(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 755 387**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04W 4/60 (2008.01)
H04W 8/18 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.01.2015 PCT/EP2015/051382**

(87) Fecha y número de publicación internacional: **27.08.2015 WO15124376**

(96) Fecha de presentación y número de la solicitud europea: **23.01.2015 E 15702199 (9)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 3108674**

(54) Título: **Método para gestionar varios perfiles en un elemento seguro**

(30) Prioridad:

18.02.2014 EP 14305224

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.04.2020

(73) Titular/es:

THALES DIS FRANCE SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

FAURE, FRÉDÉRIC y
BERARD, XAVIER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para gestionar varios perfiles en un elemento seguro

(Campo de la invención)

La presente invención se refiere a métodos para gestionar varios perfiles en un elemento seguro. Se refiere particularmente a métodos para gestionar varios perfiles activos en un elemento seguro.

(Antecedentes de la invención)

Un elemento seguro es bien un componente físico resistente a la manipulación capaz de almacenar datos y prestar servicios de manera segura, bien un componente de *software* que proporciona un área de almacenamiento fiable y servicios fiables. En general, un elemento seguro tiene una cantidad limitada de memoria, un procesador con capacidades limitadas y no tiene batería. Por ejemplo, una UICC (tarjeta de circuito integrado universal) es un elemento seguro que incorpora aplicaciones SIM para fines de telecomunicaciones. Se puede instalar un elemento seguro, de manera fija o no, en un terminal, como por ejemplo un teléfono móvil. En algunos casos, los terminales están constituidos por máquinas que se comunican con otras máquinas para aplicaciones M2M (máquina a máquina).

Un elemento seguro puede tener el formato de una tarjeta inteligente, o puede tener cualquier otro formato, tal como por ejemplo, pero sin limitarse a, un chip empaquetado como se describe en el documento PCT/SE2008/050380, o cualquier otro formato. Una UICC se puede utilizar en terminales móviles en redes GSM, CDMA o UMTS, por ejemplo. La UICC garantiza la autenticación, integridad y seguridad en red de todo tipo de datos personales. La UICC se comunica y coopera con la banda base (también llamada procesador de banda base o procesador de radio de banda base) del equipo terminal.

Ya se conoce el soldar el elemento seguro en un dispositivo anfitrión, para que dependa de este dispositivo anfitrión. Esto se realiza en aplicaciones M2M (máquina a máquina). Se alcanza el mismo objetivo cuando el dispositivo anfitrión contiene un chip (un elemento seguro) que contiene una aplicación de pago, aplicaciones SIM o USIM y archivos. El chip se suelda, por ejemplo, a la placa base del dispositivo anfitrión o la máquina anfitriona y constituye un elemento seguro integrado (eSE, por sus siglas en inglés).

Un elemento seguro puede contener un perfil que puede incluir un conjunto de aplicaciones, un conjunto de datos personales y un conjunto de datos secretos.

El perfil podría estar vinculado a un abono. Puede contener aplicaciones de acceso a la red (NAA, por sus siglas en inglés), aplicaciones de pago o aplicaciones de terceros que proporcionan seguridad para un servicio específico (por ejemplo, aplicaciones NFC).

Un elemento seguro físico puede emular varios elementos seguros virtuales, cada uno representado como un perfil. En tal caso, estos perfiles se denominan perfiles lógicos o perfiles virtuales. Un perfil emulado se llama en adelante perfil virtual. Por lo general, cada perfil virtual es un perfil basado en *software*.

La invención se refiere a una forma de gestionar varios perfiles virtuales que se ejecutan en un único elemento seguro.

En el estado de la técnica, el comportamiento básico para cambiar de un perfil virtual a otro es reinicializar físicamente todo el elemento seguro (por ejemplo: reinicializar según lo definido por el estándar IS07816-3 para una tarjeta inteligente). Después de esta reinicialización de *hardware*, el sistema operativo del elemento seguro habilita el perfil virtual recién seleccionado. Por lo tanto, solo un perfil virtual está activo a la vez en una sesión de dispositivo. Además, en la secuencia de cambio de la técnica anterior, la UICC envía un comando de regeneración proactivo al dispositivo anfitrión para solicitar un reinicio de la banda base del dispositivo anfitrión. El reinicio de la banda base permite tener en cuenta la configuración del perfil virtual recién seleccionado en la banda base y reinicializar la UICC. Luego, la banda base necesita realizar una autenticación con el servidor del operador de red móvil (MNO, por sus siglas en inglés) para conectarse a la red. Estas etapas de la secuencia de cambio tardan mucho tiempo, durante el cual hay una pérdida de conectividad entre la red del MNO y el dispositivo anfitrión.

