entidad para adquirir un servicio SM. La función SM necesita proporcionarse por el MNO o la tercera entidad. El servicio SM puede proporcionarse por la tercera entidad cuando se establece una relación comercial entre el SM y el MNO.

El SM se divide en un SM-DP para preparar con seguridad una pluralidad de perfiles relacionados con la eUICC, tal como un perfil de operación y un perfil de provisión del MNO, y un SM-SR para enrutar los perfiles, en el que el SM-SR puede enlazarse con una pluralidad de otros SM-SR basándose en una relación de confianza y el SM-DP se enlaza al sistema MNO.

En el sistema que usa el SM de la figura 1, el SM realiza la gestión global, tal como la gestión de la suscripción, una gestión de servicio opcional y una gestión del cambio de MNO. Sin embargo, dicho sistema es diferente de un servicio de comunicación actual conducido por el MNO y por ello puede enfrentarse a problemas en asegurar compatibilidad o fiabilidad.

Mientras tanto, se usa la GlobalPlatform como una especificación de una plataforma de gestión del servicio SIM.

La GlobalPlatform es una tarjeta segura y dinámica y una especificación de gestión de la aplicación y proporciona una interfaz neutra acerca de un componente de tarjeta, un conjunto de instrucciones, una secuencia de transacciones, hardware, un sistema y un sistema operativo (OS) e independiente de aplicaciones.

La presente invención puede proporcionar una estructura de entrega de un perfil MNO a un terminal y habilitar el terminal para conmutar a otro operador móvil sin cambiar la tecnología SIM convencional en un entorno en el que el MNO posee una clave del dominio de seguridad del remitente (ISD) sobre la base de GlobalPlatform.

Con este fin, una realización de ejemplo de la presente invención proporciona un método que usa un dominio de seguridad (SD) que tiene un privilegio de gestión autorizado o un privilegio de gestión delegado definidos en GlobalPlatform. Se describirá una configuración detallada de la presente invención con referencia a la figura 3.

La figura 2 ilustra una arquitectura de tarjeta basada en GlobalPlatform de acuerdo con la presente invención.

La arquitectura de tarjeta basada en GlobalPlatform incluye una pluralidad de componentes para asegurar una interfaz neutral sobre hardware y un vendedor a una aplicación y un sistema de gestión fuera de tarjeta.

Dichos componentes pueden incluir al menos una aplicación de emisor de tarjeta 210 para un emisor de la tarjeta, al menos una aplicación de proveedor de aplicación 220 para un socio comercial del emisor de la tarjeta, esto es, un proveedor de la aplicación, y al menos una aplicación de servicio global 230 para proporcionar un servicio global, por ejemplo, un servicio CSM, a otra aplicación.

Cada aplicación se asocia con un SD relevante, que incluye un SD de emisor (ISD) 211, un SD del proveedor de servicio 221 y un SD de la autoridad de control 231.

Todas las aplicaciones se implementan en un entorno de ejecución seguro 250 que incluye una API neutral sobre hardware de soporte de movilidad de las aplicaciones. La GlobalPlatform no limita un entorno de ejecución una tecnología de entorno de ejecución particular y es un componente de tarjeta principal al que un gestor de tarjeta sirve como un gestor central. Se genera una clave especial y una aplicación de gestión de la seguridad llamada SD para asegurar la separación completa de claves entre el emisor de la tarjeta y una pluralidad de diferentes proveedores SD.

Se dispone un entorno GlobalPlatform (OPEN) y un marco de confianza GP 240 bajo las aplicaciones y los SD, y el entorno de ejecución 250 se forman en virtud del mismo.

Adicionalmente, se proporciona una API de GP 241 entre las aplicaciones/SD y el entorno GlobalPlatform (OPEN) y el marco de confianza GP 240, y se proporciona una API de ejecución (API de RTE) 251 entre las aplicaciones/SD y el entorno de ejecución 250.

Los SD, tales como el ISD 211, el SD del proveedor de servicio 221 y el SD de la autoridad de control 231, sirven como representantes en tarjeta de autoridades fuera de tarjeta. Los SD pueden dividirse ampliamente en tres tipos de acuerdo con tres tipos de autoridades fuera de tarjeta percibidas por una tarjeta.

Primero, el ISD 211 es un representante en tarjeta principal y esencial para un administrador de tarjeta que es generalmente un emisor de la tarjeta.

Segundo, un SD suplementario funciona como un representante adicional y opcional en tarjeta para un emisor de la tarjeta, un proveedor de aplicación o un agente de la misma. El SD del proveedor de servicio 221 es el SD suplementario (SSD).

Tercero, un SD de la autoridad de control es un SD suplementario especial. Una autoridad de control sirve para obligar a una política de seguridad aplicada en todos los códigos de aplicación cargados en una tarjeta. También, la autoridad de control puede usar un SD de la autoridad de control como un representante en tarjeta del mismo de modo que proporcione dicha función. Puede estar presente al menos un SD de la autoridad de control.

En general, se puede hacer referencia a tres tipo de SD como simplemente los SD, que soportan servicios de seguridad, tales como manejo de claves, codificación, decodificación, creación de una firma electrónica y verificación, para los proveedores de la misma (el emisor de la tarjeta, el proveedor de aplicaciones o la autoridad de control). Cada SD se configura en lugar del emisor de la tarjeta, el proveedor de aplicaciones o la autoridad de control cuando una entidad fuera de tarjeta solicita el uso de una clave completamente aislada.

Entretanto, está presente en la tarjeta al menos una aplicación de servicio global 230, proporcionando de ese modo un servicio de método de verificación de poseedor de tarjeta (CVM) a otra aplicación en la tarjeta.

Se usa GlobalPlatform para habilitar operaciones en un entorno seguro de ejecución de tarjeta multi-aplicación. El entorno de ejecución 250 proporciona no solamente un espacio de almacenamiento e implementación seguro para aplicaciones, sino una API neutra en hardware para las aplicaciones, de modo que un código y datos de cada aplicación se retienen con seguridad por separado de otras aplicaciones. El entorno de ejecución de la tarjeta proporciona también un servicio de comunicación entre la tarjeta y una entidad fuera de tarjeta.

La tarjeta GlobalPlatform puede incluir al menos un marco de confianza 240, que proporciona comunicaciones entre aplicaciones. El marco de confianza no es ni una aplicación ni un SD pero puede existir como una extensión o parte del entorno de ejecución de la tarjeta.

Como se ha descrito anteriormente, GlobalPlatform es una especificación para la gestión de aplicaciones (applets) de una tarjeta inteligente, tal como una SIM. GlobalPlatform define software que representa a un emisor de la tarjeta (por ejemplo, MNO) como un ISD y realiza las funciones y software de gestión global necesarias de un SSD para un socio comercial del emisor de la tarjeta (por ejemplo, un proveedor de aplicaciones tal como un banco y una compañía de tarjetas de crédito) para gestionar con seguridad software de servicio e información del mismo (por ejemplo, applets de banca e información de cuentas).

Sin embargo, debido a la diferencia física respecto a una SIM extraíble convencional, el entorno eSIM implica la gestión de datos de la SIM en forma de software, y en consecuencia están actualmente bajo análisis los métodos basados en la tecnología GlobalPlatform. Sin embargo, es necesaria la definición estructural de que un MNO posee una clave ISD y desarrolla una relación comercial eSIM basándose en la clave ISD debido a problemas sobre la propiedad de la clave ISD e iniciativa en actividades basadas en eSIM (comunicaciones y servicios sociales) en GlobalPlatform.

Por ello, la presente invención divulga un método de gestión del eSIM sobre la base de una gestión autorizada y

gestión delegada en una especificación de GlobalPlatform existente, particularmente una estructura de apertura básica de una estructura y un proceso de conmutación a un operador móvil diferente.

La figura 3 ilustra una estructura interna de un eSIM y la relación entre el eSIM y los MNO externos de acuerdo con una realización de ejemplo de la presente invención.

Un sistema de acuerdo con la presente realización incluye un eSIM 300 y uno o más sistemas MNO 360 y 370.

El eSIM 300 incluye un perfil de provisión 310, GlobalPlatform 320, y un ISD 330 y un SD 340 en un nivel más alto que GlobalPlatform.

El ISD es un representante en tarjeta principal y esencial para un administrador de la tarjeta que es generalmente un emisor de la tarjeta, que indica una entidad en tarjeta principal que soporta requisitos de comunicación, control y seguridad del administrador de la tarjeta.

Además, el eSIM incluye perfiles 331 y 341 de uno o más MNO, en los que el perfil 331 de un MNO abierto inicialmente, MNO1, es gestionado por el ISD 330 y el perfil 341 de un MNO adicional, MNO2, es gestionado por el SD.

El SD 340 es un SD que tiene un privilegio de gestión autorizado o privilegio de gestión delegado, y se describirán en detalle el privilegio de gestión autorizado o privilegio de gestión delegado.

Se definen cómo sigue los términos usados en la especificación.

Un MNO es un proveedor de servicios inalámbricos, que se refiere a una entidad para proporcionar a los clientes servicios de comunicación a través de una red móvil.

La provisión es un proceso de carga de un perfil en una eUICC, y el perfil de provisión se refiere a un perfil usado para que un dispositivo se conecte a una red de comunicación de modo que dirija la provisión de otro perfil de provisión y perfil de operación.

La suscripción se refiere a una relación comercial entre un abonado y un proveedor de servicios de comunicación inalámbricos.

