(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 803 703**

(51) Int. CI.:

G06F 21/31 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.06.2016 PCT/FR2016/051605**

(87) Fecha y número de publicación internacional: **05.01.2017 WO17001770**

(96) Fecha de presentación y número de la solicitud europea: **28.06.2016 E 16747819 (7)**

(97) Fecha y número de publicación de la concesión europea: **13.05.2020 EP 3317800**

(54) Título: **Método de gestión de perfiles en un elemento seguro**

(30) Prioridad:

30.06.2015 FR 1556148

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.01.2021

(73) Titular/es:

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

(72) Inventor/es:

DUMOULIN, JÉRÔME y
MICHEL, ALEXIS

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de gestión de perfiles en un elemento seguro

La presente invención se refiere a un método de gestión de perfiles en un elemento seguro.

Un elemento seguro, tal como una tarjeta electrónica, se utiliza en un dispositivo host. El dispositivo host es, por ejemplo, un teléfono móvil u otro terminal móvil de comunicación, tal como una tableta electrónica.

Un elemento seguro puede integrarse de forma desmontable en el dispositivo host, tal como una tarjeta de tipo UICC (por ""Universal Integrated Circuit Card" – "Tarjeta de Circuito Integrado Universal") mencionada en la norma ETSI TS 102 221, y reagrupa las tarjetas electrónicas convencionales, tipo tarjeta SIM (o USIM - por "Universal Subscriber Identity Module" – "Módulo de Identidad de Abonado Universal"), pero sino también fichas (token) seguras, todas ellas identificables de forma única. El segundo tipo de elemento seguro mencionado puede integrarse (por ejemplo, soldarse) en el dispositivo host, tal, como, por ejemplo, una tarjeta del tipo eUICC (por "embeded Universal Integrated Circuit Card" – "Tarjeta de Circuito Integrado Universal integrada") y se hace referencia en la norma ETSI TS 103 383. A un elemento seguro integrado bajo la denominación de eSE se conoce en la nomenclatura anglosajona como "embeded secure element" – "elemento seguro integrado" y se hace referencia en la especificación de la tarjeta GlobalPlatform Versión 2.2.1 de la tecnología GlobalPlatform.

Por lo tanto, un usuario del dispositivo host puede sustituir una primera tarjeta del tipo UICC con una segunda tarjeta del tipo UICC, por ejemplo, cuando desea cambiar de una primera red de comunicación gestionada por un primer operador a una segunda red de comunicación gestionada por un segundo operador que posiblemente puede ser el mismo operador.

Conviene señalar que una red de comunicación incluye un conjunto de equipos de un operador que permite la conexión y conectividad de sus abonados. Dos redes de comunicación, en particular redes de telefonía móvil, pueden basarse en la misma infraestructura, aparte de algunos equipos específicos para cada operador.

Conviene señalar que el usuario no puede sustituir fácilmente una tarjeta de tipo eUICC dentro del dispositivo host.

Sin embargo, los elementos seguros, ya sean integrados o no, pueden operar de conformidad con diferentes perfiles cargados en la memoria, para cambiar de una primera red de comunicación gestionada por un operador a una segunda red de comunicación gestionada por un segundo operador, posiblemente idéntico al primer operador. Cada perfil se identifica en el elemento seguro mediante un identificador único.

De conformidad con la norma GSMA 12FAST.15, un perfil es una combinación de una estructura de archivos, datos y aplicaciones disponible o presente en el elemento seguro y que permite el acceso a una infraestructura de red de comunicación cuando se activa.

Un perfil está activo cuando la estructura de archivos y/o las aplicaciones se pueden seleccionar a través de una interfaz del dispositivo host que contiene el elemento seguro, tal como una tarjeta del tipo eUICC o del tipo UICC.

Las normas GSMA 12FAST.13 y GSMA 12FAST.15 proporcionan un procedimiento de activación de perfil, en particular utilizando órdenes ad hoc.

Además, estas normas proporcionan un procedimiento alternativo de activación o réplica o un mecanismo alternativo o de réplica ("Procedimiento de Activación de Fall-back" o "Mecanismo de Fall-back") para cambiar de manera automática de un perfil activo a un perfil de réplica en condiciones especiales de funcionamiento.

Este procedimiento de réplica se inicia, en particular, cuando el elemento seguro, tal como una tarjeta del tipo eUICC, pierde la conexión con la infraestructura de la red de comunicación a la que está conectada previamente con el perfil que se ha activado o "perfil activo". Este procedimiento se describe en el apartado 3.16 de la norma GSMA 12FAST.15 y en el apartado 3.5.13 de la norma GSMA 12FAST.13.

Durante este procedimiento, el elemento seguro pone en práctica una desactivación del perfil activo y una activación de otro perfil, identificado por un "Atributo de Fall-back" activado.

De conformidad con las normas GSMA 12FAST.13 y GSMA 12FAST.15, el atributo "Fall-back" es un atributo que permite que la identificación del perfil se active en el mecanismo de réplica ("Mecanismo de Fall-back"). Solamente un perfil a la vez dentro de una tarjeta de tipo eUICC puede tener activado el atributo "Fall-back" (consúltese la norma GSMA 12FAST.15 en la sección 4.1.1.7).

Por lo tanto, cuando la tarjeta de tipo eUICC o cualquier elemento seguro pierde la conexión que tiene con una primera red de comunicación a través de un perfil asociado con la primera red de comunicación, puede cambiar de manera automática a una segunda red de comunicación utilizando un segundo perfil asociado con la segunda red de comunicación, habiéndose activado el segundo perfil mediante el procedimiento de réplica.

Por lo tanto, el eUICC recupera una conexión y una conectividad.

La gestión de perfiles que actualmente ofrecen estas normas no es satisfactoria.

La presente invención propone mejorar esta situación.

Con este fin, la presente invención proporciona, según un primer aspecto, un método de gestión de perfiles en un elemento seguro, comprendiendo el elemento seguro un primer perfil asociado con una primera red de comunicación y un segundo perfil asociado con una segunda red de comunicación, estando el primer perfil activo, cuyo método comprende las etapas de:

- desactivación del primer perfil; y

- activación del segundo perfil.

El método de gestión de perfiles se caracteriza porque las etapas de desactivación y activación se ponen en práctica después de la detección de un fallo durante una verificación local puesta en práctica en dicho elemento seguro y relativo al primer perfil para el uso de dicho primer perfil.

Por supuesto, dicha detección puede incluir una o varias etapas de verificación relacionadas con el primer perfil, por ejemplo, verificaciones relacionadas con la seguridad con respecto al primer perfil. Y es durante un fallo de verificación cuando se ponen en práctica la desactivación y la activación.

Por lo tanto, cuando se detecta un fallo, el elemento seguro pone en práctica la activación de un segundo perfil en detrimento del primer perfil defectuoso. El elemento seguro puede utilizarse a continuación a través del segundo perfil, sin permanecer inoperativo.

