(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 671 011**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04W 4/00 (2008.01)
H04W 12/04 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.12.2013 E 13196373 (8)**

(97) Fecha y número de publicación de la concesión europea: **14.02.2018 EP 2741466**

(54) Título: **Procedimiento y sistema de gestión de un elemento de seguridad integrado eSE**

(30) Prioridad:

10.12.2012 FR 1261829

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.06.2018

(73) Titular/es:

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

(72) Inventor/es:

DANREE, ARNAUD y
LARIGNON, GUILLAUME

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento y sistema de gestión de un elemento de seguridad integrado eSE

Campo de la invención

La invención se refiere al campo de los elementos de seguridad integrados, o "embedded secure elements" eSE, y más particularmente a un procedimiento de gestión de dichos elementos de seguridad integrados, y a un sistema correspondiente.

Contexto de la invención

Se conocen varios tipos de elementos de seguridad utilizados en unos dispositivos huésped tales como terminales móviles, teléfonos portátiles inteligentes (smartphones), tabletas digitales, etc.

Un primer tipo es conocido bajo la denominación de tarjeta UICC (Universal Integrated Circuit Card) contemplada en la norma ETSI SP 102.221 y reagrupa las tarjetas de chips clásicas, tipo tarjeta SIM (o USIM - Universal Subscriber Identity Module), e igualmente unas fichas (token) de seguridad.

Un segundo tipo, que se considera en la presente invención, es conocido bajo la denominación de "embedded secure element" o eSE y se contempla en la especificación "GlobalPlatform Card Specification Version 2.2.1" relativa a la tecnología GlobalPlatform.

Estos dos tipos de elementos de seguridad disponen de medios o mecanismos de seguridad interna para asegurar la integridad y la seguridad de los datos sensibles y servicios sensibles que albergan.

Una diferencia esencial entre estos dos tipos de elementos de seguridad reside en la autonomía que tienen para establecer una conexión con un equipo distante, típicamente un servidor OTA (Over-The-Air) externo al dispositivo huésped.

La tarjeta UICC dispone de medios maestros en el establecimiento de la conexión de ese tipo. En otros términos, una aplicación de la tarjeta UICC puede tomar la iniciativa en un establecimiento de ese tipo, basándose por ejemplo en unas capacidades disponibles en el dispositivo huésped (por ejemplo las herramientas SIM ToolKits). Se dice que la tarjeta UICC es un elemento de seguridad "conectado".

Una tarjeta UICC puede enviar por su propia iniciativa un SMS a un servidor OTA para iniciar una conexión de esa forma. A título de ilustración, la publicación EP 2.453.377 describe una UICC en la que un agente administrador es capaz de gestionar un servidor OTA a través de una conexión HTTP.

El elemento de seguridad integrado eSE es, por su parte, un elemento esclavo de aplicaciones residentes en el dispositivo huésped, es decir esclavo en una relación maestro - esclavo en las capas altas del modelo OSI, principalmente en la capa de aplicación (capa 7), incluso en las capas 5 y 6. De ese modo el establecimiento de una conexión con el exterior necesita una aplicación residente en el dispositivo huésped, que es la única a tomar la iniciativa en este establecimiento. Es esta aplicación la que decide poner en relación el eSE con un servidor externo.

A título de ejemplo, el eSE puede formar el elemento de seguridad necesario para numerosos usos o servicios que se basan en una comunicación NFC (Near Field Communication) implementada por un terminal móvil huésped. Por ejemplo, un servicio de pago NFC necesita informaciones bancarias secretas del usuario que están ventajosamente almacenadas en el eSE, al abrigo de cualquier acceso intempestivo.

La Figura 1 ilustra una arquitectura lógica de un eSE 50 y de un dispositivo huésped 100 que lo integra, de acuerdo con la tecnología GlobalPlatform.

El eSE 50 comprende un sistema operativo OS_{eSE}, un dominio de seguridad principal o "raíz" 51, indicado como ISD por Issuer Security Domain, y unas aplicaciones App accesibles a través del ISD 51. Pueden preverse igualmente otros dominios de seguridad 52, 53 (supplementary security domains, SSD) de menor prioridad en el ISD 51 con sus aplicaciones App.

El ISD 51 está necesariamente en el seno del eSE para permitir una administración del elemento de seguridad eSE y principalmente la gestión de los otros dominios de seguridad. Esto permite por ejemplo al poseedor/propietario del ISD 51 subarrendar una parte del eSE o compartir el control con otros socios, por ejemplo comerciales, instalándoles unos dominios de seguridad propios.

Como el eSE es un equipo esclavo de aplicaciones residentes del dispositivo huésped 100 que proporciona a un usuario final unos servicios (App1, App2, App3), la tecnología GlobalPlatform define la interfaz entre estas

aplicaciones residentes y el eSE. Define principalmente la API (Application Programming Interface) prevista en el dispositivo huésped para acceder al eSE a través de controladores de software (drivers).

Unos ejemplos de aplicaciones App1, App2, App3 incluyen aplicaciones de pago móvil, aplicaciones de billetes de transporte (transport ticketing), aplicaciones de control de acceso, aplicaciones de peaje, etc. Se ha de observar que unos mecanismos internos del eSE (principalmente las ACF - Access Control Function) permiten asociar las aplicaciones residentes a cada dominio de seguridad del eSE.

Cada dominio de seguridad posee un juego de claves criptográficas, generalmente al menos tres claves, que se utilizan para la implementación de comunicaciones de seguridad con unos servidores de una infraestructura externa que poseen igualmente estas claves o unas claves correspondientes (caso de claves asimétricas), pero igualmente para la gestión de seguridad de contenidos en el eSE por estos servidores externos, por ejemplo la gestión de claves internas, el cifrado/descifrado, el control de la secuencia de órdenes APDU, etc. para dar seguridad al acceso a unos datos y servicios internos del eSE.

Por consiguiente, existe para cada dominio de seguridad del eSE una infraestructura o entidad externa que contiene las claves asociadas a este dominio de seguridad. Estas entidades externas ponen así a disposición de los usuarios finales unas aplicaciones a instalar sobre el terminal huésped y que interactuarán con el eSE para proporcionar servicios.

El ISD 51 se vincula al emisor o poseedor o propietario del eSE, a saber generalmente el fabricante del dispositivo huésped 100. Los SSD se vinculan a los socios comerciales del fabricante, a saber la Entidad 1 y la Entidad 2.

Para asegurar la administración de seguridad del eSE, el emisor o poseedor o propietario (Issuer) dispone de un representante de la aplicación en el seno del dispositivo huésped. Este representante se implementa mediante un agente de aplicación residente en el dispositivo huésped que permite el establecimiento entre servidores de administración del Issuer y el ISD 51 del eSE. Este agente de aplicación es conocido bajo la denominación de agente administrador o "Admin agent" según la especificación "GPD_SPE_008 - Secure Element Remote Application Management" y se configura para conectarse a uno o varios servidores de administración gestionados por el Issuer. Es de uso común denominarle "Proxy agent" porque pone en relación (función proxy) estos servidores de administración con el dominio de seguridad raíz ISD 51 del eSE. En lo que sigue, se hará esencialmente referencia a un "Admin/Proxy Agent".

Resumen de la invención

Con el fin de mejorar la oferta de servicios para un dispositivo huésped, se concibe de aquí en adelante transferir la gestión administrativa del eSE del Issuer inicial a otra entidad externa que se convierte en el nuevo "Issuer" del eSE, por ejemplo un socio local (a escala de un país, de una región por ejemplo) susceptible de proporcionar servicios locales adaptados. Esta transferencia de gestión administrativa es simultánea generalmente con una transferencia de propiedad del eSE.

A observar que la propiedad del eSE puede ser múltiple, es decir mantenida por varias entidades externas, en cuyo caso se prevén varios juegos respectivos de claves criptográficas en el dominio de seguridad raíz 51.

La gestión administrativa del eSE puede transferirse de nuevo posteriormente. De ese modo pueden producirse varias transferencias sobre el mismo eSE durante la duración de su vida.

La transferencia de gestión administrativa consiste técnicamente en transferir el juego de claves criptográficas del dominio de seguridad raíz 51 a la entidad externa nuevamente "Issuer". Esta última utiliza generalmente los privilegios de administrador nuevamente adquiridos para modificar este juego de claves. En una variante, se crea un nuevo juego de claves criptográficas y posteriormente se carga en el ISD 51 en sustitución del antiguo juego. El nuevo juego de claves se comunica al nuevo propietario. La carga puede efectuarse por un tercero de confianza denominado Certificate Authority (CA) definido por GlobalPlatform que posee un dominio de seguridad en el eSE denominado CASD. Como se describe en GlobalPlatform, el nuevo juego de claves se filtra por el juego de claves del CASD para ser transmitido de manera confidencial en el eSE.

El nuevo Issuer debe instalar entonces, en el dispositivo huésped 100, un Admin/Proxy Agent que le corresponde con el fin de acceder al eSE y de administrarlo a través del ISD 51. La necesidad de tener que recurrir a un nuevo Admin/Proxy Agent puede ser el resultado por ejemplo de especificidades protocolarias vinculadas a los servidores de administración de este nuevo Issuer.

La Figura 2 muestra este contexto en el que una aplicación App4 del nuevo propietario se ha instalado igualmente para ofrecer a los usuarios finales un servicio que le corresponde. Los dos Admin/Proxy Agents del antiguo Issuer y del nuevo Issuer coexisten así en el dispositivo huésped 100.

Surge un problema cuando el dispositivo huésped 100 es el lugar de una reinicialización (reset), voluntaria o automática. Esta reinicialización puede deberse por ejemplo a la venta del dispositivo huésped o a unos problemas de software que necesiten una reinstalación completa, pero puede sobrevenir igualmente a continuación de un robo del dispositivo huésped.

Deben definirse por tanto unos mecanismos de seguridad para impedir el acceso y la utilización de los datos y servicios sensibles del eSE.

Ahora bien, la reinicialización del dispositivo huésped conduce a la supresión del conjunto de las aplicaciones residentes, a excepción del OS. Se suprimen entonces los dos Admin/Proxy Agents. Ya no es por tanto posible administrar el eSE desde la infraestructura del nuevo Issuer, porque se recuerda que el eSE no puede iniciar una conexión de su propio jefe. El eSE se ha convertido así en inutilizable como se muestra por las cruces en la Figura 3.

La presente invención tiene así por objeto paliar al menos uno de estos inconvenientes, con el fin principalmente de asegurar la utilización del elemento de seguridad integrado cuando es de tipo no conectado.

En este contexto, un primer aspecto de la invención se refiere a un procedimiento de gestión de un elemento de seguridad integrado, eSE, en un dispositivo huésped, siendo únicamente accesible el elemento de seguridad integrado como esclavo de al menos una aplicación residente del dispositivo huésped en una relación maestro-esclavo, e incluyendo el elemento de seguridad integrado un dominio de seguridad raíz, ISD, al que se asocia un juego de claves para implementar unos mecanismos de seguridad (juego poseído por una entidad externa, el Issuer corriente, al que se busca encontrar), comprendiendo el procedimiento las etapas siguientes:

transmitir un mensaje que incluye un identificador del elemento de seguridad integrado eSE, desde un agente de aplicación integrado en un sistema operativo del dispositivo huésped con destino en una primera entidad externa al dispositivo huésped y registrado en el agente de aplicación;
determinar una segunda entidad externa al dispositivo huésped (diferente de la primera entidad externa) poseedora del juego de claves asociado al dominio de seguridad raíz.

El procedimiento de gestión según la invención contribuye a la seguridad del eSE en la medida en la que permite encontrar la entidad externa propietaria de este (el Issuer actual), es decir el único a tener los privilegios de administración total del eSE a través del ISD y esto a pesar de la desaparición de su Admin/Proxy Agent en el seno del dispositivo huésped. Podrían tomarse así unas acciones sobre el eSE cómo se describe a continuación, principalmente si se trata de que este elemento de seguridad integrado haya sido robado.

