(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 770 322**

(51) Int. CI.:

G06F 21/62 (2013.01)
G06F 9/455 (2008.01)
G06F 21/53 (2013.01)
G06F 21/77 (2013.01)
G06F 21/78 (2013.01)
H04W 12/00 (2009.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.03.2016 PCT/EP2016/056731**

(87) Fecha y número de publicación internacional: **27.10.2016 WO16169733**

(96) Fecha de presentación y número de la solicitud europea: **25.03.2016 E 16715477 (2)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2019 EP 3286934**

(54) Título: **Sistema y método para gestionar canales lógicos para acceder a varios perfiles virtuales en un elemento seguro**

(30) Prioridad:

22.04.2015 US 201514693010

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.07.2020

(73) Titular/es:

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

(72) Inventor/es:

ROZAK-DRAICCHIO, LIONEL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y método para gestionar canales lógicos para acceder a varios perfiles virtuales en un elemento seguro

(Campo de la invención)

La presente invención se refiere a métodos para gestionar canales lógicos para acceder a varios perfiles incorporados en un elemento seguro. Se refiere en particular a métodos de gestión de varios perfiles activos en un elemento seguro.

(Antecedentes de la invención)

Un elemento seguro es o bien un componente físico resistente a la manipulación que puede almacenar datos y proporcionar servicios de manera segura o 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. Puede instalarse un elemento seguro, de manera fija o no, en un terminal, como un teléfono móvil, por ejemplo. En algunos casos, los terminales están constituidos por máquinas que se comunican con otras máquinas para aplicaciones M2M (de máquina a máquina).

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

Se conoce unir o soldar el elemento seguro en un dispositivo anfitrión, para que dependa de este dispositivo anfitrión. Esto se realiza en aplicaciones M2M (de 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 de la máquina o dispositivo anfitrión y constituye un elemento seguro incorporado (eSE).

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), aplicaciones de pago o aplicaciones de terceros que proporcionan seguridad para un servicio específico (por ejemplo, aplicaciones de 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. A continuación en el presente documento, un perfil emulado se denomina perfil virtual. Por lo general, cada perfil virtual es un perfil basado en software.

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

En el estado de la técnica, el comportamiento básico es gestionar sólo un perfil virtual activo a la vez. Un perfil virtual activo puede usar varios canales lógicos en paralelo. Una operación de intercambio permite deshabilitar el perfil virtual actualmente activo y activar otro. Por tanto, sólo un perfil virtual está activo a la vez en una sesión de dispositivo. Además, según la norma IS07816-4, el canal lógico 0 (cero) desempeña un papel específico: es el que está por defecto que permite recuperar la respuesta a reinicio (ATR) del elemento seguro. El canal lógico 0 se atribuye a la aplicación seleccionada por defecto del perfil virtual. Además, el canal lógico 0 se usa como canal principal para algunos tipos de instrucciones (por ejemplo, instrucciones proactivas tal como se define en la norma ETSI TS 102 223, por ejemplo).

El documento US-2014/342719-A1 describe un sistema para establecer un canal lógico para acceder a cualquiera de los perfiles virtuales (vUICC) incorporados en una eUICC.

Es necesario manejar varios conjuntos de canales lógicos para acceder a igual número de perfiles virtuales activos simultáneamente en un elemento seguro.

(Sumario de la invención)

La invención se define en las reivindicaciones independientes 1, 8, 9 y 10. Un objeto de la invención es resolver el problema técnico mencionado anteriormente.

El objeto de la presente invención es un sistema que comprende un dispositivo anfitrión y un elemento seguro conectado al dispositivo anfitrión, comprendiendo el elemento seguro una pluralidad de perfiles virtuales y un componente de ejecución configurado para ejecutar simultáneamente varios de dicha pluralidad de perfiles virtuales, comprendiendo el sistema un agente de descubrimiento configurado para proporcionar un subconjunto de la pluralidad de perfiles virtuales y datos de configuración para cada perfil virtual de dicho subconjunto. El sistema comprende datos de capacidad que reflejan el máximo de canales lógicos manejados por el dispositivo anfitrión. El sistema comprende un agente de atribución configurado para actuar conjuntamente con el agente de descubrimiento para atribuir un intervalo de canales lógicos a cada perfil virtual del subconjunto basándose en los datos de capacidad y para determinar en cada uno de los intervalos un canal lógico principal que permanece permanentemente disponible cuando se ha inicializado el perfil virtual al que se atribuye el intervalo.