Un perfil es una combinación de una estructura de archivo, datos y una aplicación a ser suministrada a la eUICC o gestionada en la eUICC, lo que incluye toda la información presente en la eUICC, tal como un perfil de operación como información del operador, un perfil de provisión para provisión y un perfil para una función de control de política (PCF).

Un perfil de operación o información del operador se refiere a cualquier clase de perfil relacionado con la suscripción operativa.

El contenido de la tarjeta se refiere a un código e información de aplicación (no datos de aplicación) incluidos en una tarjeta bajo la responsabilidad del OPEN, por ejemplo, un archivo de carga ejecutable y una instancia de la aplicación.

Un emisor de la tarjeta es una entidad que posee una tarjeta, que es responsable de todos los aspectos de la tarjeta.

Un ISD es una entidad en tarjeta principal que proporciona soportes para requisitos de comunicación, control y seguridad de un administrador de la tarjeta.

Un SD es una entidad en tarjeta que soporta requisitos de control, seguridad y comunicación de una entidad fuera de tarjeta, por ejemplo, un emisor de la tarjeta, un proveedor de aplicaciones o una autoridad de control.

Una gestión delegada (DM) significa cambio de contenido de la tarjeta pre-autorizado realizado por un proveedor de aplicación autorizado, y un identificador (token) es un valor criptográfico proporcionado por un emisor de la tarjeta para confirmar que una operación de gestión delegada está autorizada.

Una autoridad de control es una entidad que tiene privilegios para mantener el control del contenido de la tarjeta a través de una autoridad para verificar un patrón de autenticación de datos (DAP).

El privilegio en un SD, particularmente un ISD, se formaliza, clarificando de ese modo la autoridad para acceder a una función de gestión del contenido de la tarjeta. El ISD tiene un conjunto de privilegios explícitos, que pueden incluir gestión autorizada (AM) o un nuevo tipo de privilegio, tal como una autenticación basada en identificador.

Un SD que tenga un privilegio de GA permite a un proveedor de SD gestionar el contenido de la tarjeta, gestión sin autenticación basada en identificador cuando una entidad fuera de tarjeta se autentifica como un poseedor del SD, esto es, el proveedor de SD. En este caso, no está implicado un SD que tenga un privilegio sobre la autenticación basada en identificador. Sin embargo, aún es necesario un identificador para un caso en el que la entidad fuera de

tarjeta se autentifica pero no es el proveedor de SD.

El privilegio de gestión delegada permite a un SD de un proveedor de aplicaciones tener el privilegio de realizar una carga delegada, instalación delegada, extradición delegada, actualización delegada a un registro de GlobalPlatform y borrado delegado.

El privilegio de gestión delegada permite al proveedor de aplicaciones gestionar el contenido de la tarjeta a través de autenticación, y la autenticación es controlada por un SD que tiene privilegios de autenticación basados en identificador. Dicha gestión delegada no es una característica esencial de una tarjeta GlobalPlatform.

Esto es, como se muestra en la figura 3, el eSIM 300 de acuerdo con la presente realización incluye el perfil de provisión 301 para realizar el envío a través de todas la redes, por ejemplo, MNO1 y MNO2, y GlobalPlatform 320 que tiene funciones de gestión autorizada y gestión delegada.

El sistema MNO1 360 y el sistema MNO2 370 pueden servir para realizar funciones de gestión de la tarjeta basadas en GlobalPlatform (establecimiento de un canal de comunicación para autenticación mutua con un SIM y seguridad y envío de aplicaciones y datos). Los MNO1 y MNO2 pueden necesitar estar bajo previo acuerdo para transferencia a otro proveedor de servicios.

De aquí en adelante, se describirán detalles sobre la tecnología GlobalPlatform relevantes para la presente invención.

Un SD es una aplicación privilegiada, que tiene claves criptográficas usadas para soportar una operación de protocolo de canal seguro o para autorizar una función de gestión de contenido de la tarjeta.

Cada aplicación y cada archivo de carga ejecutable pueden relacionarse con el SD, en el que la aplicación puede usar un servicio de encriptación relevante del SD.

Todas las tarjetas tienen un SD esencial, que se denomina como ISD. Debido a una tarjeta que soporte múltiples SD, un proveedor de aplicación puede gestionar sus propias aplicaciones a través de un SD propio del proveedor de aplicaciones y proporcionar un servicio codificado usando una clave completamente separada del emisor de la tarjeta.

El SD es responsable de la gestión de su propia clave, y en consecuencia pueden estar presentes aplicaciones y datos desde una pluralidad de diferentes proveedores de aplicación en la misma tarjeta sin violar la privacidad e integridad de cada proveedor de aplicaciones.

Un proceso de encriptación relacionado con las claves de todos los SD puede proporcionar un soporte seguro para comunicaciones mientras que una aplicación de un proveedor de aplicaciones se personaliza y habilita comunicaciones seguras mientras se implementa una aplicación que no incluye claves de mensaje seguro de los SD.

Un ISD generalmente funciona como un SD único particular pero tiene características que lo distinguen de otros SD.

Esto es, aunque el ISD es una aplicación instalada inicialmente en la tarjeta, el ISD no se carga o instala necesariamente de la misma manera para cada aplicación. Además, el ISD tiene un ciclo de vida de tarjeta establecido internamente y por ello no tiene un estado del ciclo de vida de SD. Cuando se elimina una aplicación privilegiada, el ISD tiene autoridad para reiniciar la tarjeta.

Además, cuando se elimina una aplicación implícitamente seleccionada sobre el mismo canal analógico de una interfaz de E/S del mismo caso, el ISD se convierte en una aplicación implícitamente seleccionada y puede seleccionarse de acuerdo con una instrucción SELECT que no tenga un campo de datos de comando.

Una aplicación que incluya un SD puede usar un servicio de un SD relevante para la aplicación para proporcionar una sesión de canal segura y otros servicios de codificación. La aplicación no necesita conocer un identificador del SD (AID) por adelantado, mientras el registro de GlobalPlatform proporciona la AID de SD y el OPEN proporciona un estándar del SD relevante para aplicación. Dado que el SD relevante puede cambiarse por extradición, la aplicación puede no necesitar almacenar el estándar.

La extradición es un método para asociar una aplicación con otro SD. Aunque se asocie primero un archivo de carga ejecutable con un SD que carga el archivo de carga, el archivo de carga se extradita inmediatamente a otro SD a través de una extradición implícita o es secuencialmente extraditado a otro SD a través de una extradición explícita durante un proceso de carga.

Un ISD no es para extradición, mientras que un SD puede asociarse con sí mismo a través de la extradición. Un SD puede separarse adicionalmente de otro SD usando el privilegio asignado a otro SD, y en consecuencia pueden formarse sobre la tarjeta una o más capas asociadas. Una raíz de cada capa se convierte en un SD asociado con la raíz.

Una aplicación puede acceder a un servicio de un SD relevante. La aplicación puede basarse en el soporte para codificación desde el SD que usa el servicio, asegurando confidencialidad e integridad durante la personalización y ejecución. El servicio SD puede tener características tales como sigue.

El SD inicia una sesión segura de canal tras la autenticación con éxito de una entidad en tarjeta, desenvuelve una instrucción recibida en la sesión de canal segura mediante verificación de la integridad o decodifica los datos originales bajo una confidencialidad segura.

Además, el SD controla la secuencia de instrucciones APDU, decodifica un bloque de datos confidencial, y establece un nivel de seguridad de confidencialidad o integridad que es aplicable a una siguiente instrucción de entrada o siguiente respuesta de salida. Adicionalmente, el servicio SD cierra la sesión de canal seguro y retira los datos confidenciales relacionados con la sesión de canal seguro bajo demanda.

Dependiendo de si soporta un protocolo de canal seguro particular, el SD puede tener una función de envoltura de una respuesta transmitida dentro de la sesión de canal seguro mediante la adición de confidencialidad, una función de codificación de los datos originales bajo la confidencialidad asegurada, o una función de codificación de un bloque de datos confidencial y control de una secuencia de respuestas APDU.

El SD puede gestionar simultáneamente múltiples sesiones de canal seguro, esto es, una pluralidad de aplicaciones seleccionadas en una pluralidad de canales lógicos arrancando cada una un canal seguro, y el control para gestionar solamente una sesión de canal seguro de entre una pluralidad de aplicaciones simultáneamente seleccionadas para el uso de servicios. Cuando el SD soporta la gestión simultánea de múltiples sesiones de canal seguro, el SD puede necesitar dividir las múltiples sesiones de canal seguro y los canales lógicos de la misma. Cuando el SD no soporta simultáneamente la gestión de múltiples sesiones de canal seguro, el SD puede rechazar una solicitud para el comienzo de una nueva sesión de canal seguro cuando la solicitud para la apertura de la sesión de canal seguro se realiza a otro canal lógico diferente de una sesión de canal seguro actual.

También, el SD puede recibir una instrucción STORE DATA hacia una de las aplicaciones asociadas. El SD desenvuelve la instrucción de acuerdo con un nivel de seguridad de la sesión de canal seguro actual antes de que se envíe la instrucción a la aplicación.

El ISD puede necesitar procesar un número de identificación del emisor (IIN), un número de imagen de tarjeta (CIN), unos datos de reconocimiento de tarjeta y unos datos dedicados del emisor de tarjeta. Estos datos pueden adquirirse desde la tarjeta a través una instrucción GET DATA.