Los documentos EP2461613 y US2012/0260095 describen cómo cambiar de un perfil virtual de usuario a otro. Sólo un perfil virtual está habilitado, el otro está deshabilitado.

Es necesario reducir el tiempo durante el cual hay una pérdida de conectividad entre la red del MNO y el dispositivo anfitrión.

(Compendio de la invención)

Un objetivo de la invención es resolver el problema técnico mencionado anteriormente.

El objeto de la presente invención es un elemento seguro que comprende una interfaz física de comunicación y un primer y segundo perfiles virtuales. El elemento seguro está configurado para intercambiar datos dirigidos a los perfiles virtuales con un dispositivo anfitrión conectado a través de la interfaz física de comunicación. El dispositivo anfitrión

comprende una primera y una segunda bandas base. El elemento seguro comprende un componente de ejecución configurado para ejecutar simultáneamente el primer y el segundo perfiles virtuales. El primer perfil virtual y la primera banda base forman una primera pareja que está asociada de forma exclusiva con un primer canal lógico de comunicación. El segundo perfil virtual y la segunda banda base forman una segunda pareja que está asociada de forma exclusiva con un segundo canal lógico de comunicación distinto del primer canal lógico de comunicación. El elemento seguro comprende un componente de comunicación configurado para demultiplexar datos entrantes recibidos a través de la interfaz física de comunicación y para multiplexar datos salientes enviados a través de la interfaz física de comunicación. El elemento seguro comprende un agente de administración que está configurado para reinicializar individualmente un perfil virtual objetivo que pertenece a la pareja asignada al canal lógico de comunicación a través del cual el elemento seguro recibe una señal específica. El perfil virtual objetivo se reinicializa sin afectar a los otros perfiles virtuales.

Ventajosamente, el elemento seguro puede comprender un agente de asignación que está configurado para definir una nueva pareja asociando de forma exclusiva uno de dichos perfiles virtuales con una de las bandas base y que está configurado para asignar de forma exclusiva un canal lógico de comunicación a la nueva pareja.

Ventajosamente, el perfil virtual objetivo puede reinicializarse en respuesta a la recepción de la señal específica a través de la interfaz física de comunicación.

Otro objeto de la invención es un sistema que comprende un elemento seguro de acuerdo con la invención y un dispositivo anfitrión que comprende una primera y una segunda bandas base. El sistema comprende un agente de asignación que está configurado para crear una nueva pareja asociando de forma exclusiva uno de dichos perfiles virtuales con una de dichas bandas base y que está configurado para asignar de forma exclusiva un canal lógico de comunicación a la nueva pareja.

Ventajosamente, el sistema puede comprender una pareja preferida que se selecciona automáticamente en caso de reinicialización del elemento seguro y el sistema puede comprender un agente de configuración configurado para determinar y registrar cuál es la pareja preferida.

Ventajosamente, el agente de asignación puede configurarse para asignar de forma exclusiva una pluralidad de canales lógicos de comunicación a dicha pareja, estando uno de dichos canales lógicos de comunicación dedicado a transmitir comandos CAT (herramientas de aplicación de tarjeta) únicamente y siendo el elemento seguro una UICC o una eUICC.

Otro objeto de la invención es un método para gestionar la comunicación entre un elemento seguro y un dispositivo anfitrión. El elemento seguro comprende una interfaz física de comunicación y un primer y un segundo perfiles virtuales. El elemento seguro está configurado para intercambiar datos dirigidos a los perfiles virtuales con el dispositivo anfitrión a través de la interfaz física de comunicación. El método comprende las siguientes etapas:

- ejecutar simultáneamente el primer y el segundo perfiles virtuales en el elemento seguro,

- demultiplexar datos entrantes recibidos a través de la interfaz física de comunicación en el elemento seguro y multiplexar datos salientes enviados por el elemento seguro a través de la interfaz física de comunicación.