La eficacia de este procedimiento se basa principalmente en la integración de un agente de aplicación, el Admin/Proxy Agent, en el seno mismo del sistema operativo del dispositivo huésped. Preferentemente, se trata del agente de aplicación del fabricante porque es el que elabora generalmente el sistema operativo. En efecto, esta configuración permite conservar este agente de aplicación a pesar de la reinicialización del dispositivo huésped y utilizarle en el proceso de identificación del Issuer actual gracias a su vínculo con el fabricante (la primera entidad externa).

Como se describe más en detalle en lo que sigue, son unas informaciones de transferencia de propiedad o de derechos de administración sobre el elemento de seguridad las que permitirán por ejemplo identificar al nuevo Issuer (la segunda entidad externa). Principalmente la determinación del nuevo Issuer se podrá conocer gracias a una o varias bases de datos dedicadas a memorizar las informaciones de transferencia de propiedad o de derechos de administración sobre el eSE.

Correlativamente, un segundo aspecto de la invención se refiere a un sistema de gestión de un elemento de seguridad integrado, eSE, en un dispositivo huésped, siendo únicamente accesible el elemento de seguridad integrado como esclavo de al menos una aplicación residente del dispositivo huésped en una relación maestro-esclavo, e incluyendo el elemento de seguridad integrado un dominio de seguridad raíz, ISD, al que se asocia un juego de claves para implementar unos mecanismos de seguridad, comprendiendo el sistema:

un agente de aplicación integrado en un sistema operativo del dispositivo huésped y configurado para transmitir un mensaje que incluye un identificador del elemento de seguridad integrado eSE, con destino en una primera entidad externa al dispositivo huésped y registrado en el agente de aplicación; y
la primera entidad (el Issuer inicial) externo al dispositivo huésped tal como está registrada en el agente de aplicación, y configurado para determinar una segunda entidad externa al dispositivo huésped poseedor del juego de claves asociado al dominio de seguridad raíz.

El sistema presenta ventajas similares al procedimiento según la invención.

Se describen en las reivindicaciones dependientes otras características del procedimiento y del sistema según unos modos de realización.

Por ejemplo, en un modo de realización, el procedimiento comprende además transmitir el mensaje recibido desde la primera entidad externa con destino en la segunda entidad externa determinada; y verificar por dicha segunda entidad externa que esta es la poseedora del juego de claves asociado al dominio de seguridad raíz a partir del mensaje recibido.

Esta disposición ofrece un grado suplementario de seguridad para encontrar al Issuer corriente del eSE, porque la segunda entidad externa (es decir la entidad determinada como pretendido Issuer corriente) verifica por sí misma ser la poseedora de las claves de cifrado con ayuda del mensaje emitido por el agente de aplicación integrado en el dispositivo huésped.

En un modo de realización, transmitir el mensaje hacia la segunda entidad externa se efectúa poco a poco, recibiendo una entidad externa el mensaje que le transmiten hacia una entidad externa destinataria registrada, en una base de datos local a la entidad externa receptora, como sucesora de la entidad externa receptora en la posesión del juego de claves asociado a dicho dominio de seguridad raíz.

Esta configuración permite elevarse por la cadena de posesión/propiedad del eSE desde el Issuer inicial (el fabricante) hasta el Issuer actual, sin tener que recurrir a unos equipos distintos a la infraestructura propia de cada uno de estos Issuers sucesivos.

En otro modo de realización, determinar una segunda entidad externa comprende:

emitir, por la primera entidad externa, una solicitud de un servidor central para obtener un identificador de la segunda entidad externa, identificando la solicitud el elemento de seguridad integrado.

Esta disposición permite acceder directamente a la entidad externa pretendidamente propietaria/Issuer actual del elemento de seguridad integrado. La verificación prevista con la ayuda del mensaje recibido permite confirmar la información de propiedad memorizada en el servidor central. Este modo de realización se convierte en más rápido que el anterior modo de realización en el caso de que la cadena de posesión/propiedad del eSE sea particularmente larga.

En otro modo de realización, determinar una segunda entidad externa y transmitir el mensaje recibido hacia la segunda entidad externa comprende:

emitir una notificación por la primera entidad externa a un servidor central, identificando dicha notificación el elemento de seguridad integrado;
a nivel del servidor central, identificar localmente la segunda entidad externa a partir del identificador del elemento de seguridad integrado indicado en la notificación, y emitir una segunda notificación a la segunda entidad externa tal como se identificó localmente;
con iniciativa en la segunda entidad externa tal como se identificó localmente, establecer una conexión entre esta segunda entidad externa y la primera entidad externa de manera que se reciba de esta última dicho mensaje.

Esta disposición permite igualmente superar largas cadenas de posesión/propiedad y permite soslayar la primera entidad externa (generalmente la infraestructura del fabricante de los dispositivos huéspedes) en caso de recepción de un gran número de mensajes. En efecto, en este modo de realización, una parte del bucle entre esta primera entidad y la entidad actualmente propietaria del elemento de seguridad integrado es desviada sobre el servidor central y sobre esta última entidad externa.

En otro modo de realización, el elemento de seguridad integrado (por ejemplo a nivel del ISD) comprende, en la memoria, un campo de datos para memorizar la identificación de una entidad externa poseedora del juego de claves asociado a dicho dominio de seguridad raíz, siendo actualizado dicho campo de datos cuando la entidad externa poseedora del juego de claves cambia, y
el agente de aplicación recupera la identificación de entidad externa indicado en el campo de datos del elemento de seguridad integrado y transmite esta identificación a la primera entidad externa de manera que esta última establezca una conexión con la segunda entidad externa con ayuda de esta identificación para transmitirle dicho mensaje.

Esta configuración permite a la vez liberarse del servidor central y de las tardanzas que pueden resultar de una larga cadena de posesión/propiedad.

En un modo de realización, el procedimiento comprende además las etapas siguientes, en el agente de aplicación integrado en el sistema operativo del dispositivo huésped:

transmitir, al dominio de seguridad raíz ISD del elemento de seguridad integrado eSE, un primer mensaje generado por el agente de aplicación;
como respuesta, recibir un mensaje cifrado por al menos una clave del juego de claves asociado al dominio de seguridad raíz;

procedimiento en el que los mensajes transmitidos a la primera y segunda entidades externas incluyen el mensaje cifrado, y la verificación por la segunda entidad externa se efectúa a partir del mensaje cifrado recibido y de al menos una clave memorizada en la segunda entidad externa.

Esta disposición ofrece un nuevo grado suplementario de seguridad para encontrar al Issuer corriente del eSE, porque la validación por la segunda entidad externa se basa en un mensaje cifrado con la ayuda de una clave de cifrado propia del eSE.

La verificación puede consistir por ejemplo en descifrar el mensaje recibido con la ayuda de la clave poseída localmente para asegurarse bien de poseer las claves correspondientes al eSE. De manera opuesta, puede consistir en cifrar un dato conocido (aquel que haya servido al eSE para generar el mensaje cifrado) con la ayuda de la clave poseída y posteriormente en comparar el resultado con el mensaje cifrado recibido.

En un modo de realización, el procedimiento comprende una etapa previa de reinicialización del dispositivo huésped (que conduce por ejemplo al borrado de cualquier dato en el dispositivo huésped salvo el sistema operativo), y en el que la etapa de transmisión del primer mensaje al dominio de seguridad raíz por el agente de aplicación se desencadena en el reinicio del dispositivo huésped consecutivamente a la reinicialización.

Esta disposición permite la implementación de la invención desde una reinicialización del dispositivo huésped, porque esta última se realiza generalmente después del robo de un equipo. El aseguramiento del elemento de seguridad según la invención se hace por tanto tan eficaz como posible contra los robos.

Según una característica particular, la reinicialización del dispositivo huésped desencadena una reinicialización del elemento de seguridad integrado mediante el envío de una orden apropiada por el sistema operativo del dispositivo huésped. En particular, la reinicialización del elemento de seguridad integrado comprende el paso automático de este a un estado bloqueado en el que las funcionalidades del elemento de seguridad integrado son reducidas.

Estas disposiciones permiten asegurar al eSE contra el acceso a sus servicios o los datos sensibles que almacena.

Según otra característica particular, el primer mensaje transmitido por el agente de aplicación incluye un valor aleatorio generado por el agente de aplicación, el mensaje cifrado incluye un criptograma correspondiente al valor aleatorio cifrado por el elemento de seguridad integrado con ayuda de al menos una clave del juego de claves asociado al dominio de seguridad raíz, y los mensajes transmitidos a la primera y segunda entidades externas incluyen el valor aleatorio generado y el criptograma correspondiente.

Esta disposición ofrece también un nuevo grado suplementario de seguridad para encontrar al Issuer corriente del eSE, porque permite principalmente autentificar al eSE.

Según otra característica particular, el procedimiento comprende además, a nivel de la segunda entidad externa: autentificar al elemento de seguridad integrado con ayuda del mensaje cifrado y de las claves en posesión; y en caso de fracaso de la autentificación por una pluralidad de mensajes cifrados emitidos por el elemento de seguridad integrado, ejecutar al menos una acción protectora.

Esta disposición tiene principalmente la misión de detectar una eventual denegación del servicio por la utilización de un falso eSE. Una acción protectora puede consistir por ejemplo en añadir dicho elemento de seguridad integrado en una lista negra (blacklist) de eSE a excluir.

Según otra característica particular, el dominio de seguridad comprende una pluralidad de juegos de claves poseídos por una pluralidad respectiva de entidades externas, y el mensaje cifrado resulta de la concatenación de un dato (por ejemplo el valor aleatorio anterior) cifrado por cada uno de los juegos de claves del dominio de seguridad raíz.

Esta configuración permite utilizar una única información de seguridad (mensaje cifrado o criptograma) que permite la identificación de uno o varios co-Issuers o copropietarios del eSE.

En un modo de realización, cuando la verificación es positiva (la segunda entidad externa es correctamente poseedora del juego de claves del ISD), la segunda entidad externa envía, al elemento de seguridad integrado, una orden de modificación de un estado interno del elemento de seguridad integrado, a través de la primera entidad externa y del agente de aplicación. Esta disposición permite actuar de manera segura sobre el eSE mientras tanto el Issuer corriente (la segunda entidad) no dispone de un canal de comunicación propio con el eSE (habiéndose suprimido su Admin o Proxy Agent por una reinicialización por ejemplo).

En particular, la segunda entidad externa obtiene un estatuto de dispositivo huésped, y la orden de modificación de un estado interno al elemento de seguridad integrado es función de dicho estatuto obtenido. Por ejemplo, la orden que pasa el eSE a un estado de fin de vida ("TERMINATED" según GlobalPlatform) se emite cuando el dispositivo huésped está en un estado "robado" o "perdido". Por el contrario, la orden emitida pasa el eSE a un estado

desbloqueado ("SECURED" según GlobalPlatform) cuando el estatuto obtenido para el dispositivo huésped confirma que este último no se ha robado ni perdido.

En un modo de realización, el procedimiento comprende las etapas siguientes:

instalar, en el dispositivo huésped, un segundo agente de aplicación diferente del agente de aplicación integrado, configurándose el segundo agente de aplicación para conectarse a la segunda entidad externa;
suprimir el segundo agente de aplicación del dispositivo huésped por un usuario; y
notificar la supresión del segundo agente de aplicación a la segunda entidad externa por el sistema operativo del dispositivo huésped.