Se usa un IIN de una entidad fuera de tarjeta para asociar una tarjeta con un sistema de gestión de tarjeta particular. El IIN incluye en general información de identificación sobre un emisor definido por ISO 7812 y transmitido por una etiqueta “42” de la ISO/IEC 7816-6. Un elemento de datos IIN tiene una longitud variable.

Se usa un CIN por un sistema de gestión de tarjeta para identificar únicamente una tarjeta en una base de tarjetas. El CIN es un valor único y se transmite mediante una etiqueta “45” (datos de un emisor de tarjeta) definido en ISO/IEC 7816 y asignado por el emisor de la tarjeta definido como el IIN. Un elemento de datos XIN tiene también una longitud variable.

Un sistema de gestión de tarjeta puede necesitar conocer información sobre una tarjeta antes de llevar a cabo interacciones con la tarjeta. La información puede incluir información sobre una clase de la tarjeta e información sobre protocolos de canal seguro disponibles. Los datos de reconocimiento de la tarjeta son un mecanismo para proporcionar la información sobre la tarjeta e impide cambios de prueba y error.

Un SD distinto del ISD puede expresarse como un dominio de seguridad suplementaria (SDD), y el SDD maneja los datos de identificación sobre el SDD. Los datos de identificación sobre el SDD pueden incluir un número de identificación de proveedor SD (SIN), un número de imagen SD, datos de gestión SD y datos dedicados del proveedor de aplicación. Estos datos pueden obtenerse desde la tarjeta a través de la instrucción GET DATA.

Se usa un SIN por una entidad fuera de tarjeta para asociar un SD con un sistema de gestión de tarjeta particular. El SIN incluye generalmente información de identificación de un proveedor de SD definido por ISO 7812 y transmitido por la etiqueta “42” de ISO/IEC 7816-6. Un elemento de datos SIN tiene una longitud variable.

Se usa un número de imagen de SD por un sistema de gestión de la tarjeta para identificar únicamente una instancia de SD dentro de una tarjeta. El número de imagen de SD puede ser un valor único y puede transmitirse por la etiqueta “45” (datos de un emisor de tarjetas) definido en ISO/IEC 7816.

Un sistema de gestión de tarjeta puede necesitar conocer información de una tarjeta antes de llevar a cabo interacciones con la tarjeta. La información puede incluir información sobre una clase de la SD e información sobre protocolos de canal seguro disponibles.

Los datos de gestión de SD son un mecanismo para proporcionar información sobre el SD e impide cambios de prueba y error. Los datos de gestión de SD se incluyen en una respuesta a la instrucción SELECT y devuelta, y pueden incluirse en una respuesta a la instrucción GET DATA y devuelta.

La información proporcionada a los datos de gestión de SD se requiere para habilitar suficientemente la tarjeta y la comunicación inicial pero no está limitado a requisitos particulares. Los datos de gestión de SD necesitan actualizarse dinámicamente por la tarjeta.

El eSIM 300 de acuerdo con una realización de ejemplo almacena un perfil de al menos un MNO, recibe un SD que tiene privilegio de gestión delegado o privilegio de gestión autorizado sobre un MNO receptor desde un sistema MNO donador, y conecta con el sistema MNO receptor usando un perfil de provisión para llevar a cabo la autenticación de SD y para recibir los perfiles o datos necesarios (datos de apertura y datos de servicios opcionales instalados).

También, cuando el eSIM 300 recibe el SD que tiene privilegios de gestión delegada o privilegios de gestión autorizada sobre el MNO receptor desde el sistema MNO donador, el eSIM puede inactivar un perfil del MNO donador.

Además, después de que se reciba un perfil enviado o datos necesarios para el MNO receptor, el eSIM de acuerdo con la presente realización puede cambiar un valor de clave de SD en un valor de clave de SD único reconocido solamente por el sistema MNO receptor.

Un eSIM 300 de acuerdo con otra realización de ejemplo de la presente invención almacena un perfil de al menos un MNO. Cuando se recibe una solicitud de retorno desde un sistema MNO abierto inicialmente, el eSIM 300 se conecta al sistema MNO abierto inicialmente usando un perfil de provisión para borrar un perfil (incluyendo un SD) de un MNO actualmente activado usando una clave ISD y para cambiar un perfil del MNO abierto inicialmente inactivado a un estado activado.

En consecuencia, el MNO abierto inicialmente retorna desde otro sistema MNO, los servicios proporcionados por el MNO abierto inicialmente pueden utilizarse como lo hizo el terminal previamente.

Un eSIM 300 de acuerdo con otra realización de ejemplo más de la presente invención almacena un perfil de al menos un MNO. Cuando ocurre un cambio de suscripción desde un MNO donador a un MNO receptor, existiendo un MNO abierto inicialmente por separado, el eSIM 300 recibe un SD que tiene privilegio de gestión delegado o privilegio de gestión autorizado sobre el MNO receptor desde el sistema MNO abierto inicialmente, borra un perfil (que incluye un SD) del MNO donador, y conecta al sistema MNO receptor usando un perfil de provisión para llevar a cabo una autenticación SD y para recibir perfiles o datos necesarios (datos de apertura y datos de servicios opcionales preinstalados).

En adelante en el presente documento, se describirán una clave ISD y una clave de SD usadas en una realización de ejemplo de la presente invención.

La clave ISD y la clave de SD de acuerdo con la presente realización tiene características tales como sigue.

La clave ISD o la clave de SD incluyen un identificador de clave para etiquetar cada clave en una entidad en tarjeta. Una clave incluye uno o más componentes de clave. Por ejemplo, una clave simétrica tiene un componente de clave, mientras que una clave asimétrica incluye una pluralidad de componentes. Todos los componentes de la clave comparten el mismo identificador de clave, y diferentes identificadores de clave se usan en una entidad en tarjeta para distinguir claves, finalidades y funciones de la misma. No hay restricción u orden predeterminado en la asignación de identificadores de clave a las claves, y pueden usarse identificadores de clave no consecutivos en la misma entidad.

La clave de SD tiene una característica de un número de versión de clave asociado. Pueden usarse diferentes versiones de clave para distinguir una pluralidad de instancias o versiones de la misma clave en una entidad en tarjeta. No hay restricción u orden predeterminado en la asignación de números de versión de clave a una clave.

Tradicionalmente, la clave de SD tiene una característica de un algoritmo de encriptación, en el que una clave particular puede asociarse con un algoritmo de encriptación. Una longitud de un algoritmo de encriptación que soporte una pluralidad de longitudes de clave y condiciones de acceso para el acceso o control de una clave puede ser característica de la clave de SD.

Dicha característica de la clave puede permitir sean claramente dirigidas una identidad, las finalidades pretendidas y funciones de una clave de encriptación a una entidad en tarjeta.

Una clave particular puede identificarse claramente en la entidad en tarjeta mediante una combinación de un identificador de clave y un número de versión de clave, y un algoritmo de encriptación y un componente de clave se identifican mediante un tipo de clave. Una clave y un algoritmo se distinguen claramente en la entidad, impidiendo de ese modo el uso erróneo de una función de encriptación. Una entidad fuera de tarjeta puede adquirir información sobre la clave de SD usando la instrucción GET DATA de un patrón de información de clave (etiqueta “E0”).

Por otro lado, un método en el que el SD gestiona una clave de acuerdo con una realización de ejemplo de la presente invención es como sigue.

Un identificador de clave y un número de versión de clave se refieren de modo único a cada clave en la entidad en tarjeta, y cada combinación identificador de clave/número de versión de clave representa una ranura de clave única en la entidad.

Añadir una clave significa asignar una nueva ranura de clave con un nuevo valor de clave, un nuevo identificador de clave o un nuevo número de versión de clave. La sustitución de una clave se asocia con la actualización de una ranura de clave con un número de versión de clave relacionado con un nuevo valor de clave. Un identificador de clave continúa siendo el mismo, y la clave previa ya no se usa más.

Un sistema de gestión de clave fuera de tarjeta puede necesitar conocer un método de identificación de clave realizado por una entidad en tarjeta. Un identificador de clave y un número de versión de clave pueden tener valores aleatorios con respecto a la tarjeta particular, y estos valores pueden cambiarse de un método de gestión de clave a otro método.

Un SD puede necesitar almacenar toda la información clave proporcionada a través una instrucción PUT KEY.

Pueden asignarse tres condiciones de acceso a la clave de SD, que son acceso por el SD, acceso por un usuario autorizado, por ejemplo, una aplicación asociada del SD, distinta de la propietaria, y acceso por todos los usuarios autorizados incluyendo el propietario de la clave de SD.

Las condiciones de acceso a la clave de SD pueden representarse por un byte. Por ejemplo, “00” representa cualquier usuario autorizado incluyendo el propietario, que es una condición de acceso básica con respecto a una clave de protocolo de canal seguro cuando no se proporciona explícitamente a través de la instrucción PUT KEY, “01” representa el propietario, esto es, el SD, que es una condición de acceso básica con respecto a un identificador y clave DAP cuando no se proporciona explícitamente a través de la instrucción PUT KEY, y “02” representa un usuario autorizado distinto del propietario, sin quedar limitado a los ejemplos anteriores. Las regulaciones de control de acceso aplicables a una clave de SD particular pueden imponerse como sigue.

Para usar un servicio de encriptación SD particular, una aplicación pide el OPEN para referencia a una interfaz de canal seguro, mientras el OPEN puede identificar un SD relacionado con la aplicación y proporciona referencia a la interfaz de canal seguro correspondiente a la aplicación.

