(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 617 862**

(51) Int. CI.:

G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.09.2012 PCT/EP2012/068314**

(87) Fecha y número de publicación internacional: **11.04.2013 WO13050240**

(96) Fecha de presentación y número de la solicitud europea: **18.09.2012 E 12759727 (6)**

(97) Fecha y número de publicación de la concesión europea: **02.11.2016 EP 2764461**

(54) Título: **Elemento seguro que comprende receptáculos separados y método correspondiente**

(30) Prioridad:

03.10.2011 EP 11306274

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.06.2017

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

BERARD, XAVIER;
ROUSSEL, NICOLAS;
PICO, RICHARD;
FAURE, FRÉDÉRIC y
GONZALVO, BENOÎT

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCION

Elemento seguro que comprende receptáculos separados y método correspondiente.

La presente invención se refiere a elementos seguros que comprenden varias aplicaciones. Se refiere particularmente a elementos seguros que comprenden una máquina y aplicaciones virtuales en receptáculos separados.

Los elementos seguros son pequeños dispositivos que comprenden una memoria, un microprocesador y un sistema operativo para tratamiento de cálculos. Dichos elementos seguros pueden comprender una pluralidad de memorias de diferentes tipos. Se les llama "seguros", porque son capaces de controlar el acceso a los datos que contienen y autorizar o no la utilización de los datos por otras máquinas. Los elementos seguros también pueden ofrecer servicios de cálculo basados en componentes criptográficos. En general, los elementos seguros han limitado los recursos de cálculo y están destinados a ser conectados a una máquina anfitriona. Los elementos seguros pueden ser extraíbles o estar fijados a un dispositivo anfitrión. Las tarjetas inteligentes son elementos seguros portátiles.

Los elementos seguros pueden incorporar una máquina virtual orientada a objetos con el fin de ser capaz de ejecutar aplicaciones escritas en un lenguaje orientado a objetos. Usualmente, estas aplicaciones orientadas a objetos gestionan datos aplicativos que se encuentran en el elemento seguro. Por ejemplo, muchas tarjetas inteligentes comprenden una máquina virtual y applets que cumplen con las especificaciones Javacard ®. Las aplicaciones que se encuentran almacenadas e instaladas en un elemento seguro se refieren generalmente a través de un identificador. Dicho identificador puede ser un Identificador de Aplicación (AID) como se define por el estándar ISO7816-5, por ejemplo. Una aplicación generalmente se gestiona a través de un paquete que se carga en el elemento seguro. A continuación, se crea una instancia de la aplicación en el elemento seguro. Se utiliza un AID para identificar cada paquete de aplicación. Se utiliza un AID para identificar cada instancia de aplicación. Hasta ahora cada AID de paquete de solicitud y cada AID de instancia de aplicación deben ser únicos en un elemento seguro. El carácter único de cada AID permite evitar la ambigüedad cuando se hace referencia a un elemento en un elemento seguro. La máquina virtual gestiona tanto la administración como la interpretación/ejecución de las aplicaciones. La administración corresponde a la carga, la creación/ de instanciación, la actualización y la eliminación de la aplicación.

Una nueva necesidad surge para la gestión de elementos de seguridad destinados a contener una pluralidad de aplicaciones. Ahora se pide descargar e instalar la misma aplicación varias veces en el mismo elemento. Esto plantea la cuestión de la unicidad de los identificadores incrustados en un único elemento seguro.

Hay una necesidad de mejorar la capacidad de administrar varias aplicaciones que utilizan el mismo identificador en un elemento seguro.

Un objeto de la invención es resolver el problema técnico antes mencionado.

El objeto de la presente invención es un elemento seguro que comprende una máquina virtual capaz de trabajar en modo administrador y en modo tiempo de ejecución. El elemento seguro comprende dos receptáculos mejorados. Cada uno de dichos receptáculos mejorados puede estar en estado activado o en estado desactivado. Uno de los receptáculos mejorados puede estar en estado activado en un momento dado. La máquina virtual está adaptada para acceder a cada uno de los receptáculos mejorados cuando se trabaja en modo administrador. La máquina virtual no puede acceder a un receptáculo mejorado que se encuentre en estado desactivado cuando se trabaja en modo tiempo de ejecución.