Dicho de otro modo, el elemento seguro vuelve a estar disponible para su uso, mientras que el primer perfil activo ha fallado o está bloqueado.

De hecho, además de la pérdida de la conexión a la infraestructura de la red de comunicación según lo previsto en la norma, otras situaciones hacen que el elemento seguro, así como el dispositivo host que contiene el elemento seguro, sea inutilizable y, por lo tanto, incapaces de conectarse a la red de comunicación.

Este es, por ejemplo, el caso cuando el elemento seguro pone en práctica verificaciones relacionadas con la seguridad en el uso de un dispositivo host a través de un perfil, tal como verificar la autenticación de un usuario o de la infraestructura de la red de comunicación, o de la integridad de los datos o aplicaciones descargados en el elemento seguro y, en consecuencia, modificando el perfil activo y poniendo en peligro su integridad operativa.

Según una característica, el elemento seguro no es extraíble en un dispositivo host.

Según una característica, el método de gestión de perfiles comprende una etapa de enviar, a un dispositivo host conectado a dicho elemento seguro, una orden para reiniciar el elemento seguro para activar un procedimiento para conexión del elemento seguro a la segunda red de comunicación utilizando el segundo perfil activado.

Según otra característica, el método de gestión de perfiles comprende una etapa de notificación de la desactivación del primer perfil y de la activación del segundo perfil, a las infraestructuras asociadas respectivamente con la primera y la segunda redes de comunicación.

Según una forma de realización, la verificación local comprende una etapa de verificación en el elemento seguro de la autorización del acceso de un usuario a dicho primer perfil. En este caso, se detecta un fallo de seguridad en el elemento seguro en caso de fallo de verificación.

De este modo, se verifica la autorización del acceso de un usuario al primer perfil. Por supuesto, otras condiciones pueden intervenir para determinar que la verificación condujo a un fallo. Por ejemplo, en los ejemplos a continuación descritos, es común esperar tres verificaciones incorrectas de un código de tipo PIN para activar una acción de seguridad, por ejemplo, el bloqueo de la tarjeta. Es cuando se bloquea la tarjeta que se detecta el fallo de seguridad.

Según una característica, la verificación en el elemento seguro de la autorización del acceso de un usuario comprende la verificación de un número de identificación personal (PIN) asociado con el primer perfil.

Según otra característica, la verificación en el elemento seguro de la autorización del acceso de un usuario comprende la verificación de una clave de desbloqueo personal (PUK) asociada con el primer perfil.

Según una característica particular, el método de gestión de perfiles comprende una etapa de bloqueo del perfil activo del elemento seguro durante el fallo de verificación. Por lo tanto, cuando se realiza una comprobación de seguridad con respecto a un perfil activo, el perfil activo se bloquea, quedando el elemento seguro inutilizable a través de este perfil.

Por ejemplo, cuando ocurre un fallo durante la verificación de seguridad del perfil activo, se genera un mensaje de error que contiene información representativa del fallo.

Según otra característica, la verificación en el elemento seguro de la autorización del acceso de un usuario incluye la verificación de los datos de autenticación del usuario.

Por lo tanto, se verifica la autorización de una red de comunicación para acceder al primer perfil.

En una forma de realización, la verificación local incluye una etapa de verificación de la integridad del primer perfil para detectar la operación incorrecta de este último.

Por lo tanto, hay una verificación de la operación incorrecta o no incorrecta del primer perfil, y/o de las funcionalidades basadas directamente en este primer perfil.

Por lo tanto, está prevista una verificación de la operación incorrecta o no incorrecta del primer perfil, y/o de las funcionalidades basadas directamente en este primer perfil.

El funcionamiento del primer perfil puede ser erróneo cuando el primer perfil se modifica con datos erróneos o incorrectos.

Según una característica, la verificación de la integridad de dicho primer perfil se lleva a cabo durante una fase de activación de dicho primer perfil.

Según una característica, el método de gestión de perfiles comprende, además, una etapa de reactivación del primer perfil, comprendiendo dicha etapa de reactivación la desactivación del segundo perfil y la activación del primer perfil.

De este modo, una vez que el primer perfil ha sido desactivado y el segundo perfil ha sido activado, el primer perfil se reactiva.

De conformidad con una forma de realización, la etapa de reactivación del primer perfil se pone en práctica al recibir, en dicho elemento seguro, una demanda para activar el primer perfil, procediendo dicha demanda de activación desde la primera red de comunicación asociada con el primer perfil.

Según una característica, la demanda para activar el primer perfil se genera a petición de un usuario.

De manera alternativa, la demanda para activar el primer perfil se genera después de la finalización de un período de tiempo predeterminado a partir de una notificación que informa de la desactivación de dicho primer perfil en el elemento seguro.

Según un segundo aspecto, la invención se refiere a un elemento seguro que comprende un primer perfil asociado con una primera red de comunicación y un segundo perfil asociado con una segunda red de comunicación, estando activo el primer perfil, cuyo elemento seguro comprende:

- medios de desactivación del primer perfil; y
- medios de activación del segundo perfil;

estando el elemento seguro configurado de modo que los medios de desactivación y activación se pongan en práctica después de la detección de un fallo durante una verificación local realizada en dicho elemento seguro y en relación con dicho primer perfil para el uso de este denominado primer perfil.

La invención se refiere según un tercer aspecto, a un dispositivo host que comprende un elemento seguro de conformidad con la invención.

En una forma de realización, el dispositivo host es un terminal móvil de comunicación.

El elemento seguro y el dispositivo host tienen características y ventajas similares a las descritas con anterioridad en relación con el método de gestión de perfiles.

Otras características y ventajas de la invención aparecerán en la descripción siguiente.

En los dibujos adjuntos, dados a modo de ejemplos no limitativos:

La Figura 1 representa, de manera esquemática, un dispositivo host que comprende un elemento seguro integrado de conformidad con una forma de realización de la invención;

La Figura 2 ilustra, de manera esquemática, un ejemplo de un sistema de comunicación en donde se puede poner en práctica una forma de realización de la presente invención; y

Las Figuras 3 y 4 representan, de manera esquemática, las etapas de un método para cambiar un perfil de conformidad con una forma de realización de la invención.

La Figura 1 muestra, de manera esquemática, un dispositivo host 10 que comprende un elemento seguro 20 de conformidad con una forma de realización de la invención.

El dispositivo host 10 es, por ejemplo, un terminal móvil, un teléfono móvil, una tableta digital o cualquier tipo de equipo electrónico, tal como un contador eléctrico, un vehículo, una máquina de café, etc. El elemento seguro 20 está incorporado en el dispositivo host 10.