Además, la aplicación puede pedir al SD un servicio de encriptación a través de la interfaz de canal seguro, mientras que el OPEN puede permitir el acceso solamente por la aplicación relacionada.

Datos y clave se gestionan de la siguiente forma. Cuando se recibe una solicitud de gestión de datos/clave, un SD relevante gestiona la clave/datos de acuerdo con las regulaciones de control de acceso del SD y un ciclo de vida de la tarjeta no está en un estado CARD_LOCKED o TERMINATED.

Cuando se recibe una instrucción DELETE KEY, PUT KEY o STORE DATA, el SD ejecutando la gestión de datos o clave aplica una política de comunicación segura del SD y un proveedor de SD puede aplicar una política de gestión de clave relacionada con el borrado de una clave.

La figura 4 es un diagrama de flujo que ilustra un proceso de provisión usando un eSIM de acuerdo con una realización de ejemplo de la presente invención.

Como un pre-requisito para el proceso de provisión y un proceso de cambio de un MNO a ser descrito a continuación, se preinstala un archivo de provisión en el eSIM. El archivo de provisión puede aplicarse igualmente a todos los MNO. Cada MNO necesita permitir el acceso a un perfil a través de una red de modo que el eSIM se gestiona a través del perfil de provisión.

Como se muestra en la figura 4, en el proceso de provisión usando el eSIM de acuerdo con la presente realización, un terminal equipado con el eSIM se conecta a una red del MNO1 usando el perfil de provisión del eSIM cuando se inicia (S410). A continuación, un sistema del MNO1 establece una autorización mutua y canal de comunicación seguro con el eSIM usando una clave ISD (S420). Posteriormente, el sistema del MNO1 envía al eSIM un perfil del MNO1, datos de apertura para comunicaciones (por ejemplo, IMSI, Ki y OPc), datos sobre servicios opcionales a ser preinstalados (por ejemplo, infra-applets para tarjetas de transporte y tarjetas de crédito) y datos necesarios para su envío a través de un canal de comunicación seguro (S430).

Cuando el terminal se reinicia después de que se haya enviado completamente el perfil o los datos en S430, el terminal realiza comunicaciones a través de la red del MNO1 y utiliza los servicios opcionales ofrecidos por el MNO1 (S440).

La figura 5 es un diagrama de flujo que ilustra un proceso de cambio de MNO usando un eSIM de acuerdo con una realización de ejemplo de la presente invención.

En la figura 5, el MNO1 es un MNO abierto inicialmente y MNO donador y el MNO2 es un MNO receptor después del cambio de MNO.

En el proceso de cambio de MNO usando el eSIM de acuerdo con la presente realización, se transmite un mensaje de solicitud de un cambio a otro proveedor de servicios o un cambio de MNO desde un sistema del MNO2 a un sistema del MNO1 (S510).

En S520, el sistema del MNO1 como el MNO abierto inicialmente y MNO donador genera un SD que tiene privilegio de gestión autorizado o privilegio de gestión delegado para el MNO2 usando una clave ISD. En este caso, una clave de SD del SD que tiene privilegio de gestión autorizado o privilegio de gestión delegado es una clave inyectada por adelantado desde el sistema del MNO2 al sistema del MNO1 a través de un módulo de seguridad de hardware (HSM). El sistema del MNO1 extradita el SD para disociar el SD generado de un ISD e inactiva un perfil del MNO1 (comunicaciones y servicios opcionales) del eSIM.

A continuación, el sistema del MNO1 notifica al sistema del MNO2 que el sistema del MNO1 está listo para un cambio a otro proveedor de servicios o un cambio de MNO (S530).

Se reinicia un terminal (S540) y se conecta a una red del MNO2 a través de un perfil de provisión. El sistema del MNO2 realiza una autorización de SD usando la clave de SD y envía aplicaciones de servicios opcionales preinstalados y datos de apertura usando el privilegio de gestión autorizado o privilegio de gestión delegado adquirido desde el ISD. A continuación, el sistema del MNO2 cambia la clave de SD a una clave reconocida solamente por el MNO2 (S550).

A continuación, cuando es reiniciado el terminal (S560), el terminal realiza comunicaciones a través de la red del MNO2 y utiliza servicios opcionales ofrecidos por el MNO2, mientras el sistema del MNO2 notifica al sistema del MNO1 que el envío está completado (S570).

La figura 6 es un diagrama de flujo que ilustra un proceso de cambio de MNO usando un eSIM de acuerdo con otra realización de ejemplo de la presente invención, en la que el MNO abierto inicialmente no es un MNO donador o receptor.

En la figura 6, a diferencia de la figura 5 en la que el MNO abierto inicialmente es un MNO donador, el MNO1 es el MNO abierto inicialmente, el MNO2 es un MNO donador antes de un cambio de MNO, y el MNO3 es un nuevo MNO receptor después del cambio de MNO.

En el proceso de cambio de MNO usando el eSIM de acuerdo con la presente realización, se transmite un mensaje de solicitud de un cambio a otro proveedor de servicios o un cambio de MNO desde un sistema del MNO3 a un sistema del MNO1 como el MNO abierto inicialmente (S610).

En S620, el sistema del MNO1 como el MNO abierto inicialmente genera un SD que tiene privilegio de gestión autorizado o privilegio de gestión delegado para el MNO3 como el MNO receptor usando una clave ISD. En este caso, una clave de SD del SD que tiene privilegio de gestión autorizado o privilegio de gestión delegado es una clave inyectada por adelantado desde el sistema del MNO3 al sistema del MNO1 a través de un módulo de seguridad de hardware (HSM). El sistema del MNO1 extradita el SD para disociar el SD generado de un ISD y borra un perfil del MNO2 como el MNO donador.

A continuación, el sistema del MNO1 notifica al sistema del MNO3 que el sistema del MNO1 está listo para un cambio a otro proveedor de servicios o para un cambio de MNO (S630).

Se reinicia un terminal (S640) y se conecta a una red del MNO3 a través de un perfil de provisión. El sistema del MNO3 realiza una autorización de SD usando la clave de SD y envía aplicaciones de servicios opcionales preinstalados y datos de apertura usando el privilegio de gestión autorizado o privilegio de gestión delegado adquirido desde el ISD. A continuación, el sistema del MNO3 cambia la clave de SD a una clave reconocida solamente por el MNO3 (S650).

A continuación, cuando es reiniciado el terminal (S660), el terminal realiza comunicaciones a través de la red del MNO3 y utiliza servicios opcionales ofrecidos por el MNO3, mientras el sistema del MNO3 notifica al sistema del MNO1 que el envío está completado (S670).

Esto es, en la realización ilustrada en la figura 5, dado que el MNO donador es el MNO abierto inicialmente, el perfil del MNO donador se inactiva en lugar de ser borrado. Sin embargo, en la realización mostrada en la figura 6, dado que el MNO donador es diferente del MNO abierto inicialmente, el perfil del MNO donador se borra.

De acuerdo con la realización mostrada en la figura 5, dado que el terminal puede volver al MNO abierto inicialmente como se ilustra en la figura 7, el perfil del MNO abierto inicialmente solamente se inactiva en lugar de ser borrado.

La figura 7 es un diagrama de flujo que ilustra un proceso de retorno a un MNO abierto inicialmente usando un eSIM de acuerdo con una realización de ejemplo de la presente invención.

En la figura 7, un terminal retorna desde el MNO2 actualmente en servicio al MNO1 como el MNO abierto inicialmente.

En el proceso de retornar al MNO abierto inicialmente usando el eSIM de acuerdo con la presente realización, el MNO1 pide al MNO2 un cambio al MNO abierto inicialmente (S710).

El terminal se reinicia (S720) y se conecta a una red del MNO1 a través de un perfil de provisión. El MNO1 borra un perfil del MNO2 (incluyendo un SD) usando una clave ISD y convierte un perfil inactivado del MNO1 en activado (S730).

A continuación, cuando es reiniciado el terminal (S740), el terminal realiza comunicaciones a través de la red del MNO1 y utiliza servicios opcionales ofrecidos por el MNO1 tal como lo hacía previamente el terminal. El sistema del MNO1 notifica al sistema del MNO2 que el terminal retorna completamente al operador móvil inicialmente abierto (S750).

De acuerdo con la presente invención anteriormente descrita, el MNO que contiene una clave IDS puede enviar un perfil de MNO a un terminal y permitir al terminal cambiar a otro operador móvil (otro MNO) sin cambio de la tecnología SIM existente en un entorno eSIM. En consecuencia, el MNO que contiene la clave ISD puede continuar asegurando la iniciativa en la apertura de la comunicación y actividades de servicios opcionales basándose en tecnologías estándar en el entorno eSIM.

Además, aunque no se describe en detalle para evitar redundancia, un eSIM, un sistema MNO, un método de provisión y un método de cambio de MNO que realiza una provisión y un cambio de MNO usando un SD que tiene privilegio de gestión autorizado o privilegio de gestión delegado puede realizarse como programas legibles por ordenador.

Estos programas pueden incluir códigos en lenguajes de programación tales como C, C++, JAVA y códigos de máquina legibles por un procesador de ordenador o CPU de modo que el ordenador lea los programas grabados en medios de registro para llevar a cabo las funcionalidades anteriores.

Los códigos pueden incluir códigos funcionales relacionados con las funciones que definen las funcionalidades anteriormente mencionadas y códigos de control relacionados con un procedimiento de ejecución necesario para que el procesador del ordenador ejecute las funcionalidades de acuerdo con un procedimiento preestablecido.