Ventajosamente, el elemento seguro puede almacenar cada perfil virtual de dicha pluralidad de perfiles virtuales en igual número de dominios de seguridad, el agente de descubrimiento puede tener un identificador fijo y el agente de descubrimiento puede almacenarse y gestionarse en el elemento seguro independientemente de los dominios de seguridad.

Ventajosamente, cada perfil virtual puede tener un estado actual que puede o bien habilitarse o bien deshabilitarse, los datos de configuración pueden proporcionar el estado actual de cada perfil virtual y el agente de atribución puede estar configurado para atribuir un intervalo de canales lógicos solamente a los perfiles virtuales que tienen un estado actual habilitado.

Ventajosamente, cada perfil virtual puede tener un estado actual que puede o bien habilitarse o bien deshabilitarse, el subconjunto proporcionado por el agente de descubrimiento puede contener sólo perfiles virtuales que tienen un estado actual habilitado.

Ventajosamente, cada perfil virtual puede tener un estado actual que puede o bien habilitarse o bien deshabilitarse, el sistema puede comprender un registro que contiene el estado actual de todos los perfiles virtuales y dicho registro puede gestionarse por una entidad configurada para actualizar automáticamente el registro cada vez que se habilita, deshabilita, instala o elimina un perfil virtual, siendo dicha entidad o bien el agente de descubrimiento o bien un agente de espionaje almacenado en el sistema.

Ventajosamente, cada perfil virtual puede tener un estado actual que puede o bien habilitarse o bien deshabilitarse y el elemento seguro puede configurarse para iniciar automáticamente una atribución de intervalo de canales lógicos tan pronto como un perfil virtual se habilita, deshabilita o elimina.

Ventajosamente, cada perfil virtual puede comprender una aplicación seleccionada por defecto y el sistema puede configurarse para asignar el canal lógico principal a la aplicación seleccionada por defecto para cada perfil virtual.

Otro objeto de la invención es un método para gestionar canales lógicos en un sistema que comprende un dispositivo anfitrión y un elemento seguro conectado al dispositivo anfitrión. El elemento seguro incluye una pluralidad de perfiles virtuales y un componente de ejecución configurado para ejecutar simultáneamente varios de dicha pluralidad de perfiles virtuales. El sistema incluye datos de capacidad que reflejan el máximo de canales lógicos manejados por el dispositivo anfitrión. El método comprende las siguientes etapas:

- identificar un subconjunto de perfiles virtuales que tienen un estado habilitado,

- atribuir un intervalo de canales lógicos a cada perfil virtual del subconjunto basándose en los datos de capacidad,

- determinar en cada uno de los intervalos atribuidos un canal lógico principal que permanece permanentemente disponible cuando se ha inicializado el perfil virtual al que se atribuye el intervalo.

Otro objeto de la invención es un elemento seguro que puede conectarse a un dispositivo anfitrión. El elemento seguro incluye una pluralidad de perfiles virtuales y un componente de ejecución configurado para ejecutar simultáneamente varios de dicha pluralidad de perfiles virtuales. El elemento seguro incluye un agente de descubrimiento configurado para proporcionar un subconjunto de la pluralidad de perfiles virtuales y datos de configuración para cada perfil virtual de dicho subconjunto, incluyendo los datos de configuración varios canales lógicos requeridos para ejecutar cada perfil virtual. El elemento seguro incluye un distribuidor de instrucciones configurado para recibir del dispositivo anfitrión un intervalo de canales lógicos atribuidos a cada perfil virtual del subconjunto y para determinar en cada uno de los intervalos un canal lógico principal que permanece permanentemente disponible cuando se ha inicializado el perfil virtual al que se atribuye el intervalo.