Gracias a esta disposición, el Issuer corriente es informado de la supresión de su agente de aplicación esencial para administrar el eSE y puede por tanto emprender unos procesos idóneos para restablecer una situación funcional, principalmente incitando al usuario a recargar y reinstalar este agente de aplicación. Varios mecanismos tales como se describen más adelante permiten detectar la supresión y de ese modo desencadenar la notificación de la supresión.

Breve descripción de las figuras

Surgirán también otras particularidades y ventajas de la invención en la descripción que sigue, ilustrada por los dibujos adjuntos, en los que:

- La Figura 1 ilustra una arquitectura lógica de un eSE y de un dispositivo huésped que lo integra, de acuerdo con la tecnología GlobalPlatform;
- la Figura 2 ilustra la misma arquitectura lógica cuando los derechos de administración sobre el eSE se han transferido a un nuevo propietario;
- la Figura 3 ilustra la situación de este eSE y del dispositivo huésped de la Figura 2 a continuación de una reinicialización en fábrica de este último;
- la Figura 4 representa, en la forma de diagrama lógico, unas etapas del procedimiento según la invención cuando el dispositivo huésped se reinicializa por un usuario;
- la Figura 4a ilustra los intercambios de mensajes entre los diversos intervinientes implementados en unas etapas de la Figura 4;
- la Figura 5 ilustra una arquitectura lógica del eSE y del dispositivo huésped que lo integra durante la etapa inicial de la Figura 4;
- la Figura 6 ilustra esta misma arquitectura lógica a continuación de una reinicialización en fábrica del dispositivo huésped;
- la Figura 7 ilustra la determinación de la propiedad corriente del eSE y la autenticación del eSE mediante esta, según un primer modo de realización;
- la Figura 8 ilustra la determinación de la propiedad corriente del eSE y la autenticación del eSE mediante esta, según un segundo modo de realización;
- la Figura 9 ilustra la determinación de la propiedad corriente del eSE y la autenticación del eSE mediante esta, según un tercer modo de realización; y
- la Figura 10 ilustra la determinación de la propiedad corriente del eSE y la autenticación del eSE mediante esta, según un cuarto modo de realización.

Descripción detallada de la invención

La Figura 4 representa, en la forma de diagrama lógico, unas etapas del procedimiento según la invención en un modo de realización en el que el dispositivo huésped 100 se reinicializa por un usuario de éste. Esta reinicialización se realiza principalmente con ayuda de una función seleccionada por el usuario en un submenú del dispositivo.

La Figura 5 ilustra una arquitectura lógica de un elemento de seguridad integrado, eSE, 50 y del dispositivo huésped 100 que lo integra, antes de la reinicialización.

El elemento de seguridad integrado eSE es del tipo no conectado, es decir que es esclavo de una o varias aplicaciones residentes del dispositivo huésped 100.

Durante la fabricación del dispositivo huésped 100, el Issuer inicial del eSE (el fabricante del dispositivo huésped por ejemplo) integra el agente de aplicación, Manufacturer Admin/Proxy Agent, en el interior del sistema operativo OS de este dispositivo huésped 100.

El Manufacturer Admin/Proxy Agent es el agente de aplicación que permite a su gestor, en este caso el fabricante, acceder al eSE 50 con un privilegio de administrador. Este acceso requiere principalmente la detención y al usuario de claves de cifrado correspondientes al juego de claves del dominio de seguridad raíz (ISD por Issuer Security Domain) 51 del eSE. El acceso como administrador permite por ejemplo a unos equipos (servidores) de la

infraestructura del fabricante acceder y modificar unos datos sensibles en el interior del eSE, crear unos dominios de seguridad secundarios para unos socios comerciales, etc.

Durante la vida del eSE, se ponen unas aplicaciones a disposición por las plataformas de descarga (almacén) del Issuer y de las entidades externas Entidad 1, Entidad 2 correspondientes a los socios. Se cargan y se instalan así unas aplicaciones App1, App2, App3 en el dispositivo huésped 100 para proporcionar unos servicios al usuario final, con ayuda del eSE (para unos datos/servicios de seguridad) y de los servidores de infraestructura de estas entidades externas.

Las aplicaciones App1, App2, App3 acceden a los servicios y datos sensibles del eSE 50 a través de la API GlobalPlatform.

El propietario o Issuer inicial del eSE 50 (fabricante del dispositivo huésped por ejemplo) cede sus derechos de propiedad y de administración sobre el eSE a una entidad externa (nuevo Issuer) que puede ceder también sus derechos a otra entidad externa, etc. Estas entidades externas pueden ser unos socios comerciales del fabricante. En la figura, solo el propietario/Issuer corriente (el último en haber adquirido los derechos) está representado por la Entidad 3.

Se memorizan unas informaciones relativas a la cesión de estos derechos con el fin de permitir posteriormente, y según la invención, encontrar al Issuer actual del eSE 50. Se conciben diversos modos de realización como se describe a continuación con referencia a las Figuras 7 a 10. Principalmente, cada Issuer que cede sus derechos puede registrar, en una base de datos local, al Issuer siguiente al que ha cedido sus derechos de administrador sobre el eSE (Figura 7). Como variante, puede preverse un servidor central al que cada Issuer que cede sus derechos comunica la identidad del nuevo Issuer al que ha cedido sus derechos de administración sobre el eSE (Figuras 8 y 9). Finalmente, en otra variante, la identidad del Issuer corriente puede memorizarse en un campo de datos dedicado en la memoria del eSE. Este campo se actualiza por tanto en cada transferencia de los derechos de administración, es decir en cada transferencia del juego de claves asociado al ISD 51 (Figura 10).

Para acceder al eSE con su propia infraestructura (sus servidores de administración), la Entidad 3 hace cargar e instalar un Admin/Proxy Agent que le corresponde, Entity3 Admin/Proxy Agent. Este agente de aplicación interactúa, a través de una red de comunicación de tipo red de telefonía móvil, con la infraestructura de la Entidad 3 de la misma manera que el Manufacturer Admin/Proxy Agent con la infraestructura del fabricante.

La Figura 5 corresponde al estado del dispositivo huésped 100 y del eSE 50 durante la etapa inicial 400 de la Figura 4.

En la etapa 405, el usuario desencadena una reinicialización del dispositivo huésped.

Esta reinicialización tiene como efecto borrar el conjunto de los datos y aplicaciones cargadas e instaladas en el dispositivo huésped 100, con la excepción del sistema operativo OS, para reponer al dispositivo huésped 100 al estado que era el suyo a la salida de la fábrica. Se trata de una reinicialización a fábrica. Esta reinicialización comprende por tanto el borrado de las aplicaciones App1, App2, App3 así como del agente de aplicación Entity3 Admin/Proxy Agent.

Como se muestra en la Figura 6, el dispositivo huésped ya no comprende más que el OS en su estado de origen con el Manufacturer Admin/Proxy Agent y la API GlobalPlatform. Las aplicaciones App y los otros Admin/Proxy Agents han sido suprimidos.

En la etapa 410, el OS del dispositivo huésped 100 envía una notificación de reinicialización al eSE 50, en respuesta a la orden de inicialización recibida del usuario. Este envío se efectúa por el Manufacturer Admin/Proxy Agent con destino en el dominio de seguridad raíz 51 del eSE. Los mecanismos ACF internos del eSE autorizan efectivamente siempre al agente de aplicación Manufacturer Admin/Proxy Agent a enviar unos datos/mensajes/notificaciones al ISD 51. Como recordatorio, el ACF verifica que está correctamente asociada una huella (hash) de una aplicación móvil (en este caso el hash del certificado del agente de aplicación) al ISD 51, tal como se registra en una base de datos interna.

Esta notificación desencadena una reinicialización del eSE 50, a saber el borrado de cualquier dato, cualquier aplicación y cualquier dominio de seguridad suplementario SSD que se haya podido cargar, instalar o crear en el eSE. Solo no se borra el dominio de seguridad raíz ISD 51, porque es obligatorio en el eSE 50. El ISD 51 conserva el o los juegos de claves criptográficas corrientes.

Esta etapa 410 contribuye a la seguridad de los datos contenidos en el eSE 50 porque, mediante su borrado, no son ya accesibles a una persona malintencionada.

El final de la supresión de los datos/aplicaciones/SSD en el eSE 50 durante la etapa 410 desencadena el paso automático 415 del eSE 50 a un estado bloqueado en el que las funcionalidades del eSE son reducidas.

La norma GlobalPlatform define principalmente los estados OP_READY, INITIALIZED, SECURED, CARD_LOCKED y TERMINATED como estados posibles para el eSE 50. El estado del eSE consiste en la memorización de una información correspondiente en una memoria no volátil del eSE.

La etapa 415 consiste de ese modo en hacer bascular al eSE 50 del estado corriente (por ejemplo SECURED, o OP_READY o INITIALIZED) hacia el estado CARD_LOCKED. La sección 11 de la "GlobalPlatform Card Specification 2.2.1" muestra principalmente las órdenes APDU que no son ya tratadas en este estado CARD_LOCKED del eSE. El acceso a las aplicaciones/servicios del eSE, excepto los servicios del eSE AUDIT y procesos de desbloqueo del eSE, y de ese modo se bloquea hasta un eventual desbloqueo.

El ISD 51 que tiene por omisión el privilegio Card Lock, efectúa directamente este basculamiento automático con la detección de la reinicialización.

A continuación de la reinicialización, el dispositivo huésped 100 rearrancará (reboot) en la etapa 420.

En un modo de realización, el procedimiento pasa directamente a la etapa 440 descrita a continuación en el curso de la que se transmite un mensaje o notificación que contiene un identificador eSE-ID del eSE 50 a la entidad externa Fabricante inicialmente propietaria del eSE. En este modo de realización, no se trasmiten ningún valor aleatorio ni criptograma ni se utiliza para validar la identidad del Issuer corriente. La entidad externa Fabricante inicialmente propietaria del eSE procederá a la determinación del Issuer corriente con ayuda de las bases de datos como se menciona a continuación en conexión con las Figuras 7 a 10 (sin utilización de criptograma). El Issuer corriente así determinado podrá emprender unas acciones en contra del eSE (envío de órdenes por ejemplo) pasando por la entidad externa Fabricante sin que haya habido validación del Issuer corriente con ayuda del mensaje cifrado o de un valor aleatorio/criptograma como se describe en el modo de realización completo a continuación.

En el modo de realización completo tal como se ilustra por la Figura 4, se prevé, en la secuencia de arranque (boot sequence) del dispositivo huésped 100 para el rearranque, que el agente de aplicación del Fabricante, Manufacturer Admin/Proxy Agent, integrado en el OS genere un valor aleatorio y lo comunique al eSE 50, principalmente al ISD 51, porque los mecanismos ACF lo autorizan.

Este envío del valor aleatorio tiene por tanto lugar con cada rearranque del dispositivo huésped 100, independientemente de saber si ha tenido lugar antes o no una reinicialización de este.

En la etapa 425, el dominio de seguridad raíz ISD 51 recupera el estado corriente del eSE 50 con la ayuda de una orden interna (lectura de información de estado en la memoria no volátil del eSE) y trata el valor aleatorio recibido de manera diferente según el estado recuperado.

Si el eSE 50 no está en el estado CARD_LOCKED, sino en uno de los estados OP_READY, INITIALIZED y SECURED, el ISD 51 devuelve a la etapa 430 un código predefinido para el agente de aplicación Manufacturer Admin/Proxy Agent. La secuencia de arranque puede así proseguirse normalmente.

Si el eSE 50 está en el estado CARD_LOCKED, el ISD 51 calcula un criptograma a partir del valor aleatorio recibido y del juego de claves criptográficas asociado al ISD 51. Posteriormente devuelve el criptograma al agente de aplicación solicitante, el Manufacturer Admin/Proxy Agent, como respuesta al valor aleatorio recibido. Se trata de la etapa 435 en la Figura.