El dispositivo host 10 comprende un bus de comunicación 100 al que están conectadas:

- una unidad de procesamiento 11, denominada en la figura como CPU (por "Central Processing Unit" – "Unidad Central de Procesamiento") y que puede comprender uno o más procesadores;
- una memoria no volátil 12, por ejemplo, memoria ROM (por "Read Only Memory" – "Memoria de Solo Lectura"), memoria EEPROM (por "Electrically Erasable Read Only Memory" – "Memoria de Solo Lectura Eléctricamente Borrable") o una memoria instantánea;
- una memoria de acceso aleatorio 13 o memoria RAM (por "Random Access Memory" – "Memoria de Acceso Aleatorio");
- una interfaz de entrada/salida 14, denominada en la Figura I/O (por "Imput/Output" – "Entrada/Salida"), por ejemplo, una pantalla, un teclado, un ratón u otro dispositivo señalador, tal como una pantalla táctil o un control remoto que permite a un usuario interactuar con el sistema a través de una interfaz gráfica; y
- una interfaz de comunicación 150, denominada COM en la figura, adecuada para intercambiar datos, por ejemplo, con un servidor SM-SR a través de una red, o de una interfaz de lectura/escritura.

El elemento seguro 20 es, por ejemplo, una tarjeta de circuito integrado universal e integrada (eUICC) conforme a la norma ETSI TS 103 383 o la norma ETSI 102 221.

Incluye un bus de comunicación 200 al que están conectadas:

- una unidad de procesamiento 21 o microprocesador, denominada en la figura CPU (por "Central Processing Unit" – "Unidad Central de Procesamiento");
- una memoria no volátil 22, por ejemplo, memoria ROM (por "Read Only Memory" – "Memoria de Solo Lectura"), memoria EEPROM (por "Electrically Erasable Read Only Memory" – "Memoria de Solo Lectura Eléctricamente Borrable") o memoria instantánea;
- una memoria de acceso aleatorio 23 o memoria RAM (por "Random Access Memory" – "Memoria de Acceso Aleatorio"); y
- una interfaz de comunicación 24, denominada COM en la figura, adaptada para intercambiar datos con el procesador 11 del dispositivo host 10.

La memoria 23 incluye registros adecuados para registrar las variables y parámetros creados y modificados durante la ejecución de un programa informático que comprende instrucciones para poner en práctica un método de conformidad con la invención. Los códigos de instrucciones del programa almacenados en la memoria no volátil 22 se cargan en la memoria RAM 23 para ser ejecutados por la unidad de procesamiento CPU 21.

La memoria no volátil 22 es, por ejemplo, una memoria regrabable del tipo EEPROM o memoria instantánea que puede constituir un soporte dentro del significado de la invención, es decir, que puede comprender un programa informático que comprende instrucciones para la puesta en práctica de los métodos según con la invención.

La Figura 2 muestra, de manera esquemática, un ejemplo de un sistema de comunicación en donde se puede poner en práctica una forma de realización de la presente invención.

En particular, la Figura 2 representa un dispositivo host 10 que comprende un elemento seguro 20, una primera red de comunicación 30 y una segunda red de comunicación 40.

La primera red de comunicación 30 y la segunda red de comunicación 40 son, por ejemplo, redes de telefonía móvil.

El dispositivo host 10 y el elemento seguro 20 se ilustran en la Figura 1.

El dispositivo host 10 es, por ejemplo, un terminal móvil, tal como un teléfono móvil o una tableta electrónica, y el elemento seguro 20 es un elemento seguro integrado, tal como una tarjeta del tipo eUICC.

En la forma de realización descrita, el elemento seguro 20 puede comunicarse con dos redes de comunicación 30, 40.

Un operador de una red de comunicación 30, 40 está representado por un servidor de preparación de los datos 320, 420, denominado SM-DP (por Subscription Manager Data Preparation” - "Preparación de Datos de Gestor de Suscripción"). Un servidor SM-DP 320, 420 genera perfiles y los proporciona al elemento seguro 20.

Por lo tanto, en la forma de realización descrita con anterioridad, dos servidores SM-DP representan, respectivamente, dos operadores de las dos redes de comunicación 30, 40.

Un servidor SM-SR 310 (por “Subscription Manager Secure Routine” - "Rutina Segura de Gestor de Suscripción") es una entidad representativa del elemento seguro 20 y está configurado para comunicarse con los servidores SM-DP 320, 420.

El conjunto formado por un servidor SM-DP 320, 420 y por el único servidor SM-SR 310 forma un servidor de gestión de suscripción denominado SM (por “Subscription Manager” - "Gestor de Suscripción") 300, 400.

De hecho, se trata de un servidor SM "virtual" en cuanto se utiliza un único servidor SM-SR 310.

Las funciones del servidor de enrutamiento seguro o del servidor SM-SR 310 y del servidor de preparación de los datos o servidor SM-DP 320, 420 se definen en las normas GSMA 12FAST.13 y GSMA 12FAST-15. El servidor SM-SR 310 se encarga, en particular, de establecer, respectivamente, un canal seguro entre la red de comunicación 30, 40 y el elemento seguro 20 con el fin de cargar, activar, desactivar y eliminar los perfiles en el elemento seguro 20. La función principal del servidor SM-DP 320, 420 es en particular la preparación de los datos de los perfiles, así como la instalación del perfil en el elemento seguro 20.

En formas de realización, con el fin de facilitar la gestión de los perfiles, el elemento seguro 20 comprende un registro de perfil ("Profile Registry” – “Registro de Perfil") que comprende una base de datos que enumera un cierto número de informaciones sobre los perfiles, tal, por ejemplo, su identificador único respectivo.

En el ejemplo de realización ilustrado en la Figura 2, dos perfiles, un primer perfil 210 o perfil A y un segundo perfil 220 o perfil B, están instalados en el elemento seguro 20.

Por ejemplo, el primer perfil 210 está asociado con la primera red de comunicación 30 y el segundo perfil 220 está asociado con la segunda red de comunicación 40.

Por lo tanto, el dispositivo host 10, y en particular el elemento seguro 20, pueden comunicarse, por ejemplo, con las redes de comunicación 30, 40 a través del primer perfil 210 y del segundo perfil 220, respectivamente.

Por supuesto, el número de perfiles instalados en el elemento seguro 20, así como el número de servidores SM-DP vinculados al servidor SM-SR puede ser mayor que dos.

En el ejemplo ilustrado, el primer perfil 210 o perfil A corresponde al perfil actualmente activo. Por lo tanto, el dispositivo host 10 puede comunicarse con la primera red de comunicación 30 a través del primer perfil 210.

En el ejemplo ilustrado, el segundo perfil 220 o perfil B corresponde al perfil que tiene activado el atributo "Fall-back".

Por lo tanto, en caso de iniciación de un mecanismo de réplica ("Mecanismo Fall-back"), el segundo perfil 220 se activa para sustituir el primer perfil 210. En consecuencia, en caso de un problema en el uso del elemento seguro 20 cuando el primer perfil 210 está activo, el segundo perfil 220 se activa a su vez, quedando el primer perfil 210 inactivo. El dispositivo host 10 puede conectarse entonces a la segunda red de comunicación 40 y utilizarse para comunicarse.