- reinicializar uno de los perfiles virtuales individualmente sin afectar a los otros perfiles virtuales en respuesta a la recepción de una señal específica enviada por el dispositivo anfitrión a través de la interfaz física de comunicación.

Ventajosamente, el dispositivo anfitrión puede comprender una primera y una segunda bandas base y el método puede comprender la etapa de definir una nueva pareja asociando de forma exclusiva uno de los perfiles virtuales con una de las bandas base y la etapa de asignar de forma exclusiva un canal lógico de comunicación a la nueva pareja.

Ventajosamente, el método puede comprender la etapa de reinicializar los perfiles virtuales que pertenecen a la pareja asignada al canal lógico de comunicación a través del cual se transmite la señal específica.

(Breve descripción de los dibujos)

Otras características y ventajas de la presente invención surgirán más claramente de una lectura de la siguiente descripción de una serie de realizaciones preferidas de la invención con referencia a los dibujos adjuntos correspondientes en los que:

- La Figura 1 es un ejemplo de un sistema que comprende un dispositivo anfitrión y un elemento seguro de acuerdo con la invención.

(Descripción detallada de las realizaciones preferidas)

La invención puede aplicarse a cualquier tipo de elemento seguro destinado a contener varios perfiles virtuales. El elemento seguro se puede acoplar a cualquier tipo de máquina anfitriona capaz de establecer una sesión de comunicación con el elemento seguro. Por ejemplo, la máquina anfitriona puede ser un teléfono móvil, una tableta, un vehículo, un medidor, una máquina expendedora, un televisor o un ordenador.

La **Figura 1** muestra un sistema SY que comprende un dispositivo anfitrión HO y un elemento seguro SC según la invención.

En este ejemplo, el dispositivo anfitrión HO es un teléfono móvil que tiene una única interfaz DP de comunicación de *hardware* para comunicarse con un elemento seguro. El dispositivo anfitrión HO comprende dos bandas base BB1 y BB2 que están diseñadas para comunicarse con elementos seguros de tipo UICC. El dispositivo anfitrión HO comprende un componente MU2 de comunicación configurado para multiplexar mensajes enviados al elemento seguro SC (y demultiplexar mensajes recibidos del mismo) a través de las interfaces DP de comunicación de *hardware*. Más específicamente, el componente MU2 de comunicación está configurado para permitir que las bandas base BB1 y BB2 se comuniquen simultáneamente con dos perfiles virtuales distintos integrados en el elemento seguro SC.

El elemento seguro SC es una UICC que comprende una interfaz SP de comunicación y un componente MX de ejecución. El componente MX de ejecución comprende los perfiles virtuales PR1 y PR2 y puede ejecutar simultáneamente ambos perfiles virtuales PR1 y PR2.

Cada uno de los dos perfiles se puede seleccionar para ejecutar un comando en cada perfil sin tener que realizar una reinicialización del elemento seguro entre estos comandos.

El elemento seguro SC comprende un componente MU1 de comunicación colocado entre la interfaz SP de comunicación y los perfiles virtuales PR1 y PR2. El componente MU1 de comunicación está configurado para demultiplexar datos entrantes IA recibidos a través de la interfaz SP de comunicación y para reenviar los datos demultiplexados al perfil virtual objetivo. El componente MU1 de comunicación está configurado para multiplexar datos salientes OA proporcionados por los perfiles virtuales y para enviar los datos salientes multiplexados a través de la interfaz SP de comunicación a las bandas base objetivo.

Por ejemplo, los datos entrantes IA pueden ser un comando APDU (unidad de datos de protocolo de aplicación) y los datos salientes OA pueden ser una respuesta APDU según lo especificado por IS07816-4.