Además, los códigos pueden incluir adicionalmente códigos relacionados con referencias de memoria con relación a información adicional necesaria para que el procesador del ordenador realice las funcionalidades o una localización o dirección de una memoria interna o externa a la que se hace referencia en el medio.

Además, cuando el procesador del ordenador necesita comunicaciones con un ordenador o servidor remoto para realizar las funcionalidades, los códigos pueden incluir adicionalmente códigos relacionados con la comunicación con relación a cómo el procesador del ordenador comunica con qué ordenador o servidor remoto usando un módulo de comunicación basado en cable y/o inalámbrico y qué clase de información o medios transmite o recibe el procesador del ordenador en las comunicaciones.

Los programas funcionales, códigos relevantes y segmentos de código para implementar la presente invención pueden inferirse o deducirse fácilmente por un programador experto en la materia a la vista de la configuración del sistema de ordenador que lee los medios registrados para ejecutar los programas.

Ejemplos de medio de registro legible por ordenador que incluyen los programas pueden incluir ROM, RAM, CD-ROM, cintas magnéticas, discos flexibles y dispositivos de medios ópticos.

Además, los medios de registro legibles por ordenador que incluyen los programas pueden distribuirse a un sistema informático conectado a través de una red, y en consecuencia los códigos legibles por ordenador podrán almacenarse e implementarse de modo distribuido. En este caso, al menos uno de la pluralidad de ordenadores distribuidos puede implementar parte de las funcionalidades y transmitir el resultado de la implementación a al menos otro de los ordenadores distribuidos, y el otro ordenador que recibe el resultado puede implementar parte de las funcionalidades y proporcionar el resultado de la implementación a otros ordenadores distribuidos.

Particularmente, un medio de registro legible por ordenador que incluye una aplicación para la ejecución de una pluralidad de funciones o métodos relacionados con la autenticación de una eUICC de acuerdo con la realización de ejemplo de la presente invención puede ser un servidor de almacén de aplicaciones, un medio de almacenamiento, tal como un disco duro, incluido en un servidor proveedor de aplicaciones, tal como un servidor web asociado con la aplicación o servicio correspondiente, o un servidor proveedor de aplicaciones.

Aunque los elementos mostrados en las realizaciones de ejemplo de la presente invención se describen como constituidos u operando independientemente, la presente invención no está limitada a las realizaciones ilustradas. Esto es, uno o más elementos selectivos pueden combinarse para funcionar dentro del alcance de la presente invención. Además, cada elemento puede construirse como un constituyente de hardware separado, mientras que parte o la totalidad de estos elementos pueden combinarse también selectivamente para formar un programa informático que tenga un módulo de programa que lleva a cabo algunas o todas las funciones combinadas de uno o de una pluralidad de constituyentes de hardware. Los códigos y segmentos de códigos para constituir el programa informático pueden inferirse fácilmente por los expertos en la materia. El programa informático se almacena en un medio legible por ordenador y se lee e implementa en el ordenador para conseguir la realización de ejemplo de la presente invención. Los medios que almacenan el programa informático pueden incluir medios de registro magnéticos, medios de registro ópticos y medios de onda portadora.

Los términos “incluyendo” “comprendiendo” o “teniendo” pueden interpretarse para indicar un cierto elemento constituyente, pero no pueden interpretarse para excluir la existencia de, o una posibilidad de una adición de, uno o más otros elementos constituyentes. A menos que se defina lo contrario, todos los términos que incluyen términos técnicos y científicos usados en el presente documento tienen el mismo significado que se entiende comúnmente por un experto en la materia a la que pertenece la invención. Se entenderá adicionalmente que términos, tales como los definidos en los diccionarios normalmente usados, deberían interpretarse como teniendo un significado que es consistente con su significado en el contexto de la técnica relevante y no se interpretarán en un sentido idealizado o excesivamente formal a menos que expresamente se defina así en el presente documento.

Mientras que se han mostrado y descrito unas pocas realizaciones de ejemplo con referencia a los dibujos adjuntos, será evidente para los expertos en la materia que pueden realizarse diversas modificaciones y variaciones a partir de las descripciones precedentes sin apartarse de la esencia de la presente invención. Las realizaciones de ejemplo se proporcionan no para restringir el concepto de la presente invención sino para ilustrar la presente invención y no limitan el alcance de la presente invención. El alcance de la invención se define por las reivindicaciones adjuntas, y todas las diferencias dentro del alcance serán interpretadas como incluidas dentro de las reivindicaciones adjuntas de la presente invención.

REIVINDICACIONES

1. Un método de cambio de un operador de red móvil, MNO, usando un módulo de identidad de abonado embebido, eSIM (300), enlazado a al menos un MNO, almacenando el eSIM un perfil de provisión (310) y un perfil (331, 341) del al menos un MNO, comprendiendo el método:

recibir, por el eSIM, un dominio de seguridad, SD (340), de un MNO receptor (370) desde un MNO donador (360), en donde un SD es una aplicación privilegiada que tiene claves criptográficas usadas para soportar la operación de protocolo de canal seguro o para autorizar una función de gestión del contenido de la tarjeta, siendo el MNO receptor el MNO después de un cambio de MNO, siendo el MNO donador el MNO antes del cambio de MNO, y
en donde el SD del MNO donador gestiona un primer perfil (331) del MNO donador mediante el uso de una clave criptográfica del SD del MNO donador, por el MNO donador, el SD del MNO receptor mediante la realización de una extradición de SD para disociar el SD del MNO receptor de un dominio de seguridad de emisor, ISD;
conectar, por el eSIM, al MNO receptor usando el perfil de provisión;
realizar, por el eSIM, una autorización de SD usando la clave criptográfica del SD del MNO receptor y recibir un segundo perfil o datos usando el privilegio del SD del MNO receptor,
en donde el SD del MNO receptor gestiona el segundo perfil del MNO receptor mediante el uso de la clave criptográfica del SD del MNO receptor;
inactivar, por el eSIM, el primer perfil del MNO donador cuando el eSIM recibe el SD del MNO receptor que tiene un privilegio de gestión delegado o un privilegio de gestión autorizado sobre el MNO receptor, desde el sistema del MNO donador; y
cambiar, por el eSIM, un valor clave de la clave criptográfica del SD del MNO receptor a un valor de clave único reconocido solamente por el MNO receptor después de que el eSIM se envíe con el segundo perfil o datos para el MNO receptor.

2. El método de la reivindicación 1, que comprende adicionalmente:

recibir una solicitud de retorno desde un sistema de MNO abierto inicialmente;
conectar al sistema del MNO abierto inicialmente usando el perfil de provisión; y
borrar un perfil actualmente activado que incluye un dominio de seguridad, SD, de un MNO usando el ISD, y convertir en activado un perfil inactivado del MNO abierto inicialmente.

3. El método de la reivindicación 1, en el que, en respuesta a un MNO abierto inicialmente que no es el mismo que el MNO donador y que sucede un cambio de suscripción desde el MNO donador al MNO receptor,
recibir el SD que tiene privilegio de gestión delegado o privilegio de gestión autorizado sobre el MNO receptor desde el MNO abierto inicialmente;
borrar un perfil del MNO donador; y
conectar al sistema del MNO receptor usando el perfil de provisión, y a continuación realizar una autorización de SD y recibir el perfil o datos.

4. El método de la reivindicación 1, que comprende adicionalmente:

transmitir un mensaje de solicitud de cambio de MNO desde el MNO receptor al MNO donador;
generar un dominio de seguridad, SD, que tiene privilegio de gestión delegado o privilegio de gestión autorizado sobre el MNO receptor por el MNO donador usando una clave ISD; y
conectar al sistema del MNO receptor y ser provisto de un servicio por un terminal equipado con el eSIM después de haber arrancado.

5. El método de la reivindicación 4, en el que una clave de SD del SD que tiene privilegio de gestión delegado o privilegio de gestión autorizado sobre el MNO receptor la transmite o la inyecta por adelantado el MNO receptor al MNO donador previamente al cambio de un MNO por el terminal de usuario.

6. El método de la reivindicación 3, que comprende adicionalmente:

transmitir un mensaje de solicitud de cambio de MNO desde el MNO receptor al MNO abierto inicialmente;
generar un SD que tiene privilegio de gestión delegado o privilegio de gestión autorizado sobre el MNO receptor por el sistema del MNO abierto inicialmente usando una clave ISD; y
conectar al MNO receptor y ser provisto con un servicio por un terminal equipado con el eSIM después de que ha arrancado un terminal móvil que tiene el eSIM embebido en él.

7. El método de la reivindicación 6, en el que el MNO receptor transmite o inyecta por adelantado una clave de SD del SD, que tiene privilegio de gestión delegado o privilegio de gestión autorizado sobre el MNO receptor, al MNO abierto inicialmente.

8. El método de la reivindicación 6, que comprende además extraditar, por el MNO abierto inicialmente, el SD para disociar el SD del MNO donador del ISD.