Otro objeto de la invención es un dispositivo anfitrión conectado a un elemento seguro que comprende una pluralidad de perfiles virtuales y un componente de ejecución configurado para ejecutar simultáneamente varios de dicha pluralidad de perfiles virtuales. El dispositivo anfitrión está configurado para enviar una solicitud al elemento seguro para recuperar un subconjunto de la pluralidad de perfiles virtuales y datos de configuración para cada perfil virtual de dicho subconjunto. El dispositivo anfitrión incluye datos de capacidad que reflejan el máximo de canales lógicos manejados por el dispositivo anfitrión. El dispositivo anfitrión incluye un agente de atribución configurado para actuar conjuntamente con el agente de descubrimiento para atribuir un intervalo de canales lógicos a cada perfil

virtual del subconjunto basándose en los datos de capacidad y para determinar en cada uno de los intervalos un canal lógico principal que permanece permanentemente disponible cuando se ha inicializado el perfil virtual al que se atribuye el intervalo.

(Breve descripción de los dibujos)

Otras características y ventajas de la presente invención surgirán más claramente de una lectura de la siguiente descripción de varias 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 según la invención,

- la Figura 2 es un ejemplo de un conjunto de perfil virtual y datos de configuración asociados según la invención,

- la Figura 3 es un ejemplo de intervalos de canales lógicos atribuidos a los perfiles virtuales comprendidos en un elemento seguro según la invención, y

- la Figura 4 es un ejemplo de canales lógicos atribuidos a la aplicación seleccionada por defecto de los perfiles virtuales comprendidos en un elemento seguro según la invención.

(Descripción detallada de las realizaciones preferidas)

La invención puede aplicarse a cualquier tipo de elemento seguro destinado a contener varios perfiles virtuales y que puede comunicarse a través de una pluralidad de canales lógicos. En particular, la invención se aplica a elementos seguros de tipo UICC y tipo UICC incorporada (e-UICC).

El elemento seguro puede acoplarse a cualquier tipo de máquina anfitriona que pueda 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 tragaperras, 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 de comunicación de hardware M2 para comunicarse con un elemento seguro. El dispositivo anfitrión HO comprende varias bandas base (no dibujadas) que están diseñadas para comunicarse con elementos seguros de tipo UICC. El dispositivo anfitrión HO comprende un componente de comunicación (no dibujado) configurado para multiplexar mensajes enviados a (y para demultiplexar mensajes recibidos desde) el elemento seguro SC a través de las interfaces de comunicación de hardware M2. Más específicamente, el componente de comunicación está configurado para permitir que las bandas base se comuniquen simultáneamente con igual número de perfiles virtuales distintos incorporados en el elemento seguro SC. El dispositivo anfitrión HO está configurado para asignar únicamente una banda base a cada perfil virtual que tenga un estado “habilitado”. Gracias a la atribución tanto de una banda base como de un intervalo de canales lógicos a cada perfil virtual “habilitado”, el dispositivo anfitrión HO puede reinicializar (reiniciar) cada perfil virtual independientemente de los demás.

El elemento seguro SC es una UICC que comprende una interfaz de comunicación M1, un sistema operativo OS y cuatro dominios de seguridad SDR, SD1, SD2 y SD3 (tal como se define en las especificaciones de la tarjeta de plataforma global v2.x). El dominio de seguridad SD1 comprende un perfil virtual P1, el dominio de seguridad SD2 comprende un perfil virtual P2 y el dominio de seguridad SD3 comprende un perfil virtual P3. El elemento seguro SC comprende un componente de ejecución (no dibujado) que está configurado para ejecutar simultáneamente varios perfiles virtuales.

El perfil virtual P1 comprende tres aplicaciones A11, A12 y A13. La aplicación A13 es la aplicación seleccionada por defecto (aplicación seleccionada de manera predeterminada) en el perfil virtual P1. Por ejemplo, la aplicación A13 es una aplicación de telecomunicaciones (UICC), la aplicación A11 es una aplicación de pago y la aplicación A12 es una aplicación de transporte.

De manera similar, el perfil virtual P2 comprende dos aplicaciones A21 y A22, donde A21 es una que se selecciona por defecto y el perfil virtual P3 comprende dos aplicaciones A31 y A32, donde A32 es una que se selecciona por defecto.

Los perfiles virtuales P1 y P3 están habilitados mientras que el perfil virtual P2 está deshabilitado. En otras palabras, los perfiles virtuales P1 y P3 están activos.