Ventajosamente, el elemento seguro puede comprender un receptáculo común que puede estar siempre en estado activado independientemente de los receptáculos mejorados. La máquina virtual puede estar adaptada para acceder al receptáculo común cuando se trabaja en modo tiempo de ejecución.

Ventajosamente, el elemento seguro puede comprender una interfaz de comunicación y medios de conmutación adaptados para activar uno de los receptáculos mejorados en respuesta a un comando dedicado recibido a través de la interfaz de comunicación.

Ventajosamente, puede ser instalada una primera aplicación en cada uno de dichos receptáculos mejorados utilizando el mismo identificador de aplicación (AID) en ambos receptáculos mejorados.

Ventajosamente, el elemento seguro puede comprender un registro global que contiene un identificador asociado a una segunda aplicación. La máquina virtual puede estar adaptada para acceder al registro global cuando opera en modo tiempo de ejecución. Cada uno de dichos receptáculos mejorados puede comprender su propio registro local asociado, conteniendo cada registro local el identificador de dicha primera aplicación.
Ventajosamente, cada uno de dichos receptáculos mejorados puede comprender datos relacionados con una suscripción.

Ventajosamente, cada uno de los receptáculos mejorados puede ser gestionado a través de un dominio seguro tal como se define en el estándar GlobalPlatform ®.

Ventajosamente, el elemento seguro puede ser una tarjeta inteligente, una eUICC o un dispositivo máquina a máquina.

Otro objeto de la invención es un método para gestionar un elemento seguro. El elemento seguro comprende un primer y un segundo receptáculo mejorado y una máquina virtual que es capaz de operar en modo administrador y en modo tiempo de ejecución. El método comprende las siguientes etapas:

- activación de un primer receptáculo mejorado, siendo automáticamente desactivado dicho segundo receptáculo mejorado, en el que la máquina virtual no puede acceder a un receptáculo mejorado que se encuentra desactivado cuando se trabaja en modo tiempo de ejecución, ,
- cargar una aplicación en el segundo receptáculo mejorado, mientras dicho segundo receptáculo mejorado permanece desactivado.

Ventajosamente, la etapa de activación puede ser accionada por la recepción de un comando dedicado.

Otro objeto de la invención es un sistema que comprende una máquina y un elemento seguro de acuerdo con la invención (como se describe más arriba). La máquina comprende medios de selección que están adaptados para generar un comando dedicado para accionar la activación de uno de los receptáculos mejorados comprendidos en el elemento seguro.

Ventajosamente, la máquina puede comprender medios gestores adaptados para generar un comando específico para accionar la creación de un nuevo receptáculo mejorado en el elemento seguro.

(Breve descripción de los dibujos)

Otras características y ventajas de la presente invención aparecerán más claramente tras la lectura de la siguiente descripción de un número de formas de realización preferidas de la invención con referencia a los correspondientes dibujos que se acompañan, en los que:

- La Figura 1 representa esquemáticamente un ejemplo de arquitectura de un elemento seguro de acuerdo con la invención;
- La Figura 2 es un ejemplo de tres receptáculos integrados en un elemento seguro de acuerdo con la invención; y
- La Figura 3 es un ejemplo de un sistema que comprende un servidor capaz de manejar la activación de un receptáculo en un elemento seguro de acuerdo con la invención.

(Descripción detallada de las realizaciones preferidas)

La invención puede aplicarse a cualquier tipo de elemento seguro que comprenden una máquina virtual. A pesar de que las siguientes realizaciones se dan para una máquina virtual Javacard ®, la invención puede aplicarse a cualquier tipo de máquina virtual.

La **Figura 1** muestra la arquitectura de un elemento seguro SC de una tarjeta inteligente según la invención. En este ejemplo, el elemento seguro SC es una tarjeta inteligente Java Card ®.

El elemento seguro SC comprende una memoria de trabajo WM, una memoria no volátil ME, un microprocesador MP y una interfaz de comunicación IN. La memoria no volátil ME comprende un sistema operativo OS, una máquina virtual orientada a objetos VM, unos medios de conmutación M1, unos medios de administración M2, unos medios de arranque M4, dos receptáculos mejorados C1 y C2 y un receptáculo común C3. El elemento de seguridad SC está destinado a comprender una pluralidad de aplicaciones orientadas a objetos compilada en código intermedio (por ejemplo, en código de bytes). Estas aplicaciones están pensadas para ser ejecutadas por la máquina virtual VM. En una realización preferida estas aplicaciones son applets JavaCard ®. La tarjeta inteligente SC está destinada a ser conectada a una máquina anfitriona a través de la interfaz de comunicación IN. Por ejemplo, la máquina anfitriona puede ser un ordenador personal o un teléfono móvil. La interfaz IN puede ser una interfaz inalámbrica o una interfaz de contacto.