FIG. 1

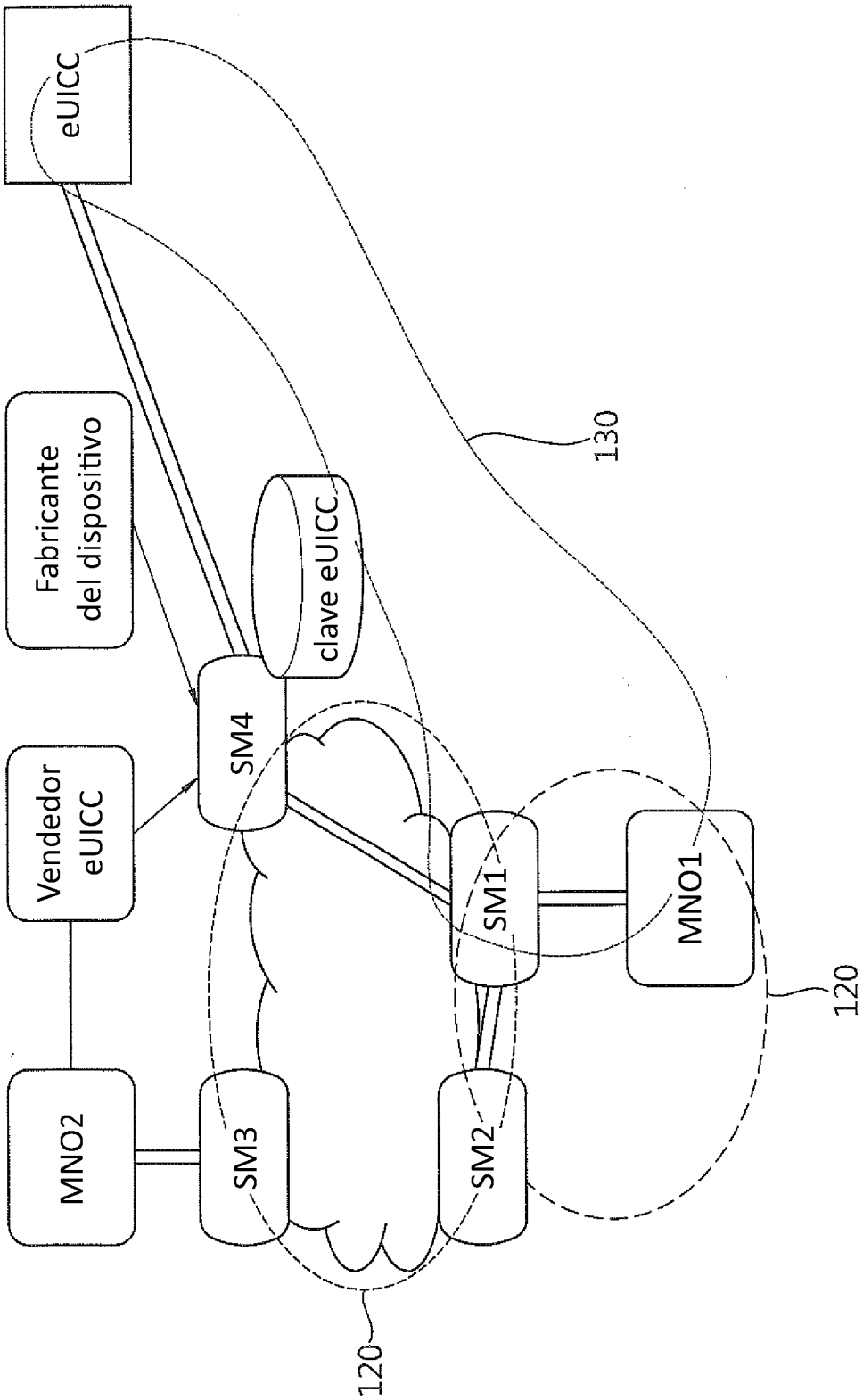

eUICC
Fabricante del dispositivo
Vendedor eUICC
MNO2
SM4
clave eUICC
SM3
SM2
SM1
MNO1
130
120
120

FIG. 2

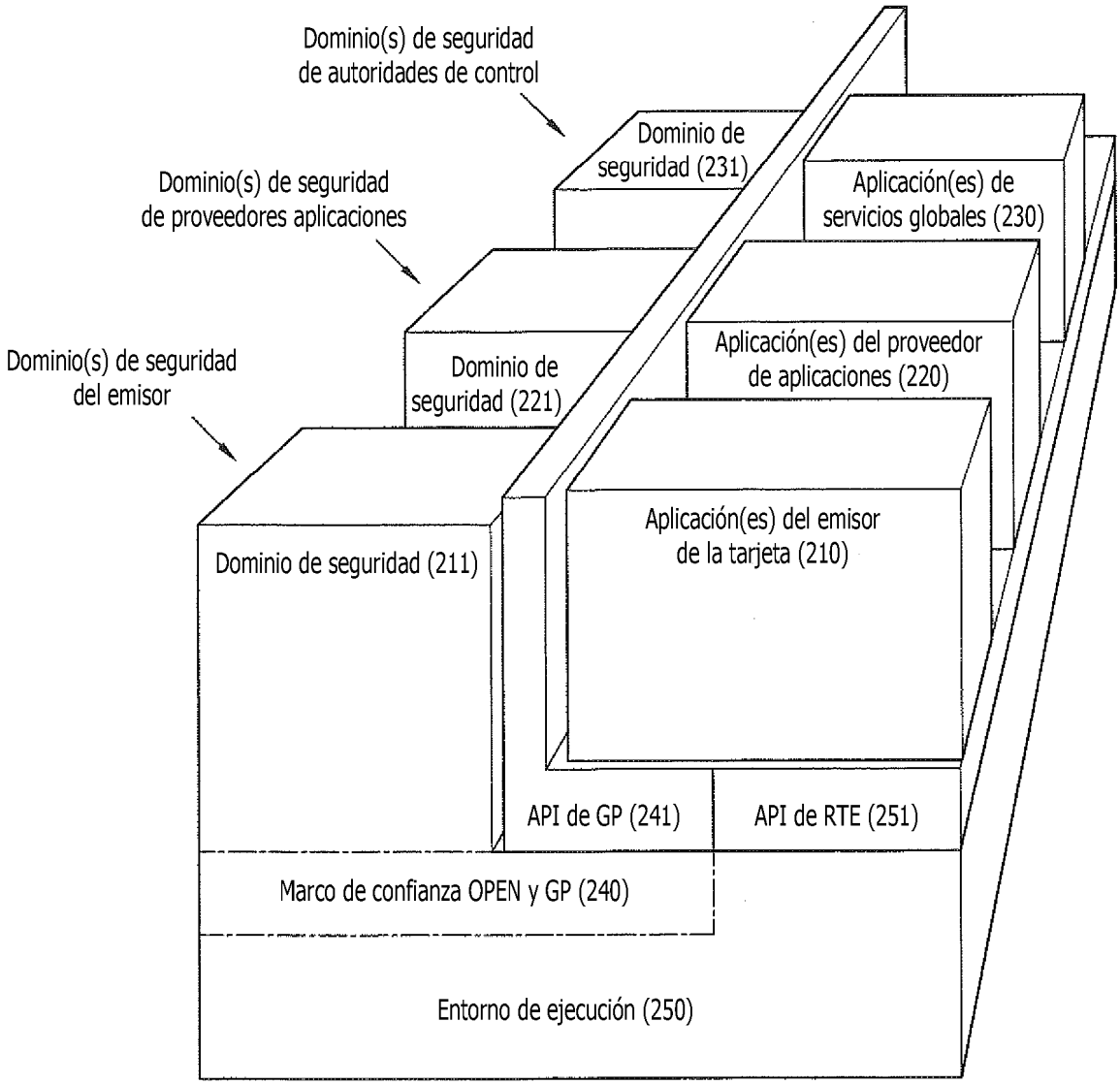

Dominio(s) de seguridad de autoridades de control
Dominio de seguridad (231)
Aplicación(es) de servicios globales (230)
Dominio(s) de seguridad de proveedores aplicaciones
Dominio de seguridad (221)
Aplicación(es) del proveedor de aplicaciones (220)
Dominio(s) de seguridad del emisor
Dominio de seguridad (211)
Aplicación(es) del emisor de la tarjeta (210)
API de GP (241)
API de RTE (251)
Marco de confianza OPEN y GP (240)
Entorno de ejecución (250)