Si existen varios juegos de claves para el ISD 51, el criptograma calculado puede ser resultado de la concatenación de criptogramas elementales, calculado cada uno a partir del valor aleatorio y de uno de los juegos de claves.

Un ejemplo de cálculo de criptograma consiste en cifrar el valor aleatorio con ayuda de una clave del juego de claves, por ejemplo utilizando un mecanismo de cifrado RSA (Rivest Shamir Adleman) o ECC (Elliptic Curve Cryptography).

Como variante, la etapa 420 puede comprender el envío de un simple mensaje/notificación, sin incluir un valor utilizado en lo que sigue para calcular un criptograma. En este caso, la etapa 430 permanece invariable. Por el contrario, la etapa 435 consistirá, para el eSE, en generar un mensaje o dato cifrado, por ejemplo en cifrar un dato predeterminado (igualmente conocido para el Issuer corriente para permitir a este último dirigir unas verificaciones como se describe a continuación).

De devolución en el ejemplo del valor aleatorio, a la recepción de un criptograma, significando por tanto que el eSE está en un estado CARD_LOCKED, el agente de aplicación Manufacturer Admin/Proxy Agent envía en la etapa 440 una notificación de reinicialización a fábrica a la entidad externa Fabricante inicialmente propietaria del eSE. Más precisamente, esta notificación se envía a un servidor de infraestructura del fabricante, indicado como servidor de Fabricante. La notificación incluye principalmente un identificador del eSE 50, por ejemplo el identificador eSE-ID definido por la norma GlobalPlatform y que el agente de aplicación puede recuperar en cualquier momento desde el ISD 51.

La información de dirección de esta infraestructura de Fabricante, por ejemplo una dirección IP, una dirección de e-mail, etc., está explícitamente contenida en el código (codificación dura) del agente de aplicación Manufacturer Admin/Proxy Agent.

En un modo de realización preferido, el valor aleatorio generado y que ha servido de base para el cálculo del criptograma se une en la notificación de reinicialización. Esta disposición permite, como se resaltará en lo que sigue, transmitir separadamente el valor aleatorio del criptograma, y así incrementar la seguridad relativa de los mecanismos implementados por el criptograma (principalmente autenticación).

En un modo de realización alternativo, el valor aleatorio se transmite con el criptograma.

El servidor Fabricante, con la recepción de la notificación, envía (etapa 445) una solicitud al agente de aplicación Manufacturer Admin/Proxy Agent con los fines de recuperar el criptograma correspondiente.

Lo que el agente de aplicación le reenvía en la etapa 450 en respuesta a esta solicitud.

La etapa 455 que sigue tiene por objetivo identificar al Issuer corriente o actual del eSE 50 con certidumbre y transmitirle el valor aleatorio y el criptograma asociado.

Se conciben ahora diferentes modos de realización de esta etapa con referencia a las Figuras 7 a 10.

En el modo de realización de la Figura 7, cada Issuer que cede sus derechos de administración sobre el eSE 50 registra, en una base de datos local BD, al Issuer según al que ha cedido sus derechos. Esta información se memoriza en asociación con el eSE-ID.

Como se ve en la figura, se conserva la cadena de los Issuers (de posesión/propiedad) consecutivos. Es posible así determinar al Issuer corriente trasmitiendo paso a paso el valor aleatorio y el criptograma hasta el Issuer corriente. Este último es el que no ha memorizado al Issuer siguiente en su base de datos para el eSE 50 considerado (eSE-ID). Así cada entidad externa intermedia (Fabricante, Issuer n.º1, Issuer n.º2) que recibe el valor aleatorio y el criptograma los transmiten hacia la entidad externa destinataria registrada, en la BD local, como sucesora de la entidad externa receptora en la cadena de los Issuers.

Prácticamente, cada entidad externa que recibe la notificación de reinicialización (incluyendo el valor aleatorio) y el criptograma (comenzando por el servidor de Fabricante) determina si ha tenido lugar una transferencia de los derechos de administrador (del juego de claves) sobre el eSE 50 consultando su BD local en una entrada correspondiente al eSE-ID. Esta consulta consiste en verificar si el identificador de otra entidad externa está indicado en esta entrada.

En caso afirmativo, la notificación de reinicialización (incluyendo el valor aleatorio) y el criptograma se transmiten (etapa 4555) a la otra entidad externa tal como se indica en la BD local.

En caso negativo, el servidor de la entidad externa corriente trata de descifrar el criptograma con ayuda del juego de claves que posee para el eSE 50 identificado por el eSE-ID de la notificación de reinicialización. Es la etapa 4556.

Si el descifrado 4556 permite encontrar el valor aleatorio, entonces el eSE 50 ha sido correctamente identificado y la entidad externa corriente es correctamente el Issuer corriente que dispone unos derechos de administración sobre el eSE 50. En este caso, el procedimiento pasa a la etapa 460 realizada por el Issuer corriente y que consiste en efectuar unas acciones particulares.

Si el descifrado 4553 revela que es negativo, entonces el procedimiento pasa a la etapa 465 realizada por el Issuer corriente y que consiste por ejemplo en efectuar unas acciones de seguridad.

En un modo de realización la etapa 460 comprende inicialmente una etapa 4601 en el curso de la que el Issuer corriente contacta con el usuario del dispositivo huésped a través de un canal de comunicación seguro (por ejemplo dirección de e-mail, teléfono móvil, teléfono fijo) para informarse de un estatuto del dispositivo, por ejemplo, "perdido", "robado", "vendido", etc.

Posteriormente en función de dicho estatuto obtenido, pueden emprenderse unas acciones diferentes.

De ese modo en la etapa 4602, si el estatuto obtenido es "perdido" o "robado", el Issuer corriente emite, con destino en el eSE 50, una orden de modificación del estado interno del eSE del estado "CARD_LOCKED" al estado de fin de vida "TERMINATED" en el que las funcionalidades e interfaces de comunicación del eSE están destruidas, estando cifrada la orden de modificación con ayuda del juego de claves asociado al ISD 51 por razones de seguridad. En efecto, los mecanismos de seguridad que rodean los elementos de seguridad integrados eSE de GlobalPlatform implican la autenticación y el cifrado del conjunto de las acciones ejecutadas entre un tal servidor externo distante y el ISD.

El estado de fin de vida "TERMINATED" significa el fin del ciclo de vida del eSE y es un estado irreversible.

La orden de modificación puede consistir en una acción destructiva en el interior del eSE, por ejemplo en el borrado de toda la memoria (volátil y no volátil) del eSE o la destrucción de un fusible en la capa de hardware del eSE.

Para comunicar con el eSE, el Issuer corriente transmite la orden cifrada al Issuer inicial que le ha transmitido el criptograma, es decir el Fabricante en el ejemplo. Posteriormente es el servidor del Fabricante el que transmite esta orden al ISD 51 a través del agente de aplicación Manufacturer Admin/Proxy Agent.

Por el contrario, en la etapa 4603, si el estatuto obtenido es "vendido", o como mínimo no es ni "perdido" ni "robado", el Issuer corriente emite igualmente, con destino en el eSE 50, una orden cifrada de modificación del estado interno del eSE para su desbloqueo, principalmente pasando del estado "CARD_LOCKED" al estado desbloqueado "SECURED", lo que permite recuperar el conjunto de las funcionalidades del eSE. Se utiliza el mismo camino de transmisión de esta orden a través del servidor de Fabricante y el agente de aplicación Manufacturer Admin/Proxy Agent.

De manera opcional después de las etapas 4602 y 4603, el Issuer corriente puede informar a las otras entidades externas socias (Entidad 1 y Entidad 2 en el ejemplo) que tenían unas informaciones/datos en el eSE 50 antes de la notificación, unas acciones realizadas y principalmente el desbloqueo o la destrucción del eSE. De este modo, Estas otras entidades externas socias pueden comprometer de nuevo unos procedimientos que se dirigen a recargar unos datos de usuarios en el eSE y el dispositivo huésped en caso de desbloqueo del eSE, o poner al eSE y al dispositivo huésped en una lista negra (blacklist) en caso de destrucción del eSE. Se trata de la etapa 4604 en la Figura. Esta etapa opcional no se implementa en el caso de un dispositivo huésped "vendido".

De este modo, la orden de modificación de estado del eSE, transmitida por el Issuer corriente, puede incluirse en un mensaje que comprende igualmente una información que precisa si deben restaurarse o no unas informaciones/datos en el eSE (si el usuario del eSE ha cambiado a continuación de una venta por ejemplo).

La etapa 460 se determina después de la subetapa 4604.

En un modo de realización, la etapa 465 (fracaso de la autenticación del eSE) comprende el incremento de un contador de fracasos de autenticación del eSE considerado (etapa 4651). Se prevé entonces un contador para cada eSE-ID.

Este contador se compara con un valor de umbral en la etapa 4652 con el fin de detectar eventuales denegaciones de servicio por el uso de un falso eSE. Por ejemplo el valor de umbral se fija en 10.

Si no se ha sobrepasado el valor de umbral, se termina la etapa 465.

Si no, se detecta una denegación de servicio. La etapa 4653 consiste entonces en realizar unas acciones protectoras en respuesta a esta denegación de servicio. Por ejemplo, el eSE puede añadirse a una lista negra (blacklist) difundida ante unas entidades externas con el fin de no tratar ningún mensaje o notificación asociado a este eSE. Posteriormente se termina la etapa 465.

La Figura 4a ilustra los intercambios de mensajes entre los diversos intervinientes implementados en unas etapas de la Figura 4. A observar que estos intercambios mencionan únicamente el desbloqueo del eSE después de la autentificación por el Issuer corriente.

Se remarcará que la etapa 4555 está compuesta de una primera subetapa de transmisión de la notificación de reinicialización (incluyendo el valor aleatorio) al Issuer corriente, posteriormente una segunda subetapa en la que el Issuer corriente solicita el criptograma ante el servidor de Fabricante, y finalmente una tercera subetapa en el curso de la que el criptograma se envía al Issuer corriente. Como se indica más arriba, esta realización permite separar el envío del valor aleatorio y del criptograma, de manera que se incremente la seguridad relativa a la utilización del criptograma (por ejemplo para la autentificación).

La Figura 8 ilustra una variante en la Figura 7. En este modo de realización, se prevé un servidor central al que cada Issuer que cede sus derechos comunica la identidad del nuevo Issuer al que ha cedido sus derechos de administración sobre el eSE. Así el servidor central puede memorizar, en una base BD local, el conjunto de la cadena de los Issuers sucesivos, o como mínimo memorizar el último Issuer, es decir el Issuer corriente.

A observar que cualquier cesión tal como la indicada por un antiguo Issuer al servidor central puede confirmarse por un nuevo Issuer antes de la memorización en la BD.

En este modo de realización, la identificación del Issuer corriente comprende la emisión (etapa 4550') de una solicitud por el servidor de Fabricante al servidor central, con el fin de obtener un identificador del Issuer corriente tal

como se ha memorizado en la BD local en el servidor central. La solicitud se incluye principalmente el identificador eSE-ID del eSE 50.

Como respuesta, el servidor central reenvía (etapa 4551') un identificador o una dirección del Issuer corriente tal como está memorizada la BD local.

Después, el servidor de Fabricante transmite la notificación de reinicialización (incluyendo el valor aleatorio) y el criptograma (etapa 4555 como se ha descrito anteriormente) al Issuer corriente indicado en la respuesta (si es diferente del Fabricante en sí). Se sigue en la etapa 4556 de descifrado del criptograma por el Issuer corriente como se ha descrito anteriormente.

La Figura 9 ilustra otra variante de la Figura 7, que se basa siempre en el servidor central.

En este modo de realización, la identificación del Issuer corriente comprende la transmisión (etapa 4550") de la notificación de reinicialización por el servidor de Fabricante al servidor central.