En el ejemplo de la Figura 1, el dispositivo anfitrión HO comprende un agente N2 de asignación que está configurado para crear una pareja asociando de forma exclusiva un perfil virtual del elemento seguro con una de las bandas base del dispositivo anfitrión HO. Esta asociación significa que la banda base y el perfil virtual de la pareja están destinados a trabajar juntos. Además, el agente N2 de asignación está configurado para asignar de forma exclusiva un canal lógico de comunicación a dicha pareja. El canal lógico de comunicación puede derivarse del mecanismo de canal lógico ETSI. Por ejemplo, se puede usar un conjunto específico de bits para codificar la referencia del canal lógico de comunicación asignado en el byte CLA del comando APDU.

Ventajosamente, el agente N2 de asignación puede asignar de forma exclusiva varios canales lógicos de comunicación a una pareja. Por lo tanto, el perfil virtual y la banda base de una pareja pueden comunicarse utilizando distintos canales lógicos de comunicación. Esta característica permite configurar un primer canal lógico de comunicación dedicado a la administración de capa baja de telecomunicaciones y un segundo canal lógico de comunicación dedicado a tratamientos aplicativos.

Cabe señalar que los canales lógicos de comunicación pueden implementarse usando el mecanismo de canales lógicos definido por IS07816-4 o usando otro mecanismo de comunicación.

Los componentes MU1 y MU2 de comunicación están configurados para tener en cuenta el canal lógico de comunicación al multiplexar y demultiplexar datos. Ambos componentes MU1 y MU2 de comunicación utilizan los canales lógicos de comunicación para encaminar los datos intercambiados al objetivo pertinente.

En el ejemplo de la Figura 1, el dispositivo anfitrión HO comprende un agente N3 de configuración que está configurado para determinar y registrar cuál es la pareja preferida. La pareja preferida es la pareja que se utiliza (si es posible) cuando se pone en marcha el dispositivo anfitrión HO. En otras palabras, la pareja preferida tiene la más alta prioridad. Por ejemplo, la pareja BB1/PR1 puede ser la pareja preferida que se habilita en un arranque en frío del dispositivo anfitrión HO.

En otro ejemplo, y suponiendo que la pareja actual sea diferente de la pareja preferida, la pareja preferida se puede seleccionar y habilitar automáticamente cuando se pierda la conexión de red (o ésta vaya por debajo de un umbral para la intensidad de la señal recibida) con la pareja actual. Este problema puede ocurrir debido a una falta de cobertura de red o debido a un fallo de la red de telecomunicaciones. En otras palabras, la pareja preferida puede ser una segunda opción de prioridad.

La pareja preferida corresponde al canal de comunicación preferido entre el dispositivo anfitrión HO y el elemento seguro SC.

El agente N3 de configuración está configurado para determinar la pareja preferida según uno o varios criterios. Estos criterios pueden ser el operador de red móvil (MNO) asociado a un perfil virtual, el tipo de abono asociado a un perfil virtual, los costos de comunicación asociados a un perfil virtual, el país actual, una medida de la calidad de la señal

recibida (cobertura de red) o una elección realizada por el usuario final o por el eSE (por ejemplo, durante una operación de cambio iniciada por el eSE).

El elemento seguro SC comprende un agente M1 de administración que está configurado para reinicializar sólo el perfil virtual que pertenezca a la pareja asignada al canal lógico de comunicación a través del cual el elemento seguro SC recibe una señal específica. El agente M1 de administración reinicializa el perfil virtual individualmente sin afectar a los otros perfiles virtuales. En otras palabras, el agente M1 de administración es capaz de reinicializar sólo un perfil virtual de modo que los otros perfiles virtuales permanezcan continuamente habilitados.

Cuando la señal específica es la reinicialización en caliente según lo definido por IS07816-3, el elemento seguro devuelve la ATR (respuesta a reinicialización), aunque no realiza una reinicialización en caliente real, sino que sólo realiza un reinicio del perfil virtual objetivo.

Como alternativa, la señal específica puede ser un comando APDU (unidad de datos de protocolo de aplicación según lo especificado por IS07816-4) preestablecido y el elemento seguro reinicia el perfil virtual objetivo en respuesta a la recepción de este comando APDU preestablecido. Por ejemplo, el comando APDU preestablecido puede ser un comando de respuesta de terminal según lo definido por ETSI TS 102 223. En tal caso, el elemento seguro inicia el reinicio del perfil virtual objetivo cuando recibe el comando APDU preestablecido en respuesta al comando de regeneración proactivo enviado previamente.