FIG. 3

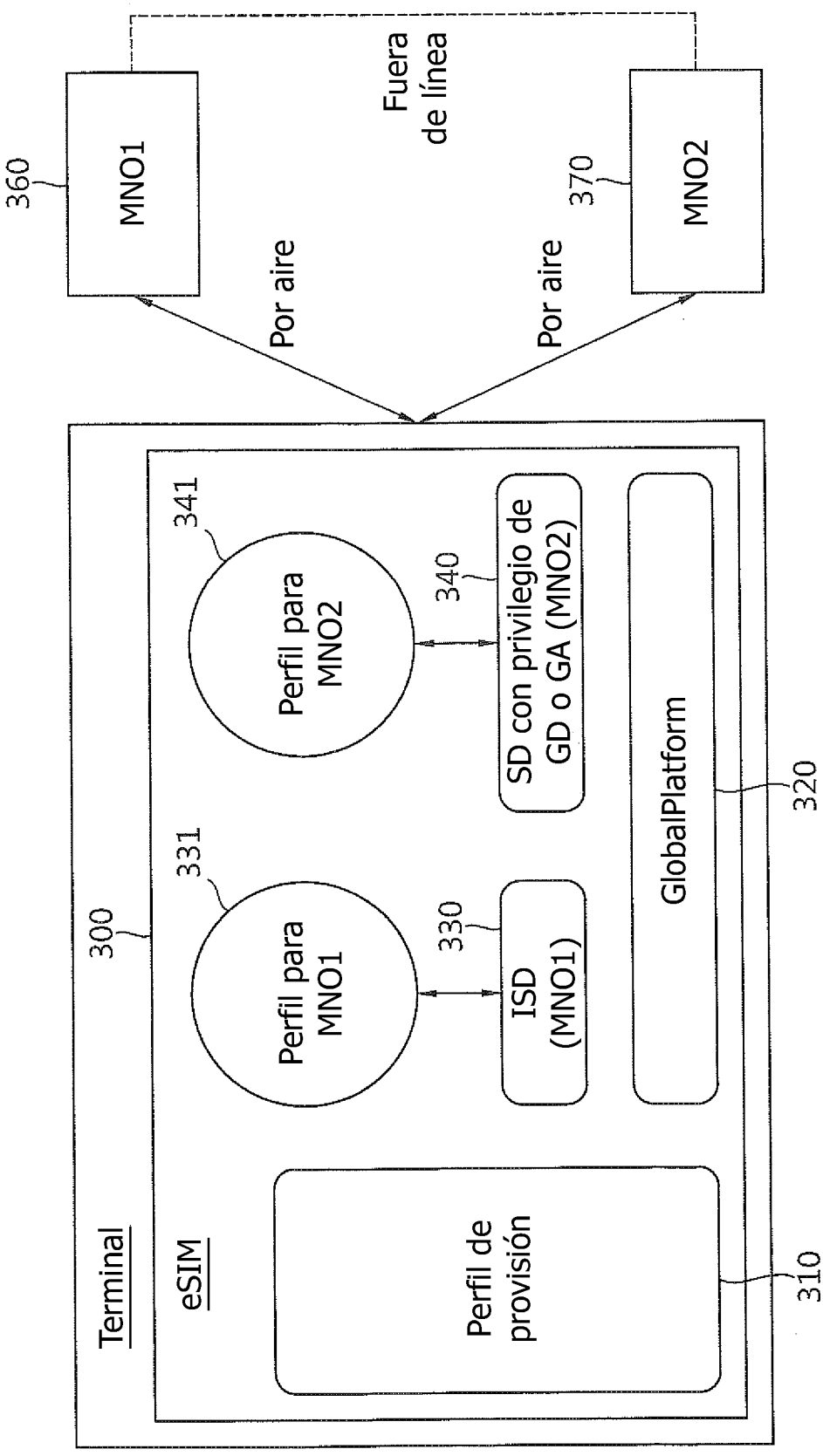

360
MNO1
Fuera de línea
370
MNO2
Por aire
Por aire
Terminal
300
eSIM
341
Perfil para MNO2
340
SD con privilegio de GD o GA (MNO2)
331
Perfil para MNO1
330
ISD (MNO1)
GlobalPlatform
320
Perfil de provisión
310

FIG. 4

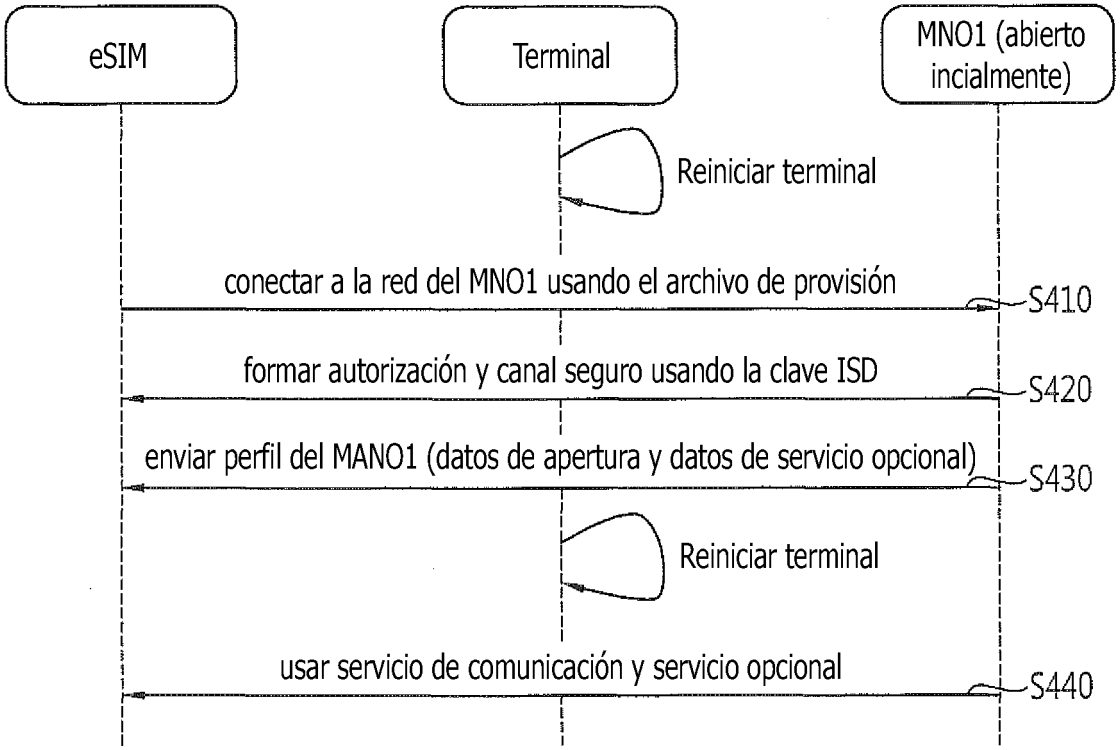

eSIM
Terminal
MNO1 (abierto incialmente)
Reiniciar terminal
conectar a la red del MNO1 usando el archivo de provisión
S410
formar autorización y canal seguro usando la clave ISD
S420
enviar perfil del MANO1 (datos de apertura y datos de servicio opcional)
S430
Reiniciar terminal
usar servicio de comunicación y servicio opcional
S440

FIG. 5

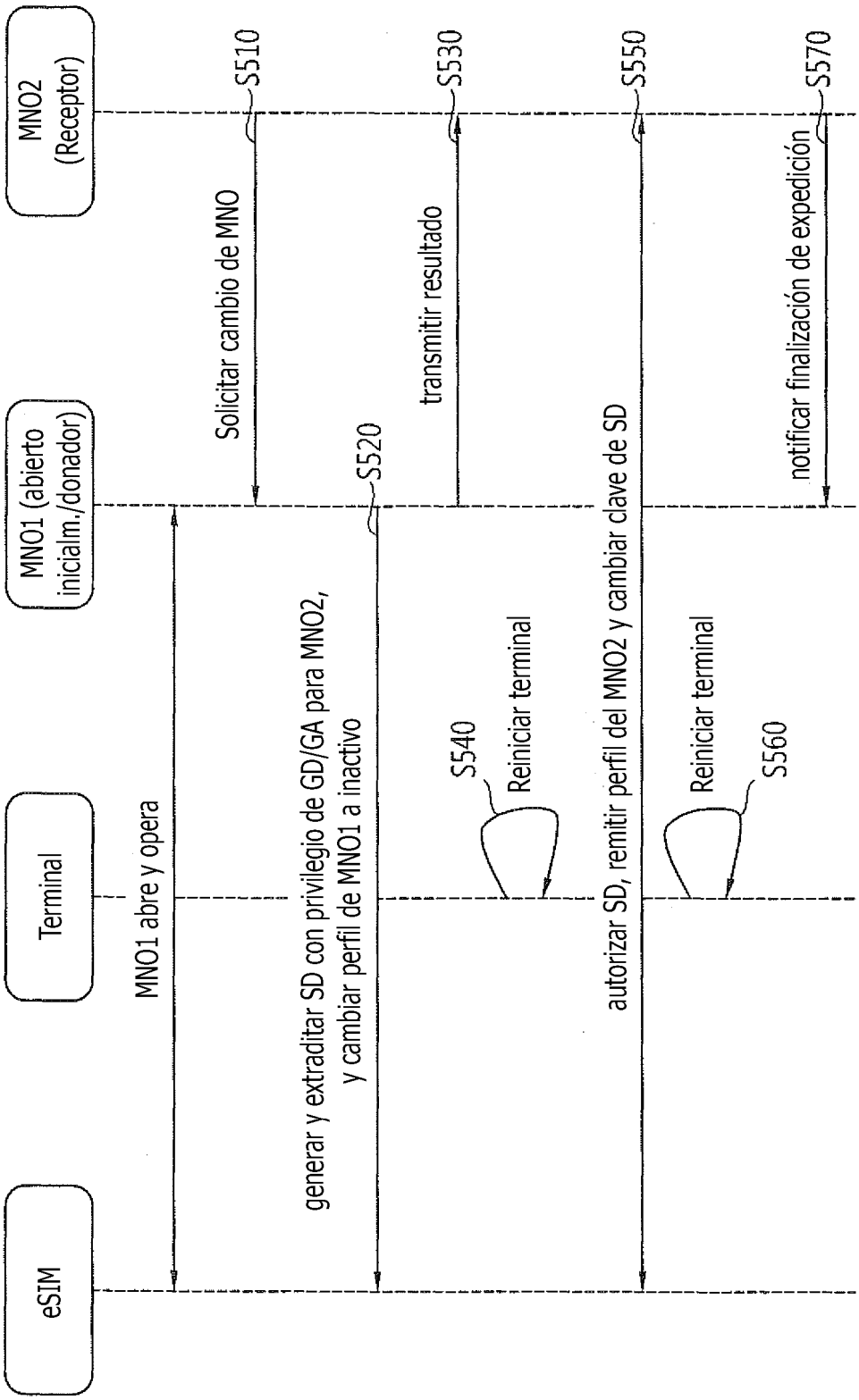

eSIM
Terminal
MNO1 (abierto inicialm./donador)
MNO2 (Receptor)
MNO1 abre y opera
Solicitar cambio de MNO
S510
generar y extraditar SD con privilegio de GD/GA para MNO2, y cambiar perfil de MNO1 a inactivo
S520
transmitir resultado
S530
S540
Reiniciar terminal
autorizar SD, remitir perfil del MNO2 y cambiar clave de SD
S550
Reiniciar terminal
S560
notificar finalización de expedición
S570