El dominio de seguridad SDR actúa como un dominio de seguridad raíz. Los otros dominios de seguridad (SD1-SD3) dependen del dominio de seguridad SDR. El dominio de seguridad SDR comprende un agente de descubrimiento EDA que está configurado para proporcionar un subconjunto de los perfiles virtuales incorporados en el elemento seguro SC y los datos de configuración correspondientes a cada perfil virtual del subconjunto. El dominio de

seguridad SDR no comprende ningún perfil virtual. Dado que el agente de descubrimiento EDA pertenece al dominio de seguridad SDR, el agente de descubrimiento EDA se almacena y se gestiona independientemente de los perfiles virtuales (es decir, independientemente de los otros dominios de seguridad) incorporados en el elemento seguro SC.

Los datos de configuración incluyen al menos el número de canales lógicos requeridos para ejecutar cada perfil virtual que pertenece al subconjunto.

Ventajosamente, el agente de descubrimiento EDA puede tener un identificador fijo (común a un lote de elementos seguros) para que el dispositivo anfitrión pueda configurarse para acceder fácilmente al agente de descubrimiento EDA.

El sistema operativo OS comprende un distribuidor de instrucciones AD que se encarga de reenviar las instrucciones recibidas a través de la interfaz de comunicación M1 al perfil o aplicación virtual relevante según el canal lógico utilizado.

El dispositivo anfitrión HO comprende un dato de capacidad CA que refleja el máximo de canales lógicos manejados por el dispositivo anfitrión HO. Por ejemplo, los datos de capacidad CA pueden indicar que el dispositivo anfitrión HO puede gestionar hasta 20 canales lógicos.

El dispositivo anfitrión HO comprende un agente de atribución AG que está configurado para atribuir un intervalo de canales lógicos solamente a los perfiles virtuales que tienen un estado actual “habilitado”. El agente de atribución AG usa los datos de capacidad CA cuando atribuye los intervalos de canales lógicos. El agente de atribución AG está adaptado para dotar al distribuidor de instrucciones AD de los intervalos atribuidos. En un ejemplo, el agente de atribución AG envía directamente los intervalos atribuidos al distribuidor de instrucciones AD. En otro ejemplo, el agente de atribución AG envía los intervalos atribuidos al agente de descubrimiento EDA, que a su vez envía los intervalos atribuidos al distribuidor de instrucciones AD.

En una realización, el canal principal (también denominado canal básico) del perfil virtual se define como el canal lógico que tiene el número más bajo entre el intervalo de canales lógicos atribuidos al perfil virtual.

En otra realización, el canal principal se selecciona por el agente de atribución AG o por el agente de descubrimiento EDA o bien al azar o bien según un criterio preestablecido (por ejemplo, un número fijo requerido por una aplicación).

El canal principal permanece permanentemente disponible para comunicarse con un perfil virtual que se ha inicializado. El canal principal se abre automáticamente cuando se inicializa el perfil virtual. Los otros canales lógicos (es decir, diferentes del canal principal) pueden abrirse y cerrarse en cualquier momento según sea necesario.

Preferiblemente, el canal principal se asigna a la aplicación seleccionada por defecto en el perfil virtual.

En el ejemplo de la Figura 1, el dominio de seguridad SDR comprende un registro RG que contiene el estado actual de todos los perfiles virtuales incorporados en el elemento seguro SC. Ventajosamente, el registro RG también puede contener el número de canales lógicos requeridos para cada perfil virtual.

En el ejemplo de la Figura 1, el sistema operativo OS comprende un agente de espionaje SP configurado para actualizar automáticamente el registro RG cada vez que se instala, elimina, habilita o deshabilita un perfil virtual. Alternativamente, el agente de descubrimiento EDA puede actuar como el agente de espionaje SP y actualizar automáticamente el registro RG.

Ventajosamente, el agente de espionaje SP (o el agente de descubrimiento EDA) puede configurarse para iniciar automáticamente una nueva atribución de intervalos de canales lógicos tan pronto como un perfil virtual se habilita, deshabilita o elimina del elemento seguro SC.

En otro ejemplo, el agente de descubrimiento EDA y el agente de atribución AG pueden implementarse ambos en el mismo lado: o bien en el dispositivo anfitrión HO o bien en el elemento seguro SC.