En la recepción, el servidor central determina (etapa 4551") al Issuer corriente tal como está memorizado en la BD local. Contacta entonces con este Issuer corriente transmitiéndole la notificación de reinicialización tal como se ha recibido acompañada de un identificador o de una dirección del servidor de Fabricante en el origen de la notificación (etapa 4552"), utilizando por ejemplo una dirección del Issuer corriente almacenada en la BD local.

En la etapa 4553", el Issuer corriente se conecta al servidor de Fabricante con el fin de recuperar (etapa 4555 descrita anteriormente) el criptograma y eventualmente el valor aleatorio si no está incluido en la notificación retransmitida. Se sigue en la etapa 4556 de descifrado del criptograma por el Issuer corriente como se ha descrito anteriormente.

En los modos de realización de las Figuras 8 y 9, el servidor de Fabricante puede, antes de solicitarlo al servidor central, determinar si no es él mismo el Issuer corriente. Esta información es fácilmente accesible puesto que consiste en saber si ha informado él mismo al servidor central de una transferencia cualquiera de derechos de administración sobre el eSE considerado. De este modo, se evita la solicitación del servidor central si no ha tenido lugar ninguna transferencia.

La Figura 10 ilustra otra variante de la Figura 7. En este modo de realización, la identidad del Issuer corriente se memoriza en un campo BD de datos dedicado en la memoria del eSE a cada transferencia de los derechos de administración, es decir en cada transferencia del juego de claves asociado al ISD 51. Por ejemplo, el servidor del Issuer que cede sus derechos puede enviar una orden para actualizar este campo con un identificador del nuevo Issuer.

En el origen, este campo incluye un identificador del servidor de Fabricante en el ejemplo tomado anteriormente.

En este modo de realización, el agente de aplicación Manufacturer Admin/Proxy Agent recupera esta información del Issuer corriente solicitándola al ISD 51. Por ejemplo esta recuperación puede tener lugar durante una etapa 437 sucesiva a la etapa 435 descrita anteriormente.

En este caso, la notificación enviada en la etapa 440 incluye igualmente esta información de Issuer corriente.

La etapa 455 consiste entonces en que el servidor de Fabricante que haya recibido esta notificación contacte indirectamente con el Issuer corriente para transmitirle la notificación de reinicialización (incluyendo el valor aleatorio) y el criptograma (etapa 4555 previamente descrita). Se sigue en la etapa 4556 de descifrado del criptograma por el Issuer corriente como se ha descrito anteriormente.

A observar que durante la utilización del dispositivo huésped 100 que integra el eSE 50, el usuario puede suprimir intencionadamente el Admin/Proxy Agent del Issuer corriente. Esta supresión no implica necesariamente riesgos de seguridad sobre el eSE.

Sin embargo, en un modo de realización se prevé que el Issuer corriente esté notificado de esta supresión, o bien por el OS del dispositivo huésped 100, o bien por el Admin/Proxy Agent en curso de supresión. En una variante, el Issuer corriente puede ser informado de esta supresión por una plataforma de descarga (o un servidor) propios de su infraestructura, contactando esta plataforma periódicamente con el Admin/Proxy Agent del eSE para asegurar el buen funcionamiento de este agente de aplicación. De ese modo en ausencia de respuesta, la plataforma es informada de la supresión o de la corrupción del Admin/Proxy Agent.

Con la detección de esta supresión/corrupción, el Issuer corriente puede invitar, mediante mensajes, al usuario final a recargar y reinstalar el Admin/Proxy Agent.

A observar igualmente que cuando varios Issuers conjuntos comparten el ISD 51, puede efectuarse lo que se ha expuesto anteriormente contra un primer Issuer conjunto corriente, antes de pasar a un Issuer conjunto siguiente en caso de fracaso.

Principalmente, todos los Issuers conjuntos tienen los mismos derechos sobre el ISD 51 y pueden desbloquear por tanto o destruir el eSE 50. Así en un modo de realización, cuando se efectúa un desbloqueo o una destrucción con la iniciativa de un Issuer conjunto corriente, son advertidos los otros Issuers conjuntos corrientes. Como variante, el desbloqueo o la destrucción efectiva del eSE no puede ser activada más que cuando el conjunto o una parte alícuota predefinida de los co-Issuers ha enviado la misma orden de modificación de estado del eSE.

Una parte al menos del procedimiento según la invención puede implementarse en forma de software. De este modo, la presente invención puede tomar la forma de elementos enteramente de software (incluyendo un micro-software, un software residente, unos micro-códigos, etc.) o la forma de elementos que combinan unos elementos de software y de hardware.

Los elementos que anteceden no son más que unos modos de realización de la invención que no la limitan.

REIVINDICACIONES

1. Procedimiento de gestión de un elemento de seguridad integrado (50), eSE, en un dispositivo huésped (100), siendo accesible únicamente el elemento de seguridad integrado (50) como esclavo de al menos una aplicación residente (App1, App2, App3) del dispositivo huésped en una relación maestro-esclavo, e incluyendo el elemento de seguridad integrado (50) un dominio de seguridad raíz (51), ISD, al que se asocia un juego de claves para implementar unos mecanismos de seguridad, estando el procedimiento caracterizado por las etapas siguientes:

transmitir (440, 450) un mensaje que incluye un identificador del elemento de seguridad integrado eSE (50), desde un agente de aplicación integrado en un sistema operativo (OS) del dispositivo huésped con destino en una primera entidad externa al dispositivo huésped y registrado en el agente de aplicación;
determinar una segunda entidad externa al dispositivo huésped poseedora del juego de claves asociado al dominio de seguridad raíz (51).

2. Procedimiento según la reivindicación 1, que comprende además:

transmitir (455, 4555) el mensaje recibido desde la primera entidad externa con destino en la segunda entidad externa determinada;
verificar (4556) por dicha segunda entidad externa que esta es la poseedora del juego de claves asociado al dominio de seguridad raíz (51) a partir del mensaje recibido.

3. Procedimiento según la reivindicación 2, en el que transmitir (455) el mensaje hacia la segunda entidad externa se efectúa poco a poco, recibiendo una entidad externa dicho mensaje que lo transmite (4555) hacia una entidad externa destinataria registrada, en una base de datos (BD) local a la entidad externa receptora, como sucesora de la entidad externa receptora en la posesión del juego de claves asociado a dicho dominio de seguridad raíz.

4. Procedimiento según la reivindicación 2, en el que determinar una segunda entidad externa comprende:

emitir (4550'), por la primera entidad externa, una solicitud de un servidor central para obtener un identificador de la segunda entidad externa, la solicitud del identificador del elemento de seguridad integrado (50).

5. Procedimiento según la reivindicación 2, en el que determinar una segunda entidad externa y transmitir (455) el mensaje recibido hacia la segunda entidad externa comprende:

emitir (4550'') una notificación por la primera entidad externa a un servidor central, identificando dicha notificación el elemento de seguridad integrado (50);
a nivel del servidor central, identificar (4551'') localmente la segunda entidad externa a partir del identificador (eSE-ID) del elemento de seguridad integrado (50) indicado en la notificación, y emitir (4552'') una segunda notificación a la segunda entidad externa tal como se identificó localmente;
con iniciativa en la segunda entidad externa tal como se identificó localmente, establecer (4553'') una conexión entre esta segunda entidad externa y la primera entidad externa de manera que se reciba (4555) de esta última dicho mensaje.

6. Procedimiento según la reivindicación 2, en el que el elemento de seguridad integrado (50) comprende, en la memoria, un campo de datos (BD) para memorizar la identificación de una entidad externa poseedora del juego de claves asociado a dicho dominio de seguridad raíz (51), actualizándose dicho campo de datos cuando la entidad externa poseedora del juego de claves cambia, y el agente de aplicación recupera (437) la identificación de entidad externa indicada en el campo de datos del elemento de seguridad integrado (50) y transmite (440) esta identificación a la primera entidad externa de manera que esta última establezca una conexión con la segunda entidad externa con ayuda de esta identificación para transmitirle (4555) dicho mensaje.

7. Procedimiento según una de las reivindicaciones 2 a 6, que comprende las etapas siguientes, en el agente de aplicación integrado en el sistema operativo (OS) del dispositivo huésped:

transmitir (420), al dominio de seguridad raíz ISD (51) del elemento de seguridad integrado eSE (50), un primer mensaje generado por el agente de aplicación;
como respuesta, recibir (435) un mensaje cifrado por al menos una clave del juego de claves asociado al dominio de seguridad raíz (51);

procedimiento en el que los mensajes transmitidos a la primera y segunda entidades externas incluyen el mensaje cifrado, y la verificación por la segunda entidad externa se efectúa a partir del mensaje cifrado recibido y de al menos una clave memorizada en la segunda entidad externa.

8. Procedimiento según la reivindicación 7, que comprende una etapa previa (405) de reinicialización del dispositivo huésped (100), y en la que la etapa de transmisión (420) del primer mensaje al dominio de seguridad raíz (51) por el agente de aplicación se desencadena en el reinicio del dispositivo huésped consecutivamente a la reinicialización.

9. Procedimiento según la reivindicación 8, en el que la reinicialización del dispositivo huésped (100) desencadena una reinicialización del elemento de seguridad integrado (50) mediante el envío (410) de una orden apropiada por el sistema operativo del dispositivo huésped.

10. Procedimiento según la reivindicación 9, en el que la reinicialización del elemento de seguridad integrado (50) comprende el paso (415) automático de este a un estado bloqueado en el que las funcionalidades del elemento de seguridad integrado son reducidas.

11. Procedimiento según una de las reivindicaciones 7 a 10, en el que el primer mensaje transmitido por el agente de aplicación incluye un valor aleatorio generado por el agente de aplicación, el mensaje cifrado incluye un criptograma correspondiente al valor aleatorio cifrado por el elemento de seguridad integrado (50) con ayuda de al menos una clave del juego de claves asociado al dominio de seguridad raíz (51), y los mensajes transmitidos a la primera y segunda entidades externas incluyen el valor aleatorio generado y el criptograma correspondiente.

12. Procedimiento según una de las reivindicaciones 7 a 11, que comprende además, a nivel de la segunda entidad externa: autentificar (4556) al elemento de seguridad integrado con ayuda del mensaje cifrado y de las claves en posesión; y en caso de fracaso de la autentificación por una pluralidad de mensajes cifrados emitidos por el elemento de seguridad integrado, ejecutar (4653) al menos una acción protectora.

13. Procedimiento según una de las reivindicaciones 7 a 12, en el que el dominio de seguridad raíz (51) comprende una pluralidad de juegos de claves poseídos por una pluralidad respectiva de entidades externas, y el mensaje cifrado resulta de la concatenación de un dato cifrado por cada uno de los juegos de claves del dominio de seguridad raíz.

14. Procedimiento según una de las reivindicaciones 2 a 13, en el que, cuando la verificación es positiva, la segunda entidad externa envía (4602, 4603), al elemento de seguridad integrado (50), una orden de modificación de un estado interno del elemento de seguridad integrado, a través de la primera entidad externa y del agente de aplicación.

15. Procedimiento según la reivindicación 14, en el que la segunda entidad externa obtiene (4601) un estatuto de dispositivo huésped (100), y la orden de modificación de un estado interno al elemento de seguridad integrado (50) es función de dicho estatuto obtenido.

16. Procedimiento según una de las reivindicaciones 1 a 15, que comprende las etapas siguientes:

instalar, en el dispositivo huésped, un segundo agente de aplicación diferente del agente de aplicación integrado, configurándose el segundo agente de aplicación para conectarse a la segunda entidad externa;
suprimir el segundo agente de aplicación del dispositivo huésped por un usuario; y
notificar la supresión del segundo agente de aplicación a la segunda entidad externa por el sistema operativo del dispositivo huésped.