En un ejemplo, el elemento seguro está configurado para recibir del dispositivo anfitrión HO un identificador del perfil virtual objetivo que se va a reinicializar. En otro ejemplo, el elemento seguro está configurado para determinar el perfil virtual objetivo que se va a reinicializar.

Preferiblemente, el agente M1 de administración es distinto del componente MU1 de comunicación.

Cabe señalar que este comportamiento es diferente de lo que existía antes de la invención. Anteriormente, el reinicio de una banda base se activaba al recibir un comando de regeneración. Cuando el comando de regeneración está configurado en el modo "Reinicializar UICC" como se especifica en el § 6.4.7 del ETSI TS 102 223 V7.6.0, todo el elemento seguro se reinicializa y se inicia una nueva sesión de elemento seguro. En tal caso, todos los perfiles virtuales habilitados se reinicializan durante la fase de reinicialización del elemento seguro.

Según la invención, se reinicia sólo la pareja (banda base/perfil) asignada al canal lógico de comunicación en el que se ha transmitido previamente el comando de regeneración.

En el ejemplo de la Figura 1, el elemento seguro SC comprende un agente M2 de asignación y un agente M3 de configuración, que son similares al agente N2 de asignación y al agente N3 de configuración descritos anteriormente.

Cabe señalar que estos agentes (M2, N2) de asignación y estos agentes (M3, N3) de configuración son opcionales. Por ejemplo, las parejas pueden ser creadas por otro dispositivo (como un servidor remoto de administración) durante una fase anterior.

En una realización preferida, el sistema SY comprende sólo un agente de asignación y un agente de configuración. El agente de asignación puede colocarse bien en el elemento seguro SC, bien en el dispositivo anfitrión HO. De manera similar, el agente de configuración puede colocarse bien en el elemento seguro SC, bien en el dispositivo anfitrión HO.

Según un primer ejemplo de la invención, el método para iniciar las parejas se puede realizar de la siguiente manera.

Durante una fase inicial de arranque del dispositivo anfitrión, se envía un comando al elemento seguro para obtener la lista de perfiles virtuales existentes. Esta lista puede contener el identificador (AID) de cada perfil virtual existente con sus metadatos asociados. El agente N2 de asignación identifica luego qué perfiles virtuales deben usarse con qué perfiles virtuales. El agente N2 de asignación proporciona a cada banda base el AID de su perfil virtual asociado. Luego, cada banda base selecciona el perfil virtual apropiado de acuerdo con la siguiente secuencia:

a) La banda base abre un canal lógico de comunicación que está determinado por el elemento seguro, el dispositivo anfitrión o preajustado a un valor fijo.

b) La banda base selecciona el perfil virtual apropiado en el canal lógico de comunicación gracias al AID. Esta etapa es opcional si el componente MU1 de comunicación gestiona completamente el encaminamiento al perfil virtual objetivo.

c) La banda base gestiona la secuencia de arranque del perfil virtual asociado con el canal lógico de comunicación enviando la señal específica como se ha descrito anteriormente.

Según un segundo ejemplo de la invención, el método para iniciar las parejas se puede realizar de la siguiente manera.

Durante una fase inicial de arranque del dispositivo anfitrión, se envía un comando al elemento seguro para obtener la lista de los canales lógicos de comunicación asignados. Esta lista puede contener el identificador (ID) de cada canal lógico de comunicación asignado a cada perfil virtual existente. Los metadatos asociados también pueden incluirse en

la lista. El agente N2 de asignación identifica luego qué perfiles virtuales deben usarse con qué perfiles virtuales. El agente N2 de asignación proporciona a cada banda base la ID de su canal lógico de comunicación asociado. Luego, cada banda base selecciona el perfil virtual apropiado de acuerdo con la siguiente secuencia:

a) La banda base abre el canal lógico de comunicación utilizando la ID proporcionada.

b) La banda base gestiona la secuencia de arranque del perfil virtual asociado con el canal lógico de comunicación.