Según un ejemplo de la invención, el método para atribuir canales lógicos a los perfiles virtuales puede realizarse como sigue.

Durante una primera etapa, el dispositivo anfitrión HO reinicia el elemento seguro SC que envía su respuesta a reinicio (ATR según la norma IS07816-3) a través del canal lógico 0.

Luego, en una segunda etapa, el dispositivo anfitrión HO requiere que el agente de descubrimiento EDA transmita una lista de perfiles virtuales y los datos de configuración asociados a cada perfil virtual.

Preferiblemente, la lista comprende todos los perfiles virtuales incorporados en el elemento seguro SC. La lista comprende un identificador (AID del dominio de seguridad que comprende el perfil virtual, por ejemplo) correspondiente a cada perfil virtual. En este caso, los datos de configuración comprenden el estado de cada perfil virtual y el número de canales lógicos requeridos para cada perfil virtual.

La Figura 2 muestra un ejemplo de la lista y los datos de configuración asociados que envía el agente de descubrimiento EDA.

El dominio de seguridad del perfil virtual P1 tiene un identificador igual a AID1, un estado establecido en “habilitado” y necesita tres canales lógicos para ejecutarse.

De manera similar, el dominio de seguridad del perfil virtual P2 tiene un identificador igual a AID2, un estado establecido en “deshabilitado” y necesita dos canales lógicos para ejecutarse y el dominio de seguridad del perfil virtual P3 tiene un identificador igual a AID3, un estado establecido en “habilitado” y necesita dos canales lógicos para ejecutarse.

Alternativamente, la lista puede comprender sólo los perfiles virtuales que tienen un estado establecido en “habilitado”. En este caso, los datos enviados comprenden sólo el identificador del dominio de seguridad que comprende cada perfil virtual y el canal lógico requerido asociado.

En ambos casos, el sistema identifica el subconjunto de perfiles virtuales que tienen un estado “habilitado”.

Cabe señalar que este subconjunto puede comprender sólo una parte de los perfiles virtuales incorporados en el elemento seguro SC, puede comprender todos los perfiles virtuales incorporados en el elemento seguro SC o incluso puede estar vacío.

En una tercera etapa, el dispositivo anfitrión HO atribuye un intervalo de canales lógicos a cada perfil virtual que pertenece al subconjunto. La operación de atribución se lleva a cabo utilizando los datos de capacidad CA. Si el número máximo de canales lógicos manejados por el dispositivo anfitrión HO es demasiado bajo, puede realizarse una atribución temporal de canales lógicos. En otro ejemplo, un agente de supervisión puede analizar el comportamiento de los perfiles virtuales para rastrear el número real de canales lógicos utilizados por cada perfil virtual. Por tanto, el agente de supervisión puede detectar que un perfil virtual específico usa menos que el número de canales lógicos previamente requeridos. Por ejemplo, el agente de supervisión puede detectar que un perfil virtual sólo usa 2 canales lógicos entre los 3 canales lógicos inicialmente requeridos. En este caso, sólo se atribuirán dos canales lógicos a este perfil virtual. En otro ejemplo, el dispositivo anfitrión HO puede pedirle al usuario que deshabilite un servicio para que disminuya la necesidad general.

En una cuarta etapa, se determina un canal principal en cada intervalo atribuido.

En una quinta etapa, los intervalos atribuidos se envían al EDA.

La Figura 3 muestra un ejemplo de atribución de intervalo de canal(es) lógico(s) a los perfiles virtuales “habilitados”. Los canales lógicos 0, 1 y 2 se atribuyen al perfil virtual P1 y los canales lógicos 3 y 4 se atribuyen al perfil virtual P3. No se atribuye ningún canal lógico al perfil virtual P2 ya que está en un estado “deshabilitado”.

En una sexta etapa, el agente de descubrimiento EDA proporciona el distribuidor de instrucciones AD con los intervalos atribuidos. El canal principal está vinculado a la aplicación seleccionada por defecto en cada perfil virtual.

La Figura 4 muestra el canal lógico principal asignado a la aplicación seleccionada por defecto de cada perfil virtual “habilitado”. En el perfil virtual P1, el canal lógico 0 se ha asignado a la aplicación A13 y en el perfil virtual P3, el canal lógico 3 se ha asignado a la aplicación A32.