17. Sistema de gestión de un elemento de seguridad integrado (50), eSE, en un dispositivo huésped (100), siendo accesible únicamente el elemento de seguridad integrado (50) como esclavo de al menos una aplicación residente (App1, App2, App3) del dispositivo huésped en una relación maestro-esclavo, e incluyendo el elemento de seguridad integrado (50) un dominio de seguridad raíz (51), ISD, al que se asocia un juego de claves para implementar unos mecanismos de seguridad, estando el sistema caracterizado por:

un agente de aplicación integrado en un sistema operativo (OS) del dispositivo huésped y configurado para transmitir un mensaje que incluye un identificador del elemento de seguridad integrado eSE, con destino en una primera entidad externa al dispositivo huésped y registrado en el agente de aplicación; y
la primera entidad externa al dispositivo huésped tal como se registra en el agente de aplicación, y configurado para determinar una segunda entidad externa al dispositivo huésped poseedora del juego de claves asociado al dominio de seguridad raíz.

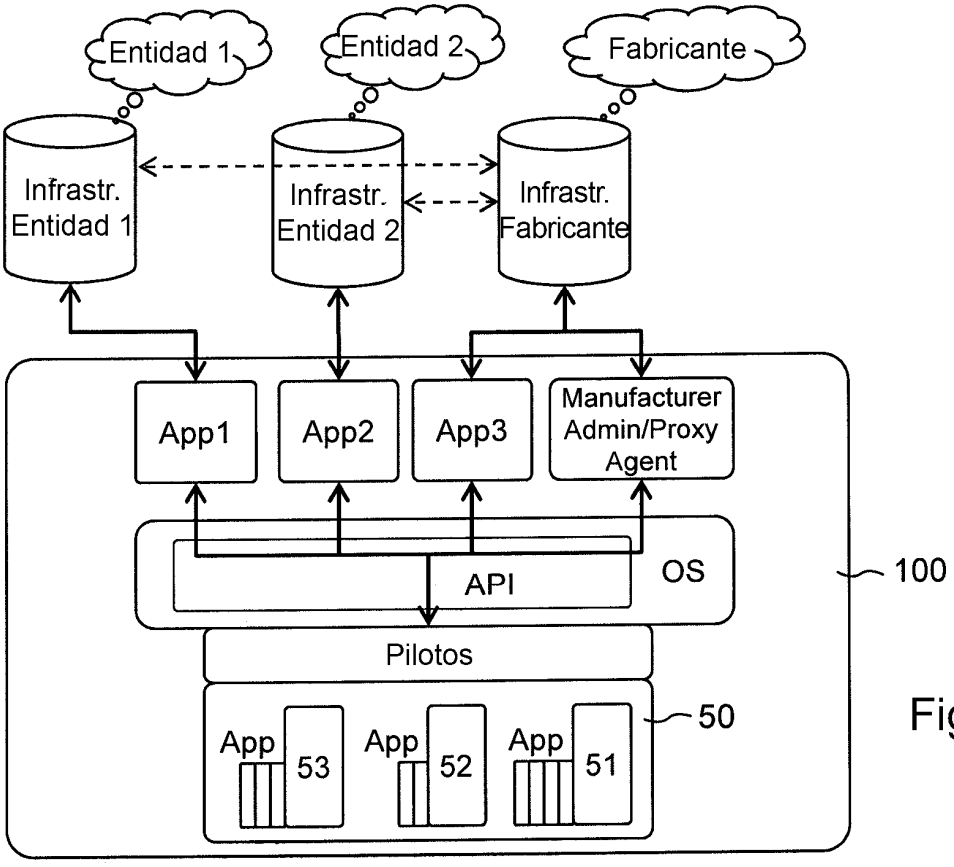


Figura 1

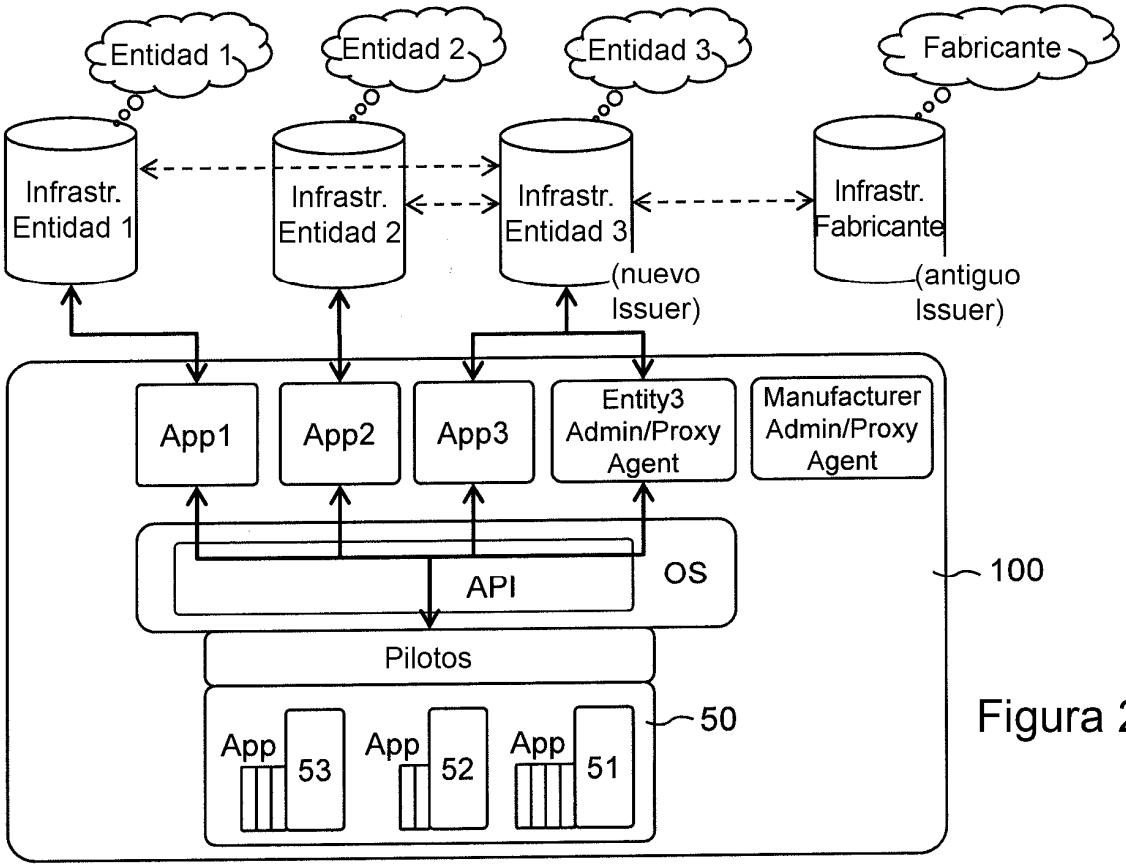


Figura 2

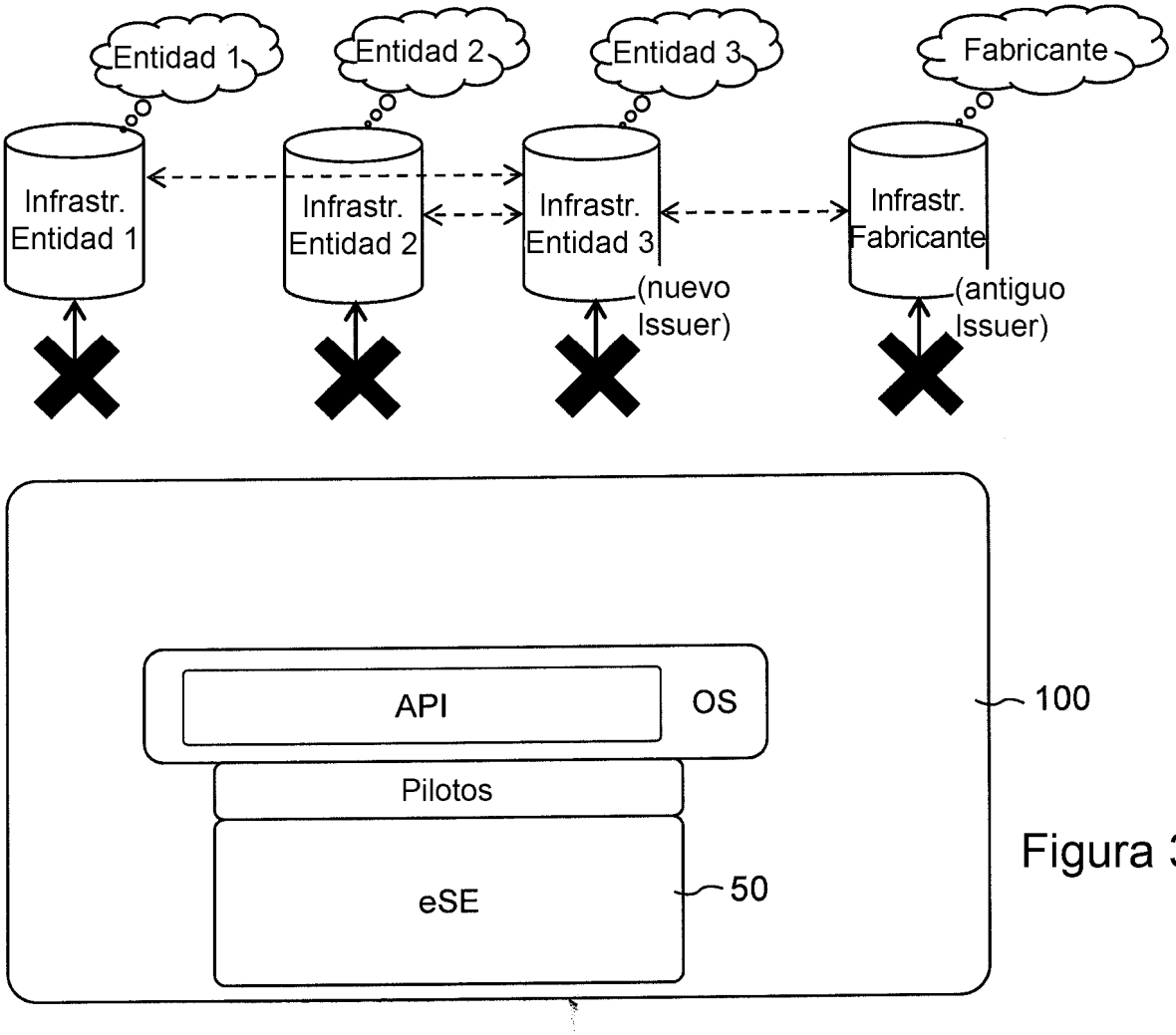

Entidad 1
Entidad 2
Entidad 3
Fabricante
Infrastr. Entidad 1
Infrastr. Entidad 2
Infrastr. Entidad 3
(nuevo Issuer)
Infrastr. Fabricante
(antiguo Issuer)
API
OS
Pilotos
eSE
50
100