Conviene señalar que solamente se puede activar un perfil a la vez en el elemento seguro 20, y que solamente un perfil a la vez puede tener activado el atributo "Fall-back".

La Figura 3 representa, de manera esquemática, una forma de realización de un método de gestión de perfiles en un elemento seguro 20, en donde el elemento seguro 20 comprende el primer perfil 210 o perfil A activo.

El método incluye una etapa de verificación E1 relacionada con la seguridad relativa al primer perfil 210.

En la forma de realización descrita con anterioridad, esta verificación E1 relacionada con la seguridad relativa al primer perfil 210, incluye una verificación de la autorización del acceso de un usuario al primer perfil 210.

Por ejemplo, la verificación de la autorización del acceso para un usuario comprende una etapa de verificación E10 de un número de identificación personal (PIN) asociado con el primer perfil 210.

En una forma de realización, la verificación de un número de identificación personal se pone en práctica un número de veces predeterminado n, por ejemplo, tres.

Cuando se encuentra un problema de seguridad con respecto al primer perfil 210, en particular uno o más fallos sucesivos de verificación del código PIN, se genera un mensaje que contiene información representativa de un error.

De manera opcional, cuando se genera un mensaje que contiene información representativa de un error durante la verificación E10 del número de identificación personal, la verificación de la autorización del acceso de un usuario comprende, además, la verificación E11 de una clave de desbloqueo personal (PUK) asociada con el primer perfil 210.

En cuanto a la verificación del número de identificación personal, la verificación E11 de la clave de desbloqueo personal se pone en práctica un número predeterminado de veces m, por ejemplo, tres.

En otra forma de realización no ilustrada, la verificación de la autorización del acceso de un usuario puede comprender, además de, o en lugar de, las verificaciones del número personal y de la clave de desbloqueo personal, la verificación de datos de autenticación del usuario, por ejemplo, datos biométricos que permitan identificar al usuario.

La verificación de un número de identificación personal, de una clave de desbloqueo personal o datos biométricos, se lleva a cabo mediante la comparación de los datos introducidos utilizando una interfaz en el elemento seguro 20 con datos almacenados en soportes de memorización (no ilustrados) del elemento seguro 20. Estos tipos de verificación son verificaciones comunes por parte de los expertos en esta técnica y no necesitan describirse en este documento.

Cuando al menos una de las verificaciones de autorización del acceso de un usuario al primer perfil 210 resulta en un fallo, un mensaje que contiene información representativa de un error y, por lo tanto, de un fallo de seguridad, se genera a este respecto. El primer perfil 210 se bloquea entonces y se genera una situación de bloqueo.

Cuando se detecta un fallo en la verificación relativa a la seguridad con respecto al primer perfil 210, el método incluye una etapa de bloqueo del primer perfil 210 contenido en el elemento seguro 20.

Después de esta etapa de bloqueo, el elemento seguro 20 ya no puede utilizar la primera red de comunicación 30.

Cuando se genera una situación de bloqueo del primer perfil 210 o perfil A, el método de gestión de perfiles comprende, además, una etapa de desactivación E20 del primer perfil 210 y a continuación una etapa de activación E21 del segundo perfil 220 o perfil B con el "atributo Fall-back". Se pueden poner en práctica los mecanismos clásicos para activar y desactivar perfiles.

Una vez que se desactiva el primer perfil 210 y se activa el segundo perfil 220, el elemento seguro 20 emite, durante una etapa de emisión E30, una orden destinada al dispositivo host 10, esta orden da lugar a un reinicio (reset) del elemento seguro, y de la misma manera, un nuevo procedimiento de conexión E40 de este elemento seguro a una

red de comunicación, utilizando el perfil activo, es decir en el presente caso, una conexión a la segunda red de comunicación 40 a partir del segundo perfil 220.

La orden emitida por el elemento seguro 20 en la etapa de emisión E30 comprende, por ejemplo, una orden REFRESH tal como se describe en la norma GSMA 12FAST.15, en particular en el apartado 3.16 sobre el procedimiento de activación de réplica ("Procedimiento de Activación de Fall-back"), que da lugar al reinicio del elemento seguro 20.

Este inicio activa este procedimiento de conexión E40 a la segunda red 40 de conformidad con los mecanismos convencionales. A continuación, el elemento seguro 20 pone en práctica una etapa de notificación 50 de la desactivación del primer perfil 210 y de la activación del segundo perfil 220 al servidor SM-SR. Durante esta etapa de notificación E50, el elemento seguro 20 inicia un procedimiento de notificación tal como se describe en el apartado 4.1.1.11 de la norma GSMA 12FAST.15.

La notificación de la desactivación del primer perfil 210 y de la activación del segundo perfil 220 al servidor SM-SR se envía, por ejemplo, por SMS. La notificación enviada al servidor SM-SR, por ejemplo, por SMS, contiene una notificación de tipo "etiqueta", es decir, datos codificados para representar un mensaje dado.

De este modo, por ejemplo, de conformidad con la norma GSMA 12FAST.15, la etiqueta ‘04' indica que se ha cambiado un perfil siguiendo un procedimiento de réplica y la etiqueta ‘05' que se ha cambiado un perfil como resultado de un procedimiento de réplica sin demanda previa del servidor SM-SR.

De conformidad con una forma de realización, se agrega un particular no previsto en la norma, por ejemplo, la etiqueta ‘06' (pero cualquier otro valor que no se haya usado ya), se agrega para indicar la desactivación del primer perfil 210 y la activación del segundo perfil 220 después de un fallo detectado durante la etapa de verificación E1 relacionado con el primer perfil o perfil activo para el uso de este perfil activo. Por ejemplo, el fallo es un fallo de seguridad detectado durante una etapa de verificación en relación con la seguridad del primer perfil.

Se observará que la verificación relacionada con el primer perfil es una verificación local, es decir que se pone en práctica en el elemento seguro 20.

Durante este procedimiento de notificación, se informa al servidor de gestión SM-SR 310 que recibe esta notificación de que se ha puesto en práctica un mecanismo de réplica después de la detección de un fallo, y que el perfil que estaba activo (en este caso el primer perfil 210) se ha desactivado y se ha activado otro perfil de "Fall-back" (en este caso, el segundo perfil 220).

El conjunto de las informaciones relativas al elemento seguro (denominado "EIS" en las normas GSMA 12FAST.13 y GSMA 12FAST.15, "EIS" por "eUICC Information Set” – “Conjunto de Información eUICC") que se registra en el servidor SM-SR es entonces actualizado durante una etapa de actualización E60, con el fin de declarar concretamente el segundo perfil 220 como un perfil activo y el primer perfil 210 como un perfil desactivado dentro de las infraestructuras de red de comunicación.