En una séptima etapa, el dispositivo anfitrión HO inicializa cada perfil virtual que tiene un estado “habilitado” utilizando el canal principal de cada perfil virtual.

Cuando el estado de un perfil virtual ha cambiado, el agente de descubrimiento EDA (o el agente de espionaje SP) puede configurarse para informar al agente de atribución AG para iniciar un nuevo proceso de atribución de canal lógico. Ventajosamente, esta solicitud de nueva atribución puede enviarse utilizando el canal lógico principal de cualquier perfil virtual “habilitado”. Si no hay un perfil virtual “habilitado”, la solicitud puede enviarse a través del canal lógico 0.

Los canales lógicos utilizados en las Figuras 1-4 cumplen con la norma IS07816-4 y se proporcionan sólo como ejemplos. El mecanismo del canal lógico puede ser diferente, siempre que los canales lógicos permitan el intercambio de datos a través de una única interfaz de comunicación física.

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. El dispositivo anfitrión no es necesario un equipo de telecomunicaciones. El perfil virtual puede ser un abono para cualquier tipo de servicios: pago, acceso al servicio, transporte, fidelidad o identidad, por ejemplo.

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 atribución AG y el agente de descubrimiento EDA pueden fusionarse como un agente único.

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

REIVINDICACIONES

1. Sistema (SY) que comprende un dispositivo anfitrión (HO) y un elemento seguro (SC) conectado al dispositivo anfitrión, comprendiendo el elemento seguro una pluralidad de perfiles virtuales (P1, P2, P3), caracterizado por que el sistema comprende un componente de comunicación configurado para habilitar comunicaciones simultáneas con varios de dicha pluralidad de perfiles virtuales, por que el sistema comprende un agente de descubrimiento (EDA) configurado para proporcionar un subconjunto de la pluralidad de perfiles virtuales que tienen un estado habilitado y datos de configuración para cada perfil virtual de dicho subconjunto, por que el sistema comprende datos de capacidad (CA) que reflejan el número máximo de canales lógicos que puede manejar el dispositivo anfitrión, por que el sistema comprende un agente de atribución (AG) configurado para actuar conjuntamente con el agente de descubrimiento para atribuir un intervalo de canales lógicos a cada perfil virtual que tiene un estado habilitado basándose en los datos de capacidad y para asignar en cada uno de los intervalos atribuidos un canal lógico principal que permanece permanentemente disponible cuando se ha inicializado el perfil virtual al que se atribuye el intervalo.

2. Sistema según la reivindicación 1, en el que el elemento seguro almacena cada perfil virtual de dicha pluralidad de perfiles virtuales en igual número de dominios de seguridad, en el que el agente de descubrimiento tiene un identificador fijo y se almacena y se gestiona en el elemento seguro independientemente de dichos dominios de seguridad.

3. Sistema según la reivindicación 1, en el que cada perfil virtual tiene un estado actual que puede o bien habilitarse o bien deshabilitarse, en el que los datos de configuración proporcionan el estado actual de cada perfil virtual y en el que el agente de atribución está configurado para atribuir un intervalo de canales lógicos solamente a los perfiles virtuales que tienen un estado actual habilitado.

4. Sistema según la reivindicación 1, en el que cada perfil virtual tiene un estado actual que puede o bien habilitarse o bien deshabilitarse, en el que el subconjunto proporcionado por el agente de descubrimiento contiene sólo perfiles virtuales que tienen un estado actual habilitado.

5. Sistema según la reivindicación 1, en el que cada perfil virtual tiene un estado actual que puede o bien habilitarse o bien deshabilitarse, en el que el sistema comprende un registro que contiene el estado actual de todos los perfiles virtuales y en el que dicho registro se gestiona por una entidad configurada para actualizar automáticamente el registro cada vez que se habilita, deshabilita, instala o elimina un perfil virtual, siendo dicha entidad o bien el agente de descubrimiento o bien un agente de espionaje almacenado en el sistema.

6. Sistema según la reivindicación 1, en el que cada perfil virtual tiene un estado actual que puede o bien habilitarse o bien deshabilitarse y en el que el elemento seguro está configurado para iniciar automáticamente una atribución de intervalo de canales lógicos tan pronto como un perfil virtual se habilita, deshabilita o elimina.