FIG. 6

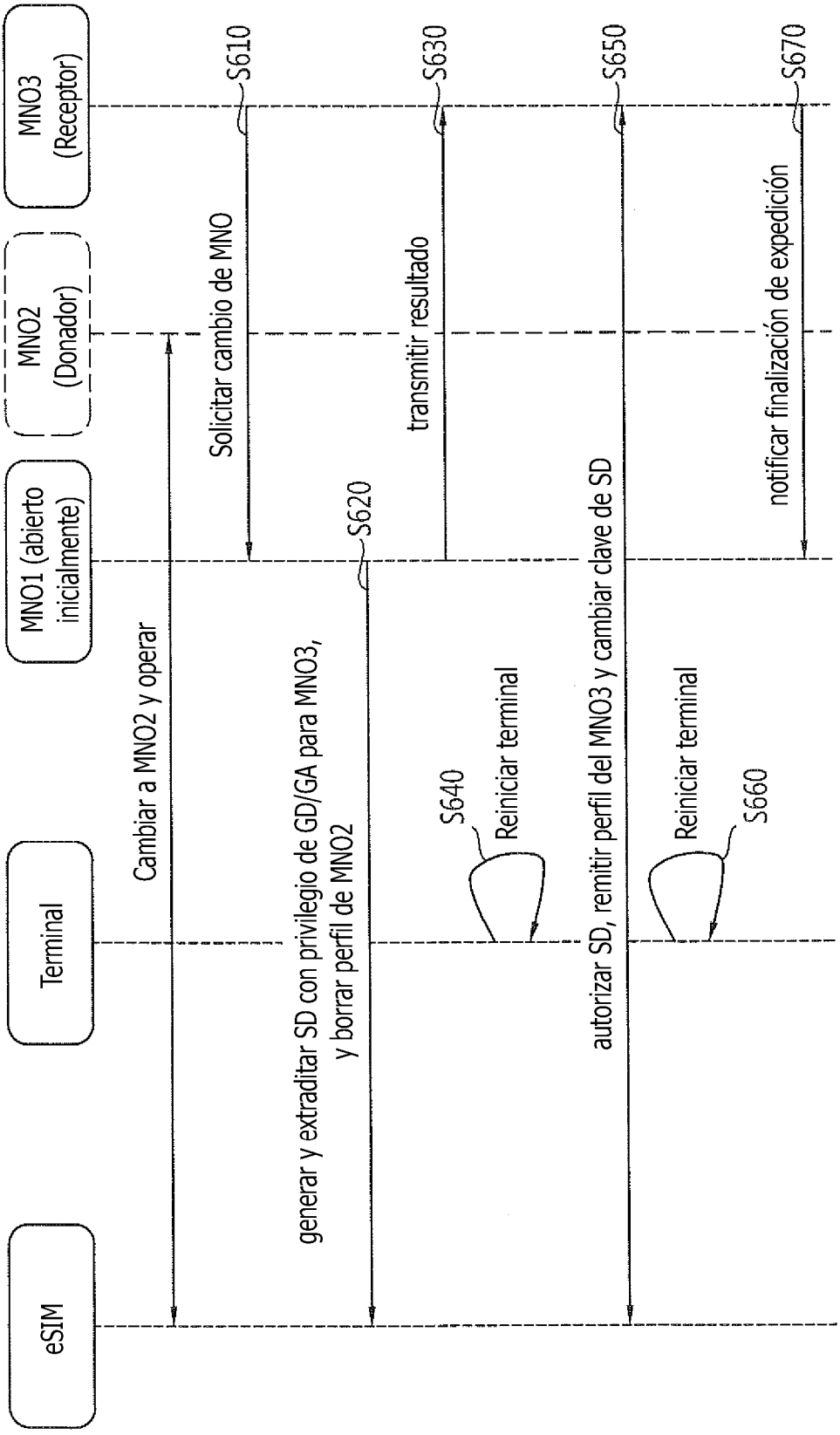
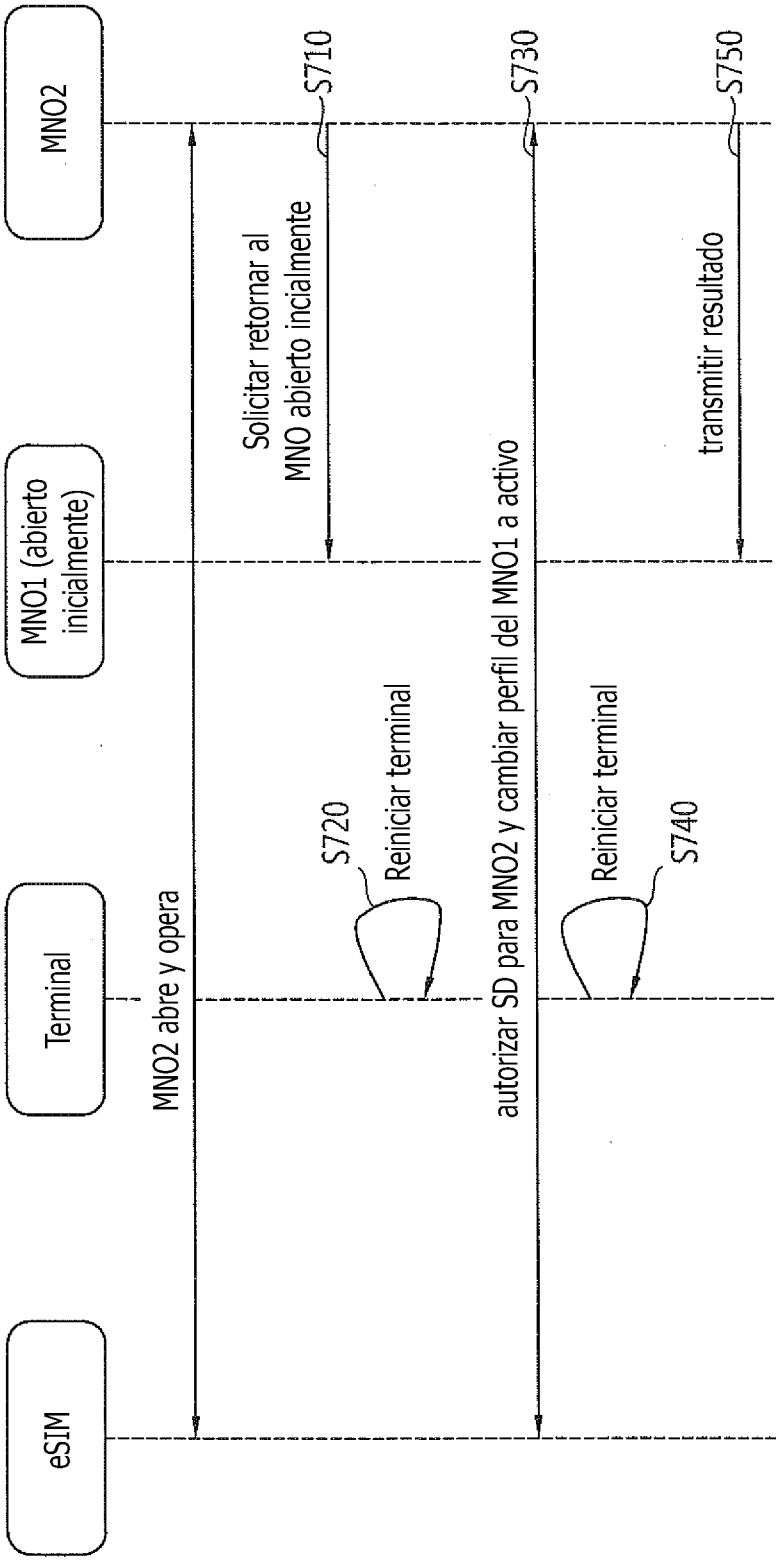

eSIM
Terminal
MNO1 (abierto inicialmente)
MNO2 (Donador)
MNO3 (Receptor)
Cambiar a MNO2 y operar
Solicitar cambio de MNO
S610
generar y extraditar SD con privilegio de GD/GA para MNO3, y borrar perfil de MNO2
S620
transmitir resultado
S630
S640
Reiniciar terminal
autorizar SD, remitir perfil del MNO3 y cambiar clave de SD
S650
Reiniciar terminal
S660
notificar finalización de expedición
S670

FIG. 7


eSIM
Terminal
MNO1 (abierto inicialmente)
MNO2
MNO2 abre y opera
S710
Solicitar retornar al MNO abierto incialmente
S720
Reiniciar terminal
S730
autorizar SD para MNO2 y cambiar perfil del MNO1 a activo
S740
Reiniciar terminal
S750
transmitir resultado