A continuación, durante una primera etapa de notificación E70, el servidor SM-SR notifica al operador de la segunda red de comunicación 40 que el segundo perfil 220 ha sido activado.

Además, durante una segunda etapa de notificación E80, el servidor SM-SR notifica al operador de la primera red de comunicación 30 que el primer perfil 210 ha sido desactivado.

Conviene señalar que las etapas E30 a E80 se basan en las etapas descritas en la norma GSMA 12FAST.15, en particular en el apartado 3.16 sobre el procedimiento de activación de réplica (“Procedimiento de Activación de Fall-back”).

La Figura 4 representa etapas adicionales a las de la Figura 3 del método de gestión de perfiles según una forma de realización de la invención.

Cuando se ha generado una situación de bloqueo del primer perfil 210 (por lo general, que se ha detectado un fallo) y que, en consecuencia, el primer perfil 210 se ha desactivado y el segundo perfil 220 se ha activado con el fin de hacer posible el uso del dispositivo host 10 así como del elemento seguro 20, pudiendo el método de gestión de perfiles incluir etapas relacionadas con la reactivación del primer perfil 210.

Por lo tanto, el método de gestión de perfiles también puede incluir una etapa de reactivación E100 del primer perfil 210, comprendiendo esta etapa de reactivación E100 la desactivación del segundo perfil 220 y a continuación, la activación del primer perfil 210.

La etapa de reactivación del primer perfil 210 se realiza a la recepción E101‘, en el elemento seguro 20, de una demanda de activación del primer perfil 210 enviado por el servidor SM-SR.

En una forma de realización, la demanda de activación proviene de la primera red de comunicación 30 asociada con el primer perfil 210.

En particular, una primera demanda de activación E101 de dicho primer perfil 210 está destinada al servidor SM-SR, que a su vez emite una segunda demanda de activación E101‘ del primer perfil 210 destinada al elemento seguro 20.

En la forma de realización ilustrada en la Figura 4, la demanda de activación E101 del primer perfil 210 se genera a petición de un usuario.

Por ejemplo, el usuario solicita la generación E102 de un nuevo número de identificación personal para el primer perfil 210, bloqueado después de varios fallos por introducir un código PIN o PUK o datos de autenticación.

Para realizar lo que antecede, el usuario se conecta a un servidor WEB asociado con la primera red de comunicación 30.

De conformidad con procedimientos conocidos, el servidor WEB de la red de comunicación 30 verifica, durante una etapa de verificación E103, la identidad del usuario y su autorización para acceder a la primera red de comunicación 30, por ejemplo, mediante la solicitud de introducción de su nombre, dirección, fecha de nacimiento, número de identificación, etc.

Una vez que el servidor WEB ha verificado que la identidad del usuario es correcta y que está autorizado para acceder a la primera red de comunicación 30 a través del primer perfil 210, el servidor WEB genera, durante una etapa de generación, nuevos datos relativos a la autorización del acceso del usuario a la primera red de comunicación 30 a través del primer perfil 210, por ejemplo, un nuevo número de identificación personal (PIN, PUK) asociado con el primer perfil 210.

El nuevo número de identificación personal asociado con el primer perfil 210 se envía E104, E101 al servidor SM-SR, que, a su vez, dicho servidor SM-SR envía el nuevo número de identificación personal al elemento seguro 20 a través de la demanda de activación E101‘. El número de identificación personal se almacena así en el elemento seguro 20 en conexión con el primer perfil 210 para verificaciones posteriores relativas a la autorización del acceso del usuario al primer perfil 210.

Según otra forma de realización que no se muestra en las figuras, la demanda para activar el primer perfil se genera después de la finalización de un período de tiempo predeterminado a partir de la generación de la situación de bloqueo del primer perfil 210.

En particular, la demanda de activación del primer perfil se genera después de la finalización de un período predeterminado a partir de la recepción, por el operador de la primera red, de la notificación E80.

De manera alternativa, el número de identificación personal (PIN/PUK) asociado con el primer perfil 210 se desbloquea de manera automática después de la finalización de un segundo período de tiempo predeterminado a partir de la etapa de notificación E80.

Una vez que el primer perfil 210 ha sido reactivado y el segundo perfil 220 ha sido desactivado, el elemento seguro 20 emite, durante una etapa de transmisión E105, una orden destinada al dispositivo host 10, activando esta orden un procedimiento de conexión E105‘ del primer perfil 210 a la primera red de comunicación 30.

La orden emitida por el elemento seguro 20 en la etapa de transmisión E105 comprende, por ejemplo, una orden REFRESH tal como se describe en la norma GSMA 12FAST.15, en particular en el apartado 3.16 sobre el procedimiento de activación de réplica ("Procedimiento de Activación de Fall-back") que conduce al reinicio del elemento seguro 20.

Esta puesta en marcha desencadena este nuevo procedimiento para unir E105‘ a la primera red 30 de conformidad con mecanismos convencionales. A continuación, el elemento seguro 20 pone en práctica una etapa de notificación E106 de la desactivación del segundo perfil 220 y de la activación del primer perfil 210. Durante esta etapa de notificación E106, el elemento seguro 20 inicia un procedimiento de notificación tal como se describe en el apartado 4.1.1.11 de la norma GSMA 12FAST.15.

La notificación de la desactivación del primer perfil 210 y de la activación del segundo perfil 220 al servidor SM-SR se envía, por ejemplo, por SMS. La notificación enviada al servidor SM-SR, por ejemplo, por SMS, contiene una notificación de tipo "etiqueta", es decir, datos codificados para representar un mensaje dado.

Tal como se describió con anterioridad, la etiqueta ‘06' puede utilizarse para notificar la desactivación del segundo perfil 210 y la activación del primer perfil 220.

Durante este procedimiento de notificación, se informa al servidor de gestión SM-SR que se ha puesto en práctica una reactivación del primer perfil 210.

El conjunto de las informaciones de EIS relativas al elemento seguro y registrado en el servidor SM-SR se actualiza a continuación durante una etapa de actualización E107, con el fin de configurar el primer perfil 210 como el perfil activo y el segundo perfil 210 como el perfil que se ha desactivado.

A continuación, durante una primera etapa de notificación E108, el servidor SM-SR notifica al operador de la primera red de comunicación 30 que el primer perfil 210 ha sido reactivado.

Además, durante una segunda etapa de notificación E109, el servidor SM-SR notifica al operador de la segunda red de comunicación 40 que el segundo perfil 210 ha sido desactivado.

Como resultado de estas etapas de notificación E108, E109, el usuario puede utilizar el dispositivo host 10 a través del primer perfil 210.

Conviene señalar que las etapas E101 a E109 se basan en las etapas descritas en la norma GSMA 12FAST.15, en particular en el apartado 3.16 sobre el procedimiento de activación de réplica (Procedimiento de Activación de Fall-back”).