7. Sistema según la reivindicación 1, en el que cada perfil virtual comprende una aplicación seleccionada por defecto y en el que el sistema está configurado para asignar el canal lógico principal a la aplicación seleccionada por defecto para cada perfil virtual.

8. Método para gestionar canales lógicos en un sistema (SY) que comprende un dispositivo anfitrión (HO) y un elemento seguro (SC) conectado al dispositivo anfitrión, comprendiendo el elemento seguro una pluralidad de perfiles virtuales, caracterizado por habilitar mediante un componente de comunicación comunicaciones simultáneas con varios de dicha pluralidad de perfiles virtuales, reflejando mediante un dato de capacidad (CA) el número máximo de canales lógicos que puede manejar el dispositivo anfitrión, y por que el método comprende las etapas:

- identificar por un agente de descubrimiento (EDA) un subconjunto de perfiles virtuales que tienen un estado habilitado,

- atribuir por un agente de atribución (AG) actuando conjuntamente con el agente de descubrimiento un intervalo de canales lógicos a cada perfil virtual del subconjunto que tiene un estado habilitado basándose en los datos de capacidad,

- asignar en cada uno de los intervalos atribuidos un canal lógico principal que permanece permanentemente disponible cuando se ha inicializado el perfil virtual al que se atribuye el intervalo.

9. Elemento seguro (SC) que puede conectarse a un dispositivo anfitrión (HO), comprendiendo el elemento seguro una pluralidad de perfiles virtuales (P1, P2, P3), caracterizado por que el elemento seguro comprende un componente de ejecución configurado para habilitar comunicaciones simultáneas con varios de dicha pluralidad de perfiles virtuales, por que el elemento seguro comprende un agente de descubrimiento (EDA) configurado para proporcionar al dispositivo anfitrión un subconjunto de la pluralidad de perfiles virtuales que tienen un estado habilitado y datos de configuración para cada perfil virtual de dicho subconjunto, incluyendo los datos de configuración varios canales lógicos requeridos para ejecutar cada perfil virtual, por que el elemento seguro comprende un distribuidor de instrucciones (AD) configurado para recibir del dispositivo anfitrión un intervalo de canales lógicos atribuidos a cada perfil virtual del subconjunto que tiene un estado habilitado y para determinar en

cada uno de los intervalos un canal lógico principal que permanece permanentemente disponible cuando se ha inicializado el perfil virtual al que se atribuye el intervalo.

10. Dispositivo anfitrión (HO) conectado a un elemento seguro (SC) que comprende una pluralidad de perfiles virtuales y un componente de ejecución configurado para habilitar comunicaciones simultáneas con varios de dicha pluralidad de perfiles virtuales, caracterizado por que el dispositivo anfitrión está configurado para enviar una solicitud al elemento seguro para recuperar un subconjunto de la pluralidad de perfiles virtuales que tienen un estado habilitado y datos de configuración para cada perfil virtual de dicho subconjunto, por que el dispositivo anfitrión comprende datos de capacidad (CA) que reflejan el número máximo de canales lógicos que puede manejar el dispositivo anfitrión, por que el dispositivo anfitrión comprende un agente de atribución (AG) configurado para atribuir un intervalo de canales lógicos a cada perfil virtual que tiene un estado habilitado basándose en los datos de capacidad y para asignar en cada uno de los intervalos un canal lógico principal que permanece permanentemente disponible cuando se ha inicializado el perfil virtual al que se atribuye el intervalo, proporcionándose entonces los intervalos atribuidos al elemento seguro.