La memoria de trabajo WM puede ser una RAM. La memoria ME puede ser NAND, flash o memoria EEPROM u otro tipo de memoria no volátil.

En una realización preferida, la memoria ME se implementa como un componente de memoria única. Alternativamente, la memoria ME puede ser implementada gracias a varios componentes de memoria.

Cada uno de los receptáculos mejorados C1 y C2 es un área lógica independiente. El receptáculo común C3 es

también un área lógica independiente. Se supone que todas las aplicaciones y datos aplicativos se almacenan o en receptáculo mejorado o en un receptáculo común. Se supone que todos los elementos del sistema de archivo se almacenan o en receptáculo mejorado o en un receptáculo común.

Cuando un receptáculo mejorado está activo, todos los otros receptáculos mejorados están desactivados. El receptáculo común C3 permanece siempre activo.

Los medios de conmutación M1 son capaces de activar un receptáculo mejorado específico y desactivar el receptáculo mejorado previamente activo. Los medios de conmutación M1 pueden ser activados por un comando dedicado DC1 recibido de una máquina externa. El comando dedicado DC1 puede contener el identificador del receptáculo mejorado específico que se va a activar. Ventajosamente, los medios de conmutación M1 puede activar automáticamente un receptáculo mejorado preestablecido cuando se inicia el elemento seguro SC.

Ventajosamente, los medios de conmutación M1 pueden ser capaces de calcular unos de datos de autorización basados en una clave secreta almacenada previamente en el elemento seguro. Los medios de conmutación M1 pueden ser capaces de autorizar la activación de un receptáculo mejorado sólo si los datos de autorización calculados son correctos. Alternativamente, los medios de conmutación M1 pueden ser capaces de comprobar que se ha establecido una sesión segura con un servidor remoto de confianza o una máquina host conectada. Alternativamente, los medios de conmutación M1 pueden ser capaces de verificar que se han concedido derechos particulares en el elemento seguro SC.

Cuando se trabaja en modo de tiempo de ejecución, la máquina virtual VN no puede acceder a los receptáculos mejorados que están desactivados. En este caso, los receptáculos mejorados que están en estado de desactivación se encuentran ocultos y no se pueden ver o acceder por parte de la máquina virtual. En otras palabras, el contenido de los receptáculos mejorados no es accesible por la máquina virtual. La máquina virtual se considera en modo de tiempo de ejecución cuando la máquina virtual ejecuta (o está a punto de ejecutar) una aplicación escrita en lenguaje intermedio. En el modo de tiempo de ejecución, la máquina virtual sólo puede acceder al contenido del receptáculo mejorado activo y al contenido del receptáculo común. Por lo tanto, en el modo de tiempo de ejecución, la máquina virtual sólo puede acceder al contenido de un único receptáculo mejorado en un momento dado.

Una posible alternativa sería que, en el modo de tiempo de ejecución, la máquina virtual pudiera acceder al contenido de varios receptáculos mejorados, estando cada acceso separado de los otros, por ejemplo a través de un canal lógico de tarjeta inteligente dedicado. De esta manera, sería posible tener varios receptáculos mejorados activos simultáneamente, siendo accesible simultáneamente el receptáculo común desde cada canal lógico.

Cuando se trabaja en el modo de administración, la máquina virtual VM puede acceder a todos los receptáculos existentes mejorados cualquiera que sea su estado. Se considera que la máquina virtual está en modo de administración cuando la máquina virtual realiza (o está a punto de realizar) tratamientos relacionados con la administración del elemento seguro SC. Por ejemplo, tratamientos de administración pueden ser la descarga de una aplicación (o un paquete que incluye una aplicación), tratamientos relacionados con la instanciación de una aplicación escrita en lenguaje intermedio, la personalización de una aplicación, la actualización de una aplicación, la supresión de una aplicación, la creación de un archivo o la creación de un nuevo receptáculo mejorado.