REIVINDICACIONES

1. Método de gestión de perfiles en un elemento seguro (20), comprendiendo el elemento seguro (20) un primer perfil (210) asociado con una primera red de comunicación (30) y un segundo perfil (220) asociado con una segunda red de comunicación (40), estando activo el primer perfil (210), comprendiendo el método las etapas de:

- desactivación (E20) de dicho primer perfil; y

- activación (E21) de dicho segundo perfil;

estando dicho método caracterizado por cuanto que las etapas de desactivación (E20) y activación (E21) se ponen en práctica después de la detección de un fallo durante una verificación local realizada en dicho elemento seguro y que pertenece a dicho primer perfil (210) para el uso de dicho primer perfil (210).

2. Método de gestión de perfiles conforme a la reivindicación 1, caracterizado porque la verificación local comprende una etapa de verificación (E1) en dicho elemento seguro (20) de la autorización del acceso de un usuario a dicho primer perfil, y se detecta un fallo de seguridad en dicho elemento seguro (20) en caso de fallo de verificación.

3. Método de gestión de perfiles conforme a la reivindicación 2, caracterizado porque la verificación en el elemento seguro (20) de la autorización del acceso de un usuario comprende la verificación (E10) de un número de identificación personal (PIN) asociado a dicho primer perfil.

4. Método de gestión de perfiles conforme a una de las reivindicaciones 2 o 3, caracterizado porque la verificación en el elemento seguro (20) de la autorización del acceso de un usuario comprende la verificación (E11) de una clave de desbloqueo personal (PUK) asociada con dicho primer perfil.

5. Método de gestión de perfiles conforme a una de las reivindicaciones 2 a 4, caracterizado porque la verificación en el elemento seguro (20) de la autorización del acceso del usuario incluye la verificación de datos de autenticación de usuario.

6. Método de gestión de perfiles conforme a una de las reivindicaciones 1 a 5, caracterizado porque la verificación local comprende una etapa de verificación de la integridad de dicho primer perfil (210) para detectar un funcionamiento incorrecto del mismo.

7. Método de gestión de perfiles conforme a la reivindicación 6, caracterizado porque la verificación de la integridad de dicho primer perfil (210) se lleva a cabo durante una fase de activación de dicho primer perfil (210).

8. Método de gestión de perfiles conforme a una de las reivindicaciones 1 a 7, caracterizado porque comprende, además, una etapa de reactivación (E100) de dicho primer perfil, comprendiendo la etapa de reactivación la desactivación de dicho segundo perfil (220) y la activación de dicho primer perfil (210).

9. Método de gestión de perfiles conforme a la reivindicación 8, caracterizado porque la etapa de reactivación (E100) del primer perfil se pone en práctica al recibir (E101'), en dicho elemento seguro, una demanda de activación de dicho primer perfil (210), proviniendo dicha demanda de activación de la primera red de comunicación (30) asociada con dicho primer perfil (210).

10. Método de gestión de perfiles conforme a la reivindicación 9, caracterizado porque dicha demanda de activación de dicho primer perfil (210) se genera a petición de un usuario.

11. Método de gestión de perfiles conforme a la reivindicación 9, caracterizado porque dicha demanda de activación de dicho primer perfil (210) se genera después de la finalización de un período de tiempo predeterminado a partir de una notificación que informa de la desactivación de dicho primer perfil (210) en el elemento seguro (20).

12. Elemento seguro que comprende un primer perfil (210) asociado con una primera red de comunicación (30) y un segundo perfil (220) asociado con una segunda red de comunicación (40), estando dicho primer perfil (210) activo, comprendiendo dicho elemento seguro (20):

- medios de desactivación de dicho primer perfil (210); y

- medios de activación de dicho segundo perfil (220);

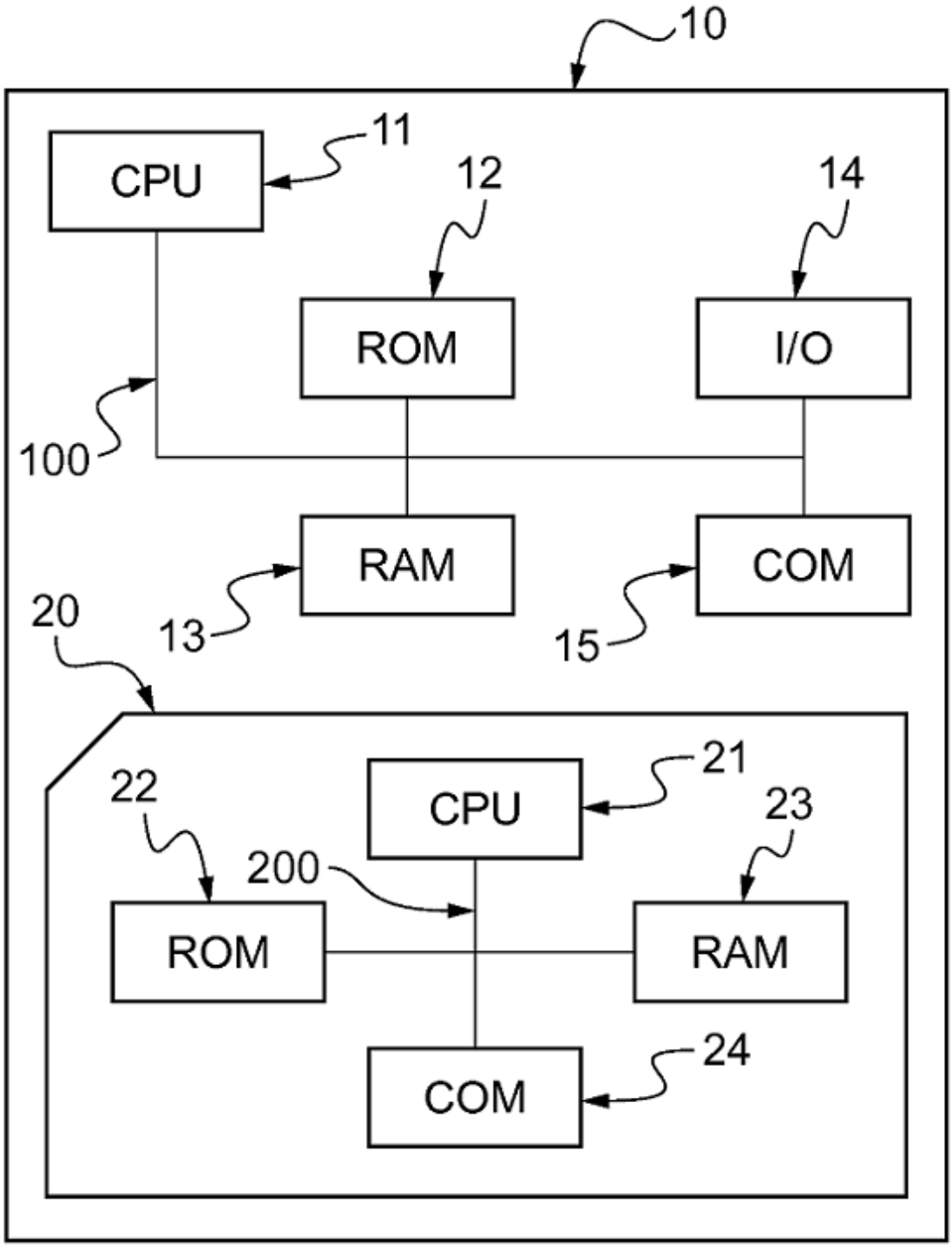
y estando el elemento seguro (20) configurado para que los medios de desactivación y de activación se pongan en práctica después de la detección de un fallo durante una verificación local realizada en dicho elemento seguro y que pertenece a dicho primer perfil (210) para el uso de dicho primer perfil (210).