Gracias a la invención, la pareja BB1/PR1 permanece habilitada y activa durante el reinicio de la banda base BB2. Por lo tanto, la pareja BB1/PR1 proporciona continuamente conectividad para la red de telecomunicaciones.

Gracias a la invención, se usa una pareja preferida para la comunicación, mientras que otra es una pareja de respaldo que se puede usar en caso de fallo de conectividad en la pareja preferida.

Según un ejemplo de la invención, el método para actualizar la pareja preferida se puede realizar como sigue. Téngase en cuenta que la expresión "canal de comunicación preferido" puede usarse como equivalente de la pareja preferida.

Este ejemplo supone que la banda base BB1 está asociada con el perfil virtual PR1 y el canal lógico de comunicación 1. Esta pareja BB1/PR1 es la pareja preferida. Este ejemplo también supone que la banda base BB2 está asociada con el perfil virtual PR2 y el canal lógico de comunicación 2. Además, este ejemplo también supone que el elemento seguro comprende un tercer perfil virtual PR3 (no mostrado en la Figura 1).

En una primera etapa, el dispositivo anfitrión solicita un cambio del perfil virtual PR2 al perfil virtual PR3 a través del canal lógico de comunicación 2 para actualizar la pareja BB2/PR2.

En una etapa S2, el elemento seguro habilita el perfil virtual PR3 y deshabilita el perfil virtual PR2 para la banda base BB2.

En una tercera etapa, el elemento seguro envía un comando de regeneración de las herramientas de aplicación de tarjeta (CAT) a la banda base BB2 a través del canal lógico de comunicación 2. En respuesta, en la cuarta etapa, la banda base BB2 se reinicia utilizando la configuración del perfil virtual PR3 recién seleccionado. La banda base BB2 envía la señal específica al elemento seguro como se ha descrito anteriormente. En una quinta etapa, la banda base BB2 se conecta a la red de telecomunicaciones utilizando el perfil virtual PR3.

En una sexta etapa, el elemento seguro envía un PreferredCommChannel con un parámetro igual a "2" que indica que la segunda pareja (banda base BB2/perfil virtual PR3) se convierte en la pareja preferida para la comunicación entre el dispositivo anfitrión y el elemento seguro.

Como alternativa, el cambio de pareja preferida puede ser administrado por el dispositivo anfitrión. Por ejemplo, el dispositivo anfitrión puede realizar una actualización de la pareja preferida tan pronto como detecte que la banda base BB2 está conectada a la red de telecomunicaciones (quinta etapa).

Cabe señalar que varias parejas pueden comunicarse en paralelo mediante un intercambio de datos a través de una interfaz física común. Además, el perfil virtual preferido (por ejemplo, pareja preferida) se puede cambiar varias veces durante una única sesión de elemento seguro. En otras palabras, no hay reinicialización del elemento seguro entre varias reinicializaciones del perfil virtual actual.

Las operaciones por el aire (OTA, por sus siglas en inglés) se pueden realizar en dos perfiles virtuales simultáneamente.

Debe entenderse, dentro del alcance de la invención, que las realizaciones descritas anteriormente se proporcionan como ejemplos no limitativos. En particular, el elemento seguro puede comprender cualquier número de perfiles virtuales.

La arquitectura del dispositivo anfitrión y la arquitectura del elemento seguro que se muestran en la Figura 1 se proporcionan sólo como ejemplos. Estas arquitecturas pueden ser diferentes. Por ejemplo, el agente de asignación y el agente de configuración pueden fusionarse como un agente único.

La invención se aplica a elementos seguros de tipo UICC y de tipo UICC integrada.

Las interfaces de comunicación descritas anteriormente son interfaces físicas que pueden funcionar en modo de contacto o en modo sin contacto.

Una ventaja de la invención es permitir la instalación y el uso de una misma aplicación que tiene un AID (identificador de aplicación) único en varios identificadores de perfiles virtuales.