Los medios de administración M2 son capaces de crear un nuevo receptáculo mejorado o una aplicación o un elemento del sistema de archivos en un receptáculo mejorado predestinado. Los medios de administración M2 pueden acceder tanto a receptáculos mejorados activos como inactivos. Los medios de administración M2 también pueden acceder al receptáculo común C3. Los medios de administración M2 pueden ser activados por un comando específico DC2 recibido de una máquina externa. El comando específico DC2 puede contener el identificador del receptáculo mejorado que se va a crear o el identificador del receptáculo mejorado en el que se va a crear una nueva aplicación o elemento del sistema de archivos.

Los medios de administración M2 son capaces de cargar una aplicación (o el paquete de una aplicación), de instanciar una aplicación, de crear un archivo o un sistema de archivos, de actualizar un archivo, de actualizar una aplicación o un aplicativo de datos.

La máquina virtual VM comprende ambos medios M1 y M2.

Un elemento seguro SC no está limitado a dos receptáculos mejorados y puede comprender cualquier número de receptáculos mejorados.

La **Figura 2** muestra un ejemplo de forma de realización de tres receptáculos C1, C2 y C3, que están incrustados en el elemento seguro SC de acuerdo con la invención. C1 y C2 son receptáculos mejorados. C3 es un receptáculo común.

En esta realización, los receptáculos se implementan a través del mecanismo de dominio de seguridad como se define en el estándar de las Especificaciones de Tarjeta de GlobalPlatfom V2.2 ®.

El receptáculo común C3 comprende el dominio de seguridad emisor (también llamado ISD) y un dominio de seguridad suplementario (también llamado SSD). El identificador del dominio de seguridad emisor es AID-1. El identificador del dominio de seguridad suplementario es AID-2. El dominio de seguridad suplementario comprende una aplicación (también llamada AP) cuyo AID es AID-5.

El receptáculo mejorado C1 comprende un dominio de seguridad suplementario cuyo identificador es AID-3. Este dominio de seguridad suplementario comprende dos aplicaciones cuyos AID son AID-6 y AID-7, respectivamente.

El receptáculo mejorado C2 comprende un dominio de seguridad suplementario cuyo identificador es AID-4. Este dominio de seguridad suplementario comprende dos aplicaciones cuyos AID son AID-6 y AID-8, respectivamente.

Cabe señalar que tanto el C1 como el C2 contienen una aplicación con el mismo identificador (es decir, AID-6). Según la invención, solamente un receptáculo mejorado puede estar activo en cualquier momento dado. Según la invención, cuando la máquina virtual VM está en modo de tiempo de ejecución, dicha máquina virtual VM ve sólo el receptáculo mejorado activo y el receptáculo común C3. En consecuencia, no hay ambigüedad cuando la máquina virtual VM debe ejecutar la aplicación cuyo identificador es AID-6.

De acuerdo con la invención, cuando la máquina virtual VM está en el modo de carga, dicha máquina virtual VM ve todos los receptáculos mejorados existentes.

Se puede utilizar un mecanismo basado en varios registros para diferenciar de manera correcta el identificador de cada aplicación. Por ejemplo, el receptáculo común C3 puede tener un registro global y cada receptáculo mejorado puede tener su propio registro local.

El registro global puede contener el identificador de todos los elementos (por ejemplo aplicaciones, paquetes, dominio de seguridad) que están presentes en el receptáculo común C3. El registro global también puede contener el identificador de todos los receptáculos mejorados existentes. Ventajosamente, el registro global también puede contener una referencia al registro local de cada uno de los receptáculos mejorados existentes.

Un registro local contiene el identificador de todos los elementos (por ejemplo, aplicaciones, paquetes, dominio de seguridad) que están presentes en el receptáculo mejorado asociado a este registro local.

Alternativamente, sólo hay un registro global (es decir, sin necesidad de registro local), que contiene el identificador de todos los elementos existentes en todos los receptáculos. En este caso, el AID-6 se produce dos veces en el registro global: una vez ligada al AID-3 y la segunda ligada al AID-4 con el fin de distinguir claramente ambas aplicaciones que comparten el mismo identificador.