13. Elemento seguro conforme a la reivindicación 12, caracterizado porque es una tarjeta de tipo UICC integrada (eUICC).

14. Dispositivo host caracterizado porque comprende un elemento seguro de conformidad con una de las reivindicaciones 12 o 13.

15. Dispositivo host conforme a la reivindicación 14, caracterizado porque es un terminal móvil de comunicación.

Fig.1


10
CPU
11
12
14
ROM
I/O
100
RAM
COM
13
15
20
22
CPU
21
23
200
ROM
RAM
COM
24

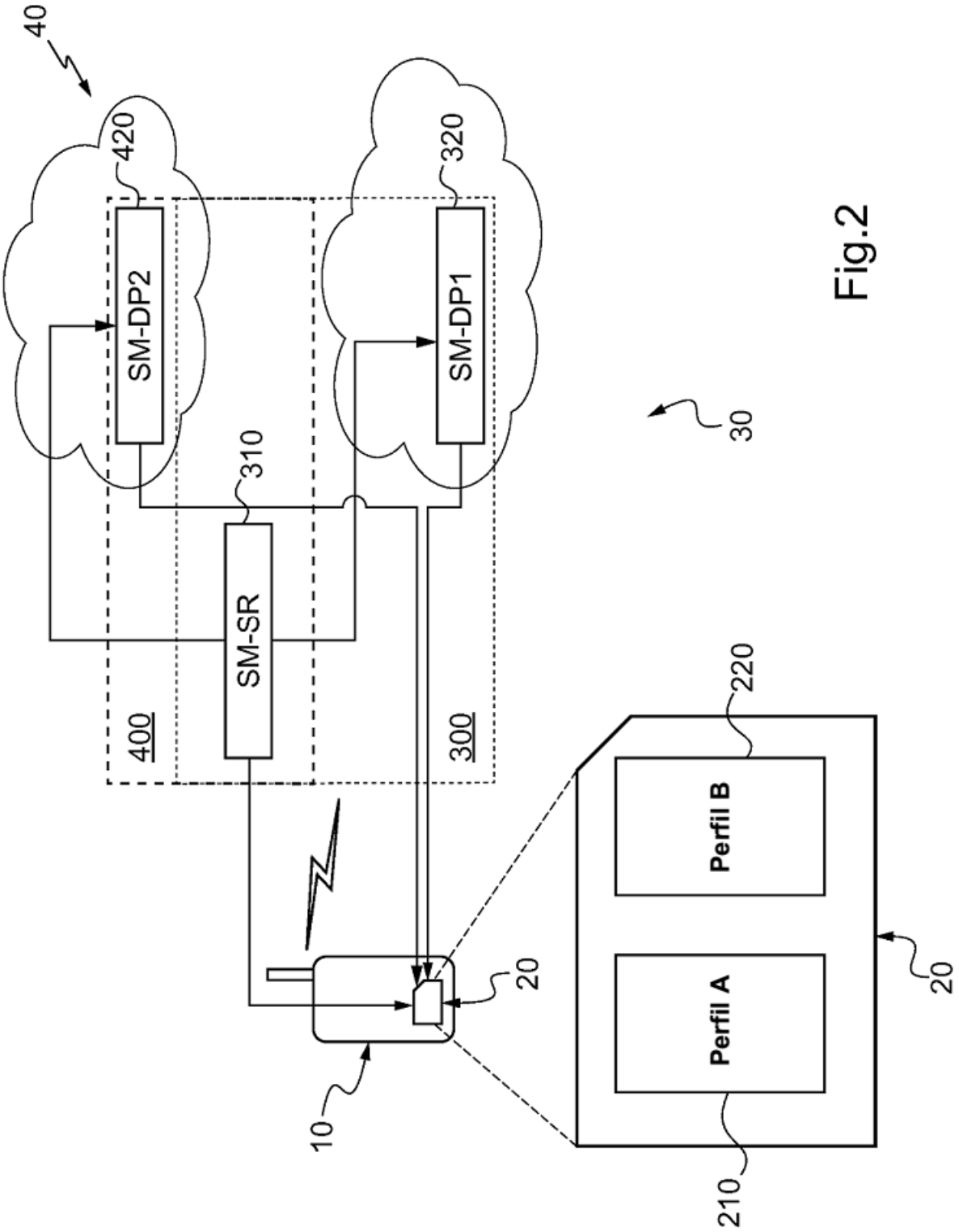