Figura 3

Figura 4

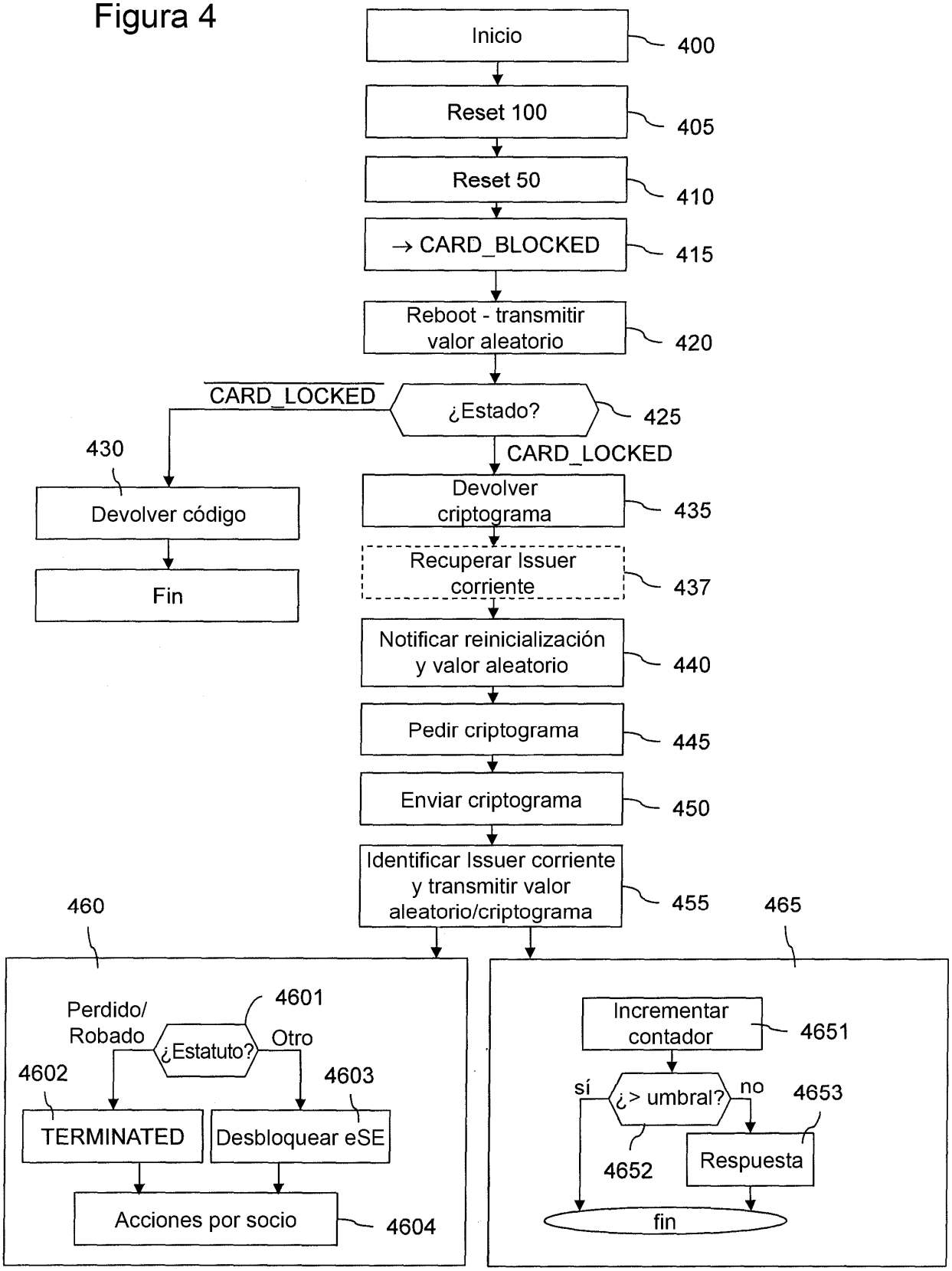
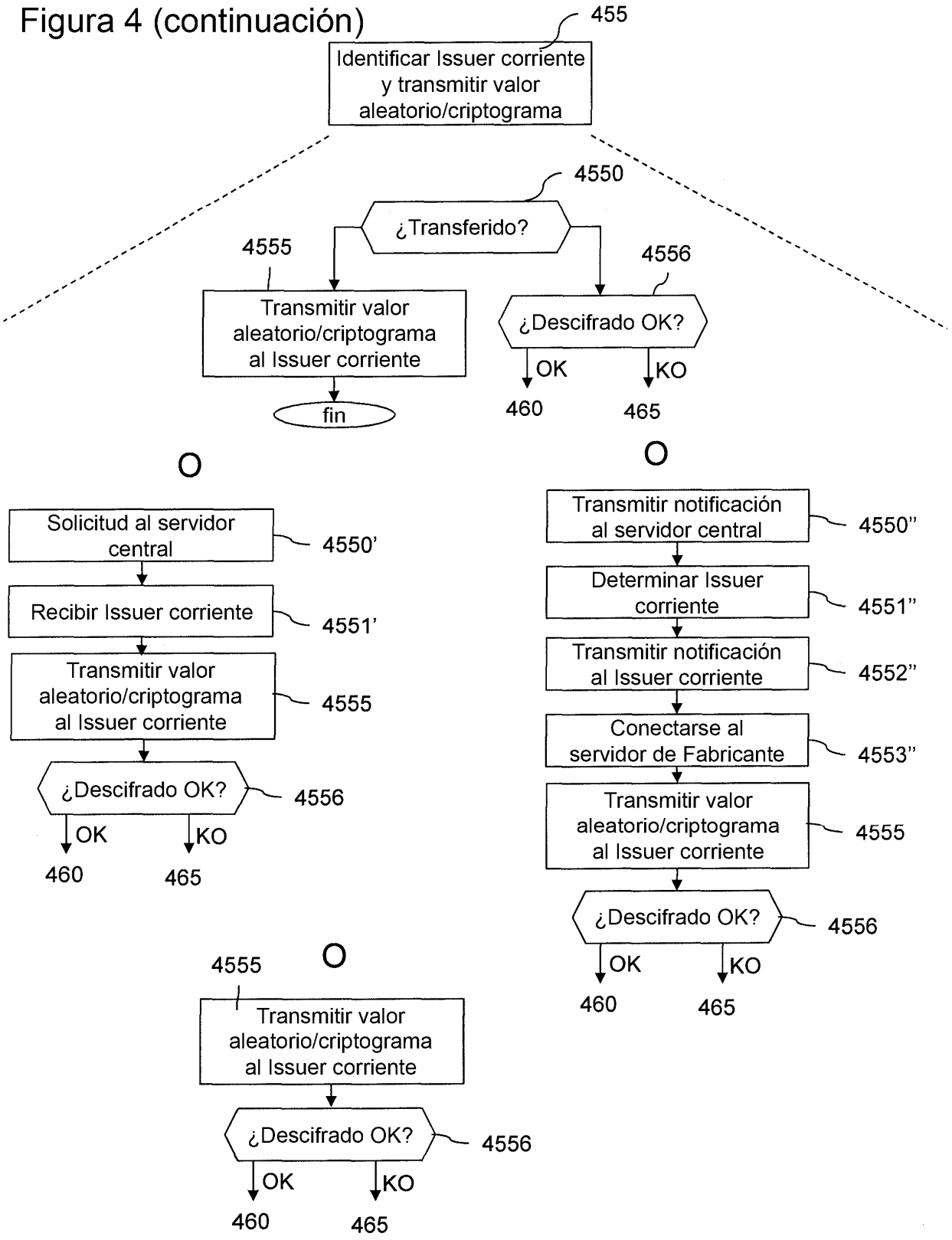

Inicio
400
Reset 100
405
Reset 50
410
→ CARD_BLOCKED
415
Reboot - transmitir valor aleatorio
420
CARD_LOCKED
¿Estado?
425
CARD_LOCKED
430
Devolver código
Fin
Devolver criptograma
435
Recuperar Issuer corriente
437
Notificar reinicialización y valor aleatorio
440
Pedir criptograma
445
Enviar criptograma
450
Identificar Issuer corriente y transmitir valor aleatorio/criptograma
455
460
465
Perdido/ Robado
4601
¿Estatuto?
Otro
4602
4603
TERMINATED
Desbloquear eSE
Acciones por socio
4604
Incrementar contador
4651
sí
¿> umbral?
no
4653
4652
Respuesta
fin

Figura 4 (continuación)



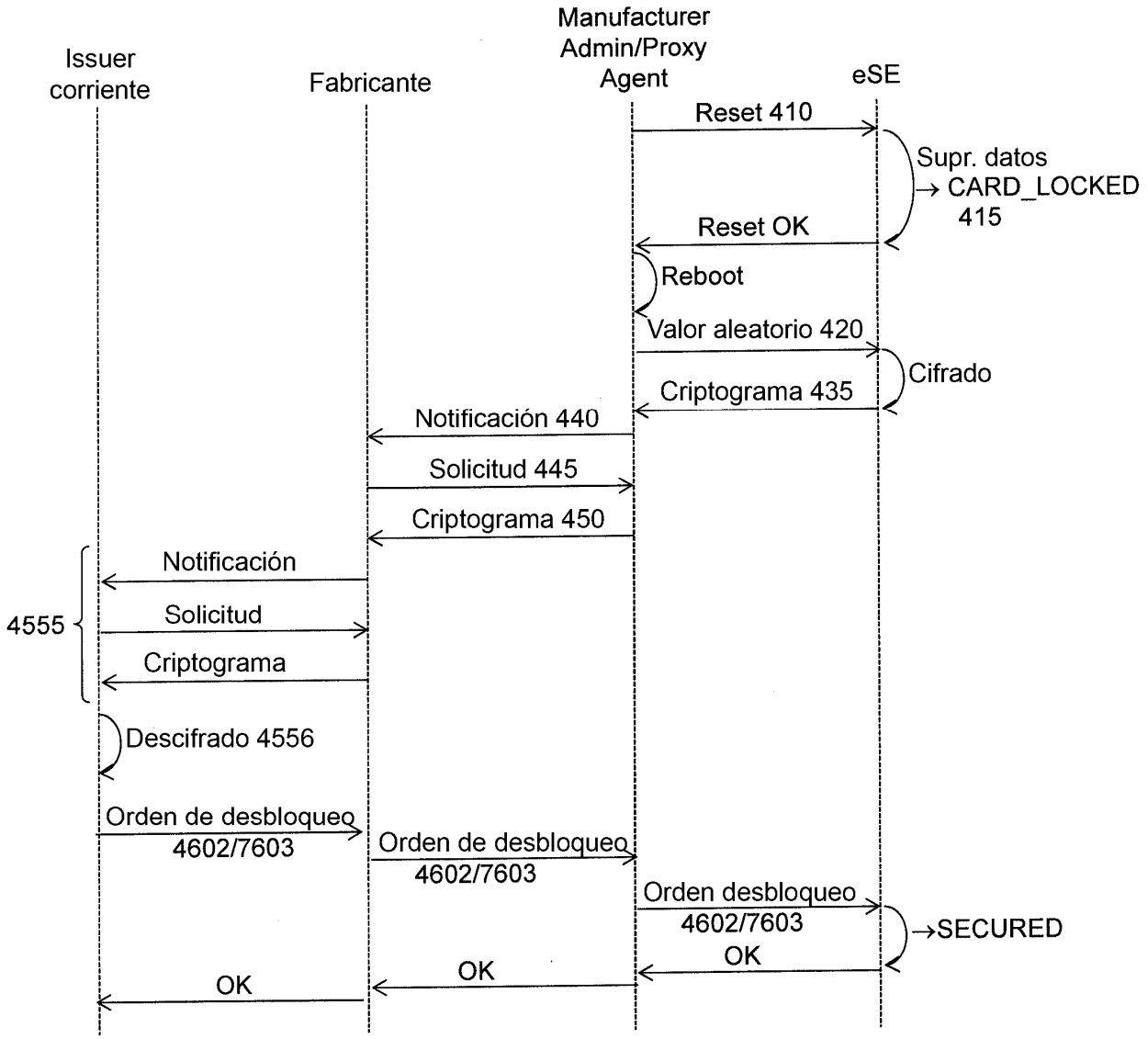

Issuer corriente
Fabricante
Manufacturer Admin/Proxy Agent
eSE
Reset 410
Supr. datos
→ CARD_LOCKED
415
Reset OK
Reboot
Valor aleatorio 420
Cifrado
Criptograma 435
Notificación 440
Solicitud 445
Criptograma 450
Notificación
Solicitud
Criptograma
4555
Descifrado 4556
Orden de desbloqueo
4602/7603
Orden de desbloqueo
4602/7603
Orden desbloqueo
4602/7603
→SECURED
OK
OK
OK