Una nueva aplicación cuyo identificador es AID-7 se puede cargar e instanciar en el receptáculo mejorado C2. Incluso si una aplicación que tiene el identificador AID-7 ya está instalada en el receptáculo mejorado C1. Esta nueva aplicación se puede descargar en el elemento seguro SC mediante las formas habituales. Por ejemplo, si el elemento seguro SC es una eUICC (Tarjeta Universal de Circuito Integrado incrustado), la solicitud puede ser enviada a través del mecanismo Over-the-Air (OTA) definido en el estándar de Telecomunicaciones. Si el elemento seguro SC está conectado a una máquina host que puede acceder a Internet, la solicitud puede ser enviada a través de Internet y otras redes.

El comando específico DC2 puede ser enviado a la RAM (Gestión de Aplicación Remota, como se define en el estándar ETSI 102.226) entidad asociada con el receptáculo mejorado predestinado.

Ventajosamente, cada receptáculo mejorado puede ser dedicado a una suscripción. En este caso, el receptáculo mejorado comprende todos los elementos que corresponden a la suscripción. Estos elementos pueden ser cualquier combinación de un conjunto de aplicaciones, un conjunto de datos secretos, un conjunto de datos aplicativos, un conjunto de datos de administración, un conjunto de archivos estructurados en un sistema de archivos, etc. Por ejemplo, el receptáculo mejorado C1 puede corresponder a una suscripción de telecomunicaciones y el receptáculo mejorado C2 puede corresponder a una suscripción bancaria. En otro ejemplo, el receptáculo C1 puede corresponder a una suscripción de telecomunicaciones profesional y el receptáculo C1 del contenedor puede corresponder a una suscripción de telecomunicaciones privada con el mismo operador de red móvil. En este caso ambas suscripciones se supone que comprenden muchos elementos idénticos.

Los receptáculos mejorados pueden implementarse a través de cualquier mecanismo lógico o físico que permita identificar un conjunto de elementos que son gestionados gracias a normas comunes.

La **Figura 3** muestra un ejemplo de un sistema SY que comprende un servidor SV capaz de desencadenar la activación de un receptáculo mejorado en un elemento seguro SC de acuerdo con la invención.

La invención resulta muy adecuada para permitir que un servidor remoto desencadene la activación de un receptáculo mejorado predestinado en un elemento de seguridad que ya se encuentra desplegado en el ámbito. Por

ejemplo, el elemento seguro puede ser un módulo Máquina-a-Máquina o cualquier tipo de tarjeta inteligente.

El SV servidor remoto SV accede al elemento seguro SC a través de una red que puede estar basada en una red privada o pública. Por ejemplo, el servidor SV puede utilizar una red de telecomunicaciones (perteneciente a un operador móvil) cuando se comunica con un elemento de seguro. El servidor SV comprende unos medios de selección M3 adaptados para generar un comando destinado DC1 previsto para activar los medios de conmutación M1 del elemento seguro SC. El comando DC1 construido por los medios de selección M3 contiene el identificador pertinente del receptáculo mejorado predestinado. El receptáculo mejorado puede tener un identificador destinado asignado por el elemento seguro o el servidor remoto en tiempo de creación. Alternativamente, en el caso de receptáculos mejorados implementados a través de dominio de seguridad, el AID del receptáculo mejorado puede ser el AID de su dominio de seguridad correspondiente. Por ejemplo, el comando DC1 puede contener el AID-4 como identificador si se requiere la activación del receptáculo mejorado C2.

El servidor SV comprende unos medios de gestión M5 adaptados para generar un comando específico DC2 previsto para activar los medios de administración M2 del elemento seguro SC. Ventajosamente, el comando DC2 construido por los medios de gestión M5 puede contener el identificador del nuevo receptáculo mejorado.

Ventajosamente, el SV servidor también puede ser capaz de enviar directamente el comando DC1 al elemento seguro. Alternativamente, el comando DC1 puede ser enviado al elemento seguro SC por una máquina intermediaria.

En el caso del módulo de Máquina-a-Máquina, el servidor SV puede acceder al elemento seguro a través de Internet, de una red inalámbrica o de cualquier canal existente.

El comando específico DC2 se puede implementar a través de un comando "Instalar para instalar" como se define por GlobalPlatform V2.2 ®, por ejemplo, mediante el uso de un privilegio particular. Por ejemplo, el privilegio de Gestión Autorizada puede ser utilizado con una diferencia frente a GP 2.2: no hay derecho a eliminar los antecesores.