REIVINDICACIONES

1. Un elemento seguro (SC) que comprende una interfaz física (SP) de comunicación y un primer y un segundo perfiles virtuales (PR1, PR2), estando dicho elemento seguro (SC) configurado para intercambiar datos dirigidos a dichos perfiles virtuales (PR1, PR2) con un dispositivo anfitrión (HO) conectado a través de dicha interfaz física (SP) de comunicación, comprendiendo dicho dispositivo anfitrión (HO) una primera y una segunda bandas base (BB1, BB2),

comprendiendo dicho elemento seguro (SC) un componente (MX) de ejecución configurado para ejecutar **simultáneamente** dichos primer y segundo perfiles virtuales (PR1, PR2), denominándose habilitado un perfil virtual en ejecución, formando dicho primer perfil virtual (PR1) y dicha primera banda base (BB1) una primera pareja que está asociada de forma exclusiva con un primer canal lógico de comunicación, formando dicho segundo perfil virtual (PR2) y dicha segunda banda base (BB2) una segunda pareja que está asociada de forma exclusiva con un segundo canal lógico de comunicación distinto de dicho primer canal lógico de comunicación, **comprendiendo dicho elemento seguro (SC) un componente (MU1) de comunicación configurado para demultiplexar** datos entrantes (IA) recibidos a través de la interfaz física (SP) de comunicación y para multiplexar datos salientes (OA) enviados a través de la interfaz física (SP) de comunicación y comprendiendo dicho elemento seguro (SC) un agente (M1) de administración configurado para reinicializar **individualmente** un perfil virtual objetivo que pertenece a la pareja asignada al canal lógico de comunicación a través del cual el elemento seguro (SC) recibe una señal específica, permaneciendo habilitado continuamente el otro perfil virtual.

2. Un elemento seguro (SC) según la reivindicación 1, comprendiendo dicho elemento seguro (SC) un agente (M2) de asignación que está configurado para definir una nueva pareja asociando de forma exclusiva uno de dichos perfiles virtuales (PR1, PR2) con una de dichas bandas base (BB1, BB2) y que está configurado para asignar de forma exclusiva un canal lógico de comunicación a dicha nueva pareja.

3. Un elemento seguro (SC) según la reivindicación 1, en donde el perfil virtual objetivo se reinicializa en respuesta a la recepción de la señal específica a través de la interfaz física (SP) de comunicación.

4. Un sistema (SY) que comprende un elemento seguro (SC) según la reivindicación 1 y un dispositivo anfitrión (HO), comprendiendo el dispositivo anfitrión (HO) una primera y una segunda bandas base (BB1, BB2) y comprendiendo dicho sistema (SY) un agente (M2, N2) de asignación que está configurado para crear una pareja asociando de forma exclusiva uno de dichos perfiles virtuales (PR1, PR2) con una de dichas bandas base (BB1, BB2) y que está configurado para asignar de forma exclusiva un canal lógico de comunicación a dicha pareja.

5. Un sistema (SY) según la reivindicación 4, comprendiendo el sistema (SY) una pareja preferida que se selecciona automáticamente en caso de reinicialización del elemento seguro (SC) y comprendiendo el sistema (SY) un agente (M3, N3) de configuración configurado para determinar y registrar cuál es la pareja preferida.

6. Un sistema (SY) según la reivindicación 4, en donde el agente (M2, N2) de asignación está configurado para asignar de forma exclusiva una pluralidad de canales lógicos de comunicación a dicha pareja, estando uno de dichos canales lógicos de comunicación dedicado a transmitir comandos CAT únicamente, y en donde el elemento seguro (SC) es una UICC o una eUICC.

7. Un sistema (SY) según la reivindicación 4, en donde el dispositivo anfitrión (HO) puede enviar una solicitud para cambiar de un perfil virtual antiguo a un nuevo perfil virtual en una pareja objetivo, en donde, en respuesta a la recepción de dicha solicitud, el elemento seguro (SC) está configurado para deshabilitar el perfil virtual antiguo y habilitar el nuevo perfil virtual y para enviar un comando de regeneración de herramientas de aplicación de tarjeta a la banda base de la pareja objetivo.