Figura 4a

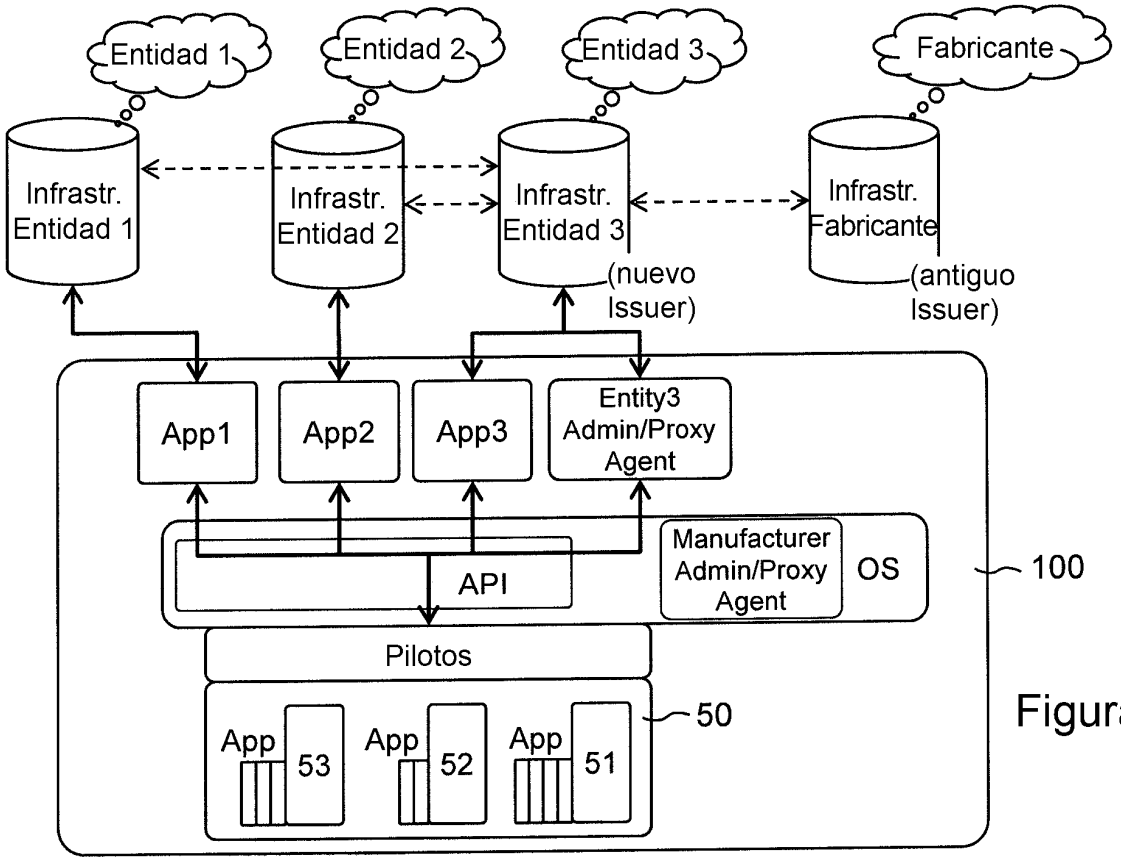


Figura 5

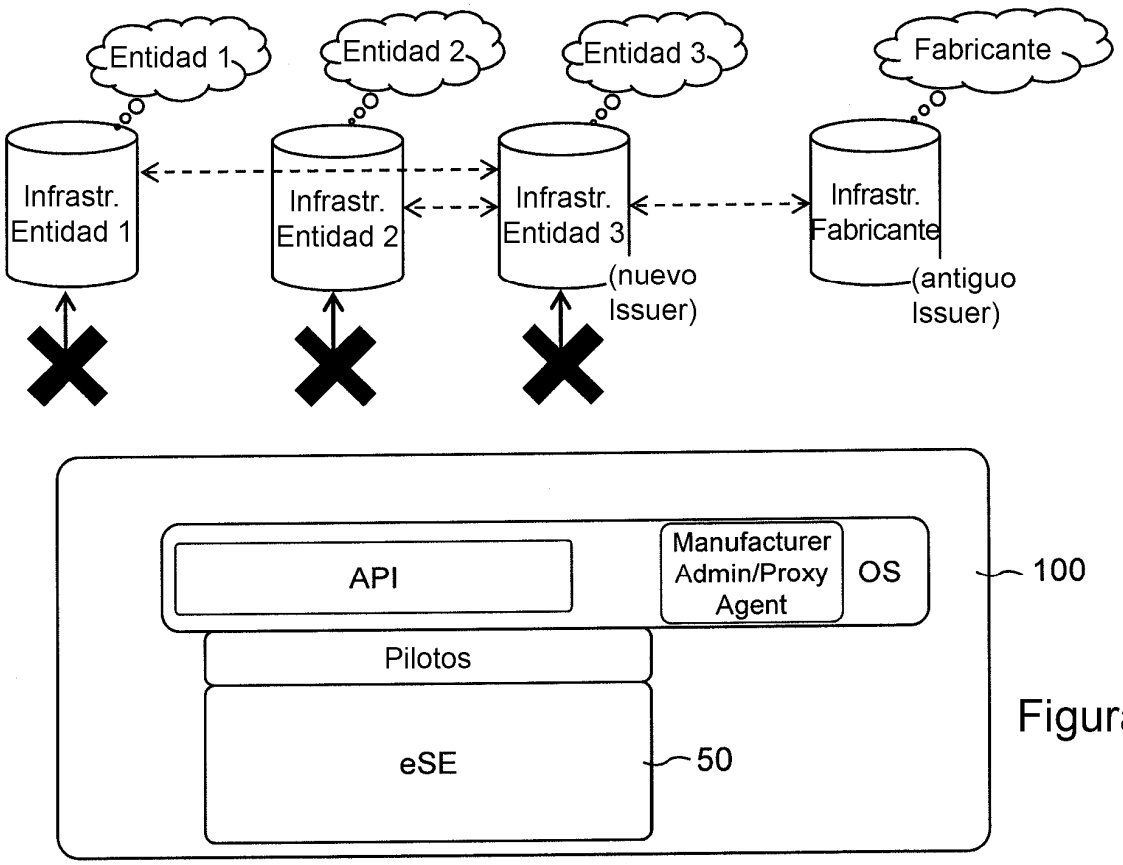


Figura 6

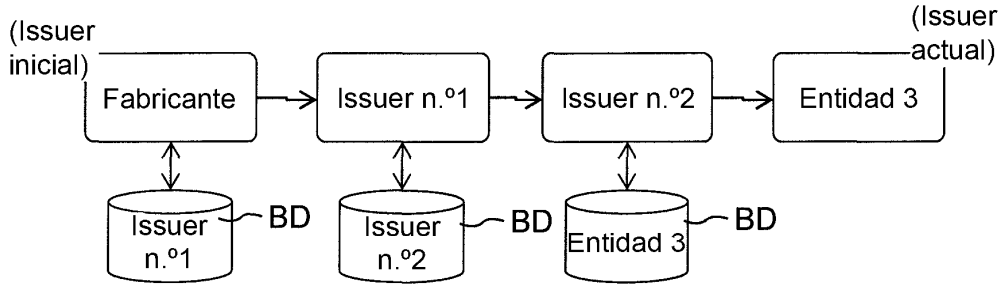


Figura 7

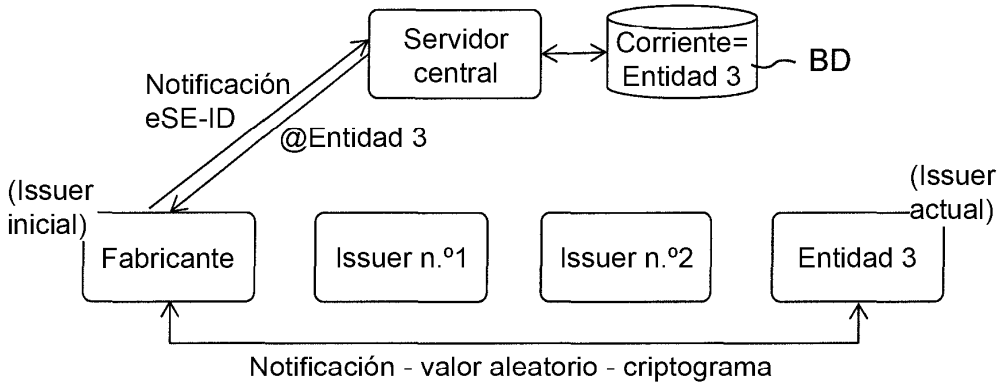


Figura 8

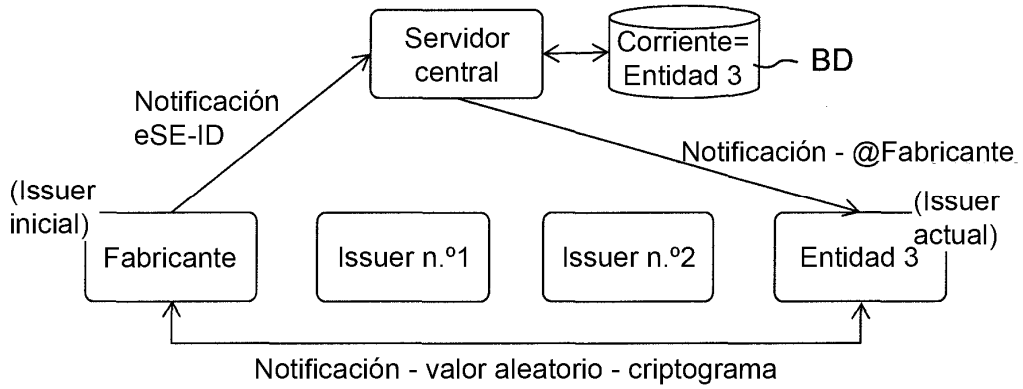


Figura 9

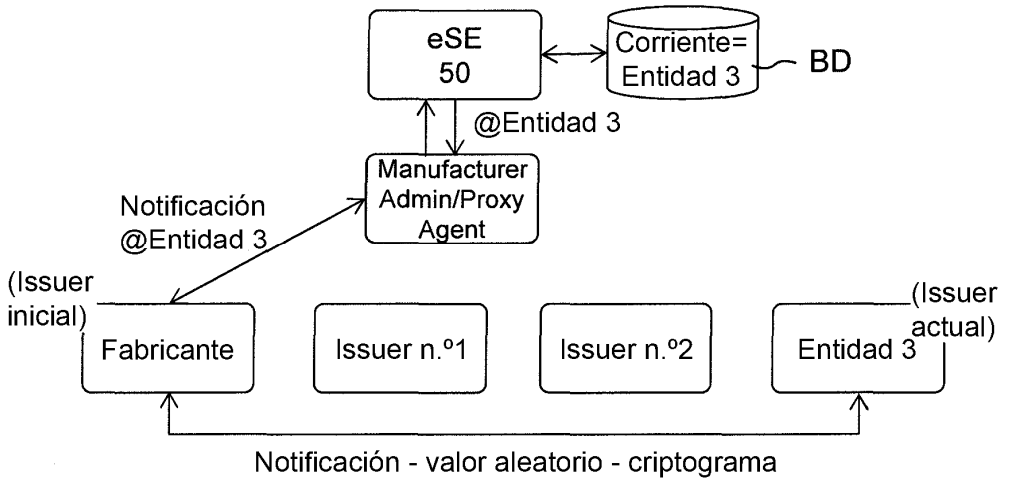


Figura 10