El comando destinado DC1 puede implementarse mediante un comando "Establecer estado" tal como se define por GlobalPlatform V2.2 ®, mediante el uso de "Estado Personalizado".

Ventajosamente, la máquina virtual VM puede comprender unos medios de inicialización M4 que permiten iniciarse al elemento seguro SC sin la existencia de receptáculo mejorado. Una vez que el elemento seguro ha arrancado a través de los medios de inicialización M4, los medios de administración M2 pueden ser activados para crear un primer receptáculo mejorado en respuesta a la recepción del comando DC2.

Como se ha descrito anteriormente, se puede instanciar una aplicación en varios receptáculos mejorados utilizando el mismo identificador. Gracias a la invención, no hay preocupación por los identificadores conflictivos. De la misma manera, un paquete de aplicación se puede cargar en varios receptáculos mejorados utilizando el mismo identificador.

De acuerdo con la invención, el elemento seguro SC gestiona por sí mismo la existencia de varios componentes con idénticos identificadores. Las máquinas externas (por ejemplo, servidor remoto o máquina host conectada) no tienen que preocuparse por la colisión de identificador entre receptáculos mejorados distintos. Las máquinas externas sólo necesitan asegurarse del carácter único del identificador dentro del mismo receptáculo mejorado.

REIVINDICACIONES

1. Un elemento seguro (SC) que comprende una máquina virtual (VM) capaz de trabajar en modo de administración y en modo de tiempo de ejecución,
caracterizado porque dicho elemento seguro (SC) comprende dos receptáculos mejorados (C1, C2), pudiendo estar cada uno de dichos receptáculos mejorados (C1, C2) o bien en un estado activado o en un estado desactivado, **y porque** la máquina virtual (VM) es capaz de acceder a cada uno de dichos receptáculos mejorados (C1, C2) cuando trabaja en el modo de administración, **y porque** sólo uno de dichos receptáculos mejorados (C1, C2) puede estar en estado activado en un momento dado, **y porque** la máquina virtual (VM) no puede acceder a un receptáculo mejorado que esté en estado desactivado cuando trabaja en modo de tiempo de ejecución, **y porque** dicho elemento seguro (SC) comprende unos medios de administración (M2) adaptados para almacenar una instancia de una misma aplicación en cada uno de dichos receptáculos mejorados (C1, C2) utilizando un mismo identificador.

2. Un elemento seguro (SC) según la reivindicación 1, en el que dicho elemento seguro (SC) comprende un receptáculo común (C3) que siempre está en estado activado independientemente de dichos receptáculos mejorados (C1, C2), y en el que la máquina virtual (VM) está adaptada para acceder a dicho receptáculo común (C3) cuando trabaja en modo de tiempo de ejecución.

3. Un elemento seguro (SC) según cualquiera de las reivindicaciones 1 a 2, en el que dicho elemento seguro (SC) comprende una interfaz de comunicación (IN) y unos medios de conmutación (M1) adaptados para activar uno de dichos receptáculos mejorados (C1, C2) en respuesta a un comando dedicado (DC1) recibido a través de la interfaz de comunicación (IN).

4. Un elemento seguro (SC) según cualquiera de las reivindicaciones 1 a 3, en el que dicho elemento seguro (SC) comprende un registro global que contiene un identificador asociado a una segunda aplicación, en el que la máquina virtual (VM) está adaptada para acceder al registro global cuando trabaja en modo de tiempo de ejecución, en el que cada uno de dichos receptáculos mejorados (C1, C2) comprende su propio registro local asociado, cada registro local conteniendo el identificador de dicha primera aplicación.

5. Un elemento seguro (SC) según cualquiera de las reivindicaciones 1 a 4, en el que cada uno de dichos receptáculos mejorados (C1, C2) comprende datos relacionados con una suscripción.

6. Un elemento seguro (SC) según cualquiera de las reivindicaciones 1 a 5, en el que cada uno de dichos receptáculos mejorados (C1, C2) se gestiona a través de un dominio de seguridad tal como se define en el estándar GlobalPlatform ®.

7. Un elemento seguro (SC) según cualquiera de las reivindicaciones 1 a 6, en el que dicho elemento seguro (SC) es una tarjeta inteligente, una eUICC o un dispositivo Máquina-a-Máquina.