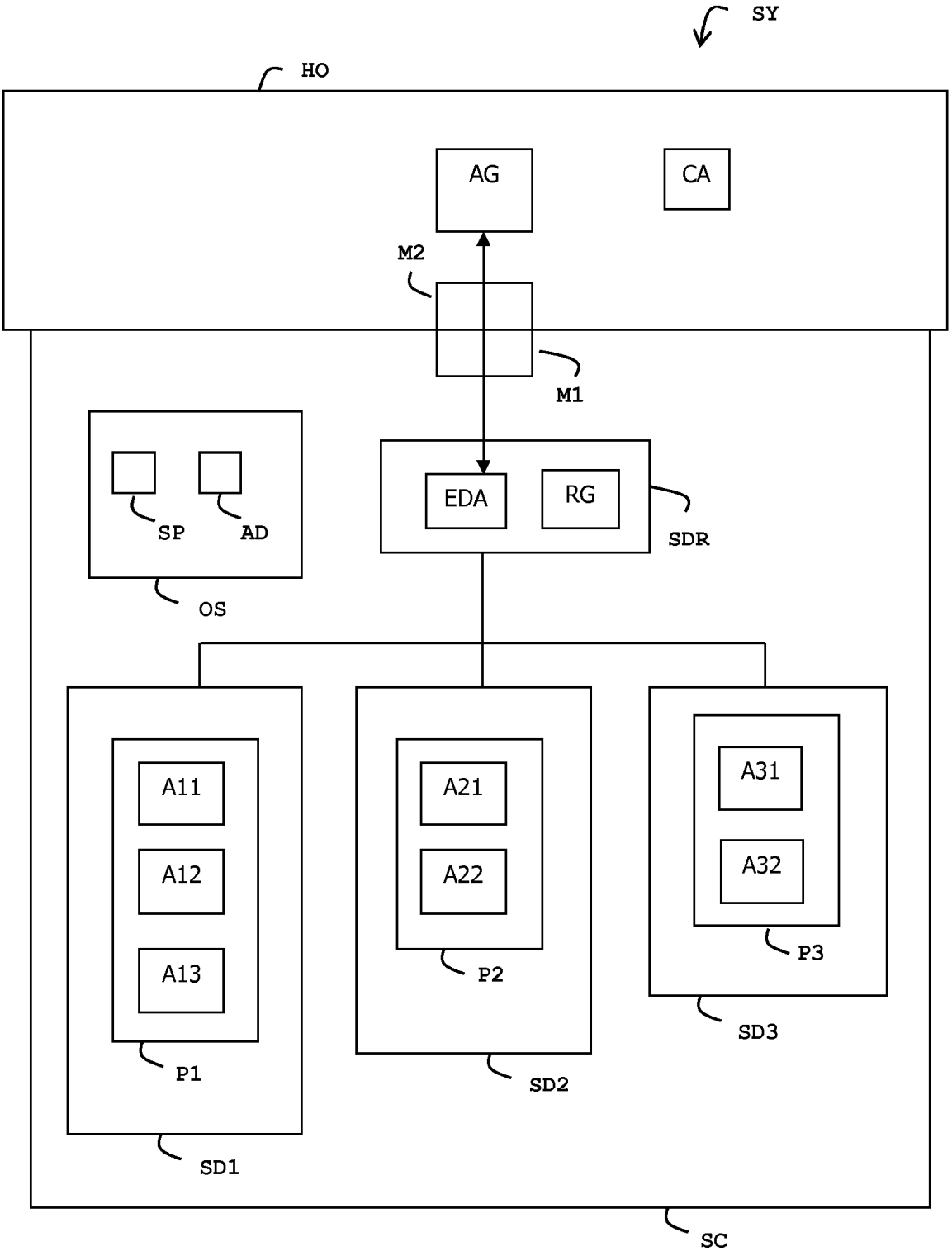
SY
HO
AG
CA
M2
M1
SP
AD
OS
EDA
RG
SDR
A11
A12
A13
P1
SD1
A21
A22
P2
SD2
A31
A32
P3
SD3
SC

FIG. 1

SD-AID	ESTADO	CANALES LÓGICOS REQUERIDOS
AID1	HABILITADO	3
AID2	DESHABILITADO	2
AID3	HABILITADO	2

FIG. 2

SD-AID	ESTADO	CANALES LÓGICOS REQUERIDOS	INTERVALO ATRIBUIDO
AID1	HABILITADO	3	0-2
AID2	DESHABILITADO	2	-
AID3	HABILITADO	2	3-4

FIG. 3

SD-AID	APLICACIÓN SELECCIONADA POR DEFECTO	CANAL LÓGICO ATRIBUIDO
AID1	A13	0
AID2	A21	-
AID3	A32	3

FIG. 4