40
420
SM-DP2
320
SM-DP1
310
SM-SR
400
300
30
220
Perfil B
Perfil A
210
20
20
10

Fig.2

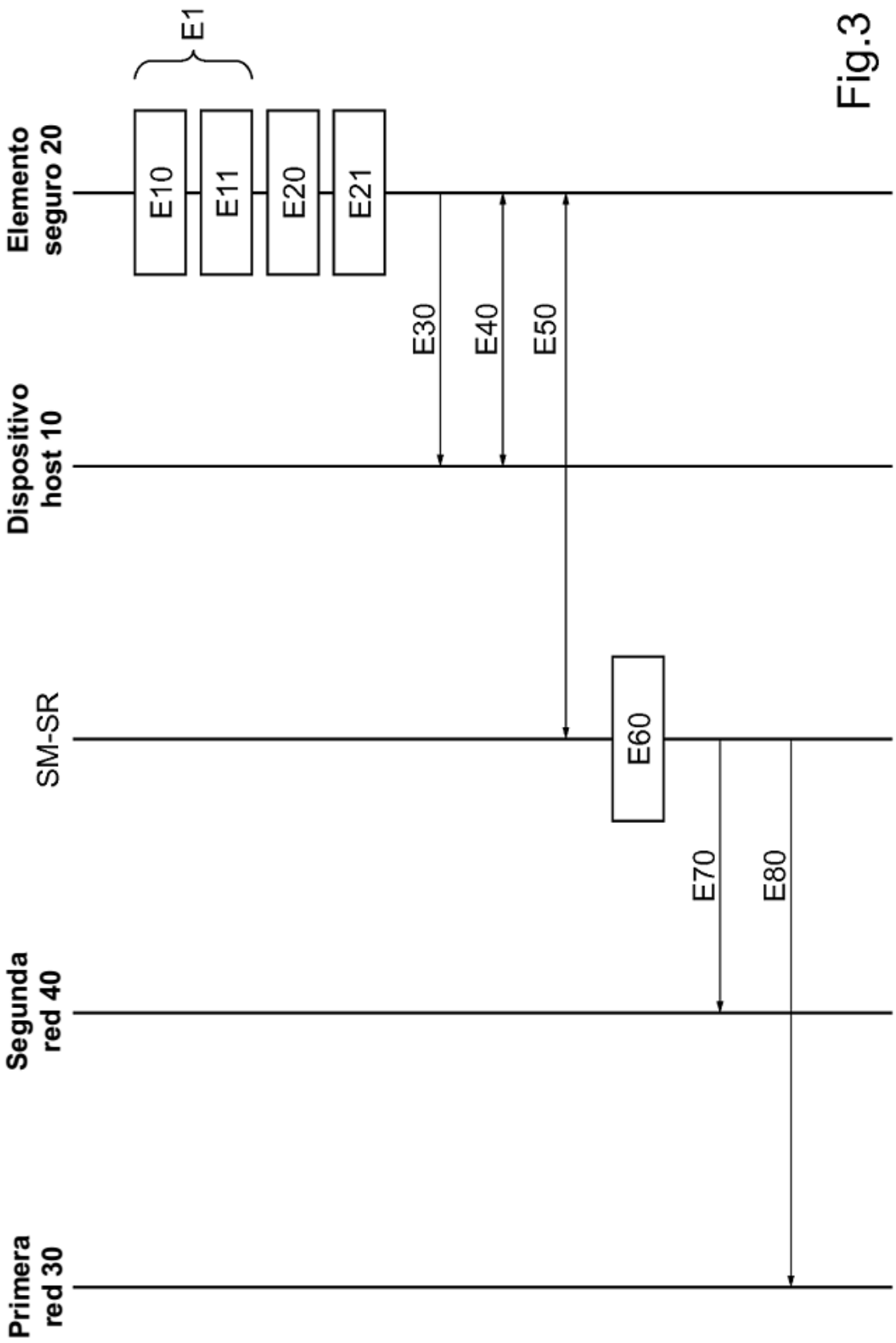

E1
Elemento seguro 20
E10
E11
E20
E21
E30
E40
E50
Dispositivo host 10
SM-SR
E60
E70
E80
Segunda red 40
Primera red 30

Fig.3

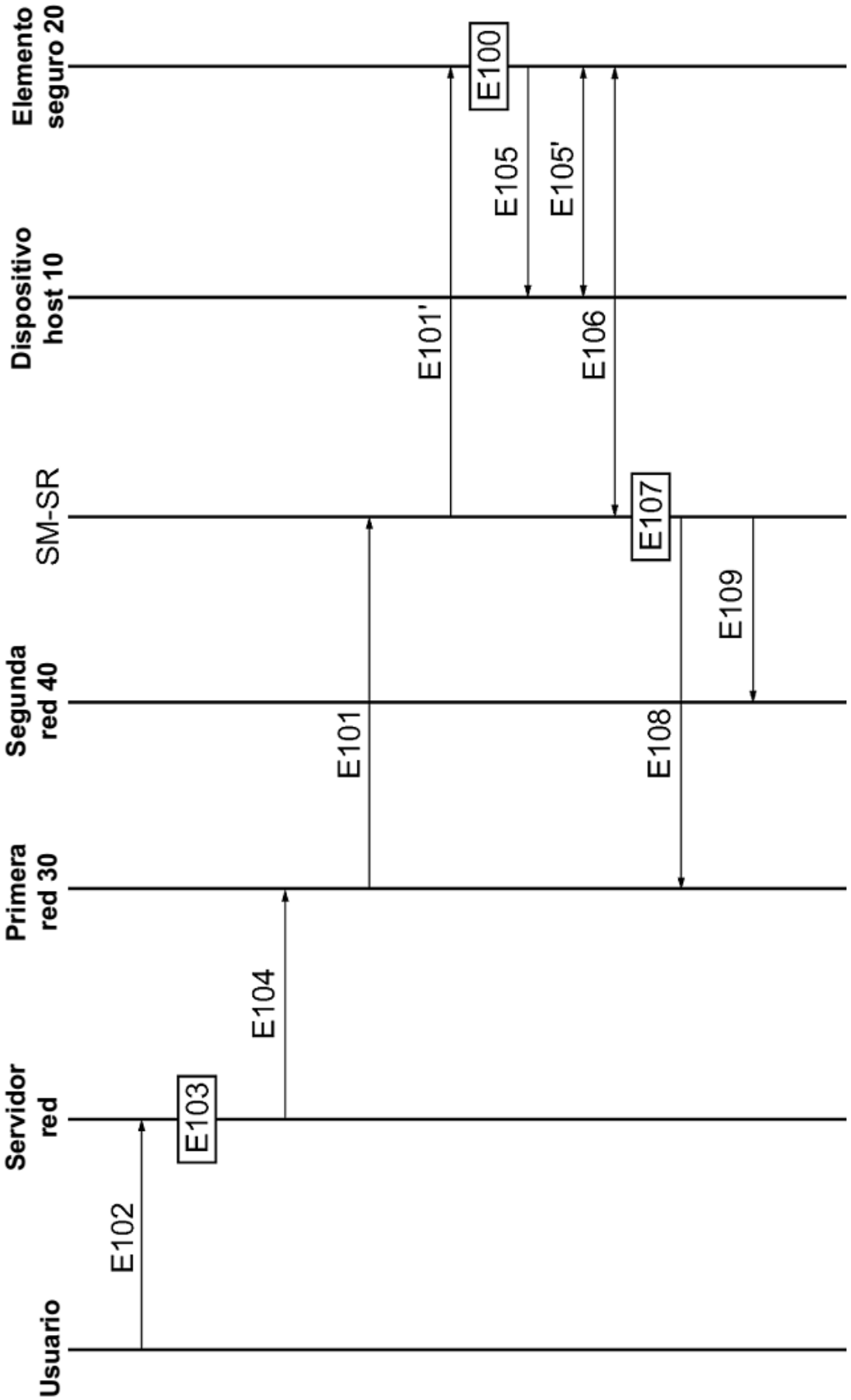

Usuario
Servidor red
Primera red 30
Segunda red 40
SM-SR
Dispositivo host 10
Elemento seguro 20
E102
E103
E104
E101
E101'
E100
E105
E105'
E106
E107
E108
E109

Fig.4