8. Un método para la gestión de un elemento seguro (SC), que comprende una máquina virtual (VM) capaz de trabajar en modo de administración y en modo de tiempo de ejecución,
caracterizado porque dicho elemento seguro (SC) comprende un primer y un segundo receptáculo mejorado (C1, C2) y **porque** dicho método comprende los siguientes pasos:

- activación del primer receptáculo mejorado (C1), estando dicho segundo receptáculo mejorado (C2) desactivado automáticamente, en el que la máquina virtual (VM) no puede acceder a un receptáculo mejorado se encuentra desactivado cuando trabaja en modo de tiempo de ejecución,

- cargar una aplicación en dicho segundo receptáculo mejorado (C2), mientras dicho segundo receptáculo mejorado (C2) permanece desactivado, estando dicha aplicación ya cargada en dicho primer receptáculo mejorado (C1) utilizando un mismo identificador de aplicación.

9. Un sistema (SY) que comprende una máquina (SV) y un elemento seguro (SC),
caracterizado porque el elemento seguro (SC) es de acuerdo con la reivindicación 1 **y porque** dicha máquina (SV) comprende unos medios de selección (M3) adaptados para generar un comando dedicado (DC1) para iniciar la activación de uno de los receptáculos mejorados (C1, C2) comprendido en el elemento seguro (SC).

10. Un sistema de acuerdo con la reivindicación 9, en el que dicha máquina (SV) comprende unos medios de gestión (M5) adaptados para generar un comando específico (DC2) para activar la creación de un nuevo receptáculo mejorado en el elemento seguro (SC).