8. Un método para gestionar la comunicación entre un elemento seguro (SC) y un dispositivo anfitrión (HO), comprendiendo dicho elemento seguro (SC) una interfaz física (SP) de comunicación y un primer y un segundo perfiles virtuales (PR1, PR2), estando dicho elemento seguro (SC) configurado para intercambiar datos dirigidos a dichos perfiles virtuales (PR1, PR2) con el dispositivo anfitrión (HO) a través de dicha interfaz física (SP) de comunicación, dicho método comprende las etapas:

- ejecutar **simultáneamente** dichos primer y segundo perfiles virtuales (PR1, PR2) en el elemento seguro (SC), denominándose habilitado un perfil virtual en ejecución,

- **en el elemento seguro** (SC), demultiplexar datos entrantes (IA) recibidos a través de la interfaz física (SP) de comunicación y multiplexar datos salientes (OA) enviados por el elemento seguro (SC) a través de la interfaz física (SP) de comunicación,

- en respuesta a la recepción de una señal específica enviada por el dispositivo anfitrión (HO) a través de la interfaz física (SP) de comunicación, reinicializar uno de dichos perfiles virtuales (PR1, PR2) **individualmente** y mantener continuamente habilitado el otro perfil virtual.

9. Un método según la reivindicación 8, comprendiendo el dispositivo anfitrión (HO) una primera y una segunda bandas base (BB1, BB2) y comprendiendo el método la etapa de definir una pareja asociando de forma exclusiva uno de

dichos perfiles virtuales (PR1, PR2) con una de dichas bandas base (BB1, BB2) y la etapa de asignar de forma exclusiva un canal lógico de comunicación a dicha pareja.

10. Un método según la reivindicación 9, comprendiendo el método la etapa de reinicializar los perfiles virtuales que pertenecen a la pareja asignada al canal lógico de comunicación a través del cual se transmite la señal específica.

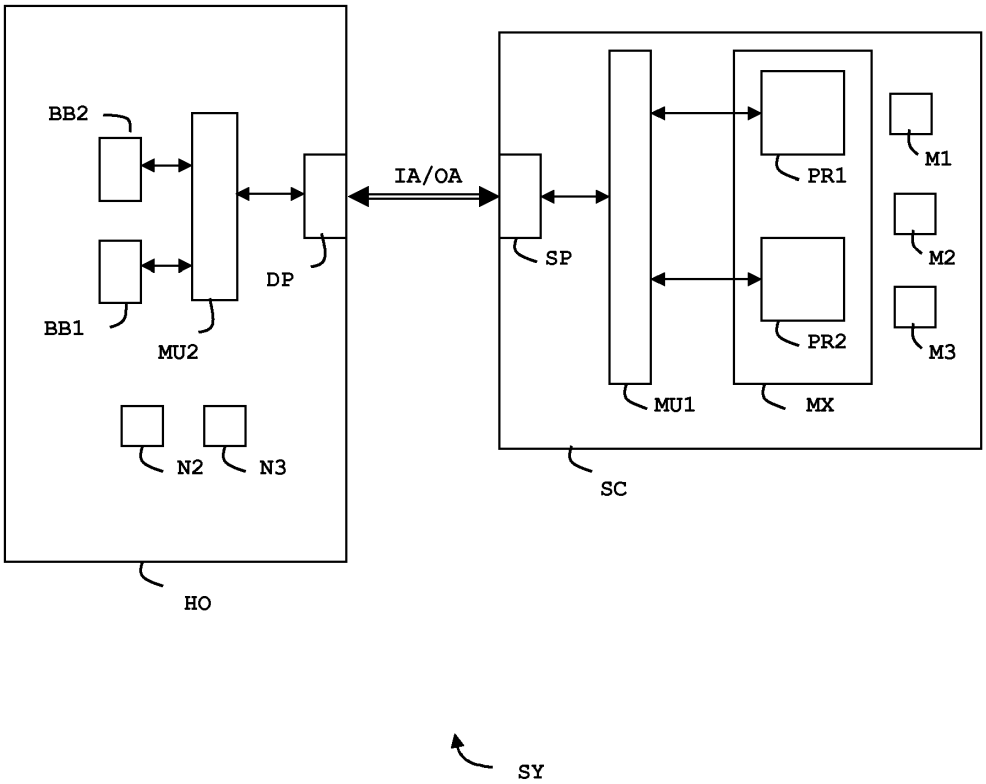

FIG. 1