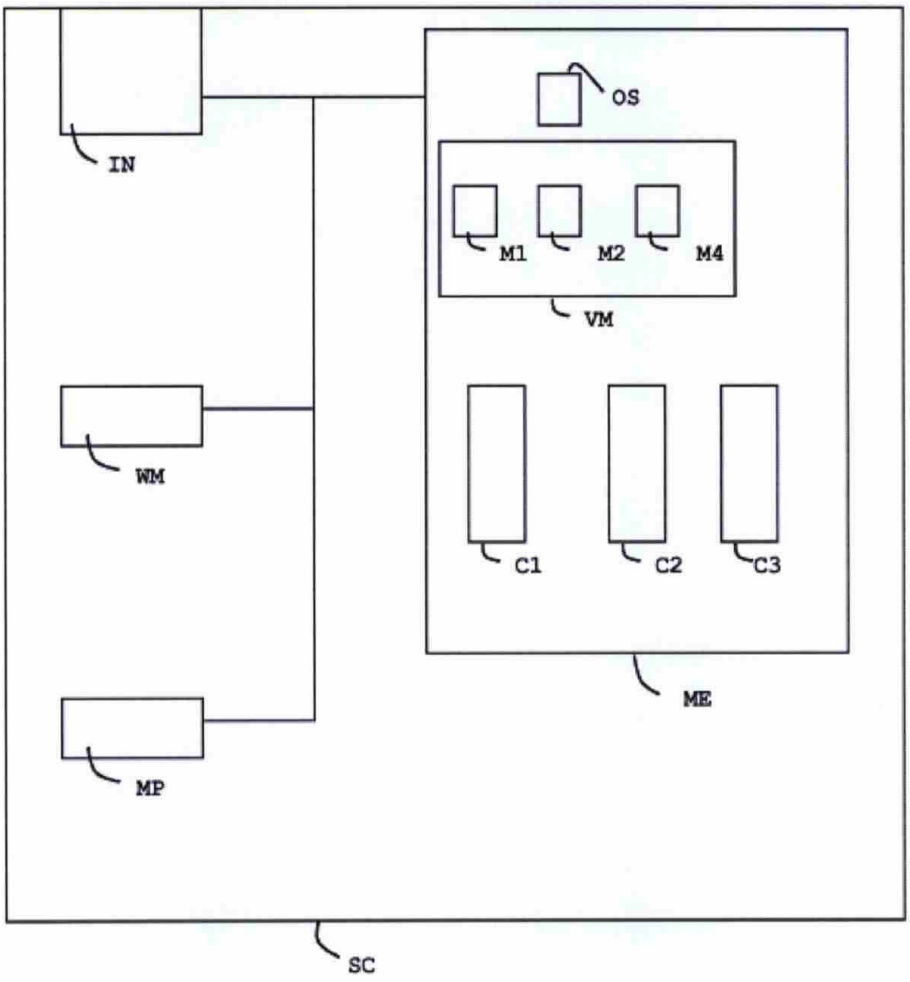

FIG.1

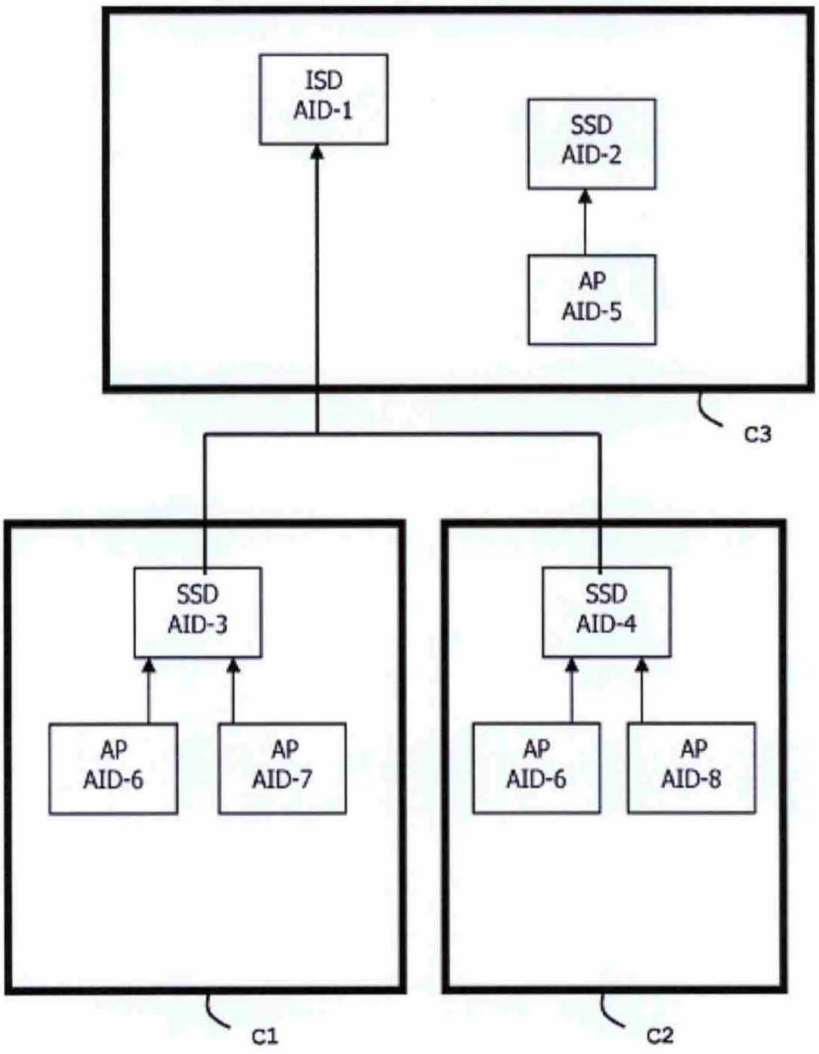
ISD
AID-1
SSD
AID-2
AP
AID-5
C3
SSD
AID-3
AP
AID-6
AP
AID-7
C1
SSD
AID-4
AP
AID-6
AP
AID-8
C2

FIG.2

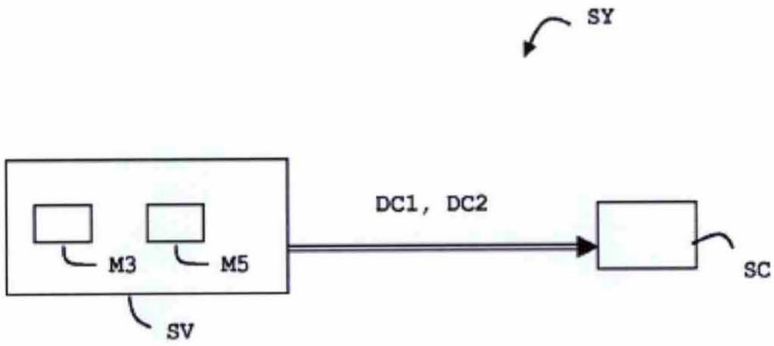

FIG.3