(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 770 039**

(51) Int. CI.:

H04W 4/50 (2008.01)
H04W 4/60 (2008.01)
H04W 4/80 (2008.01)
H04W 4/00 (2008.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.09.2016 PCT/EP2016/071906**

(87) Fecha y número de publicación internacional: **27.04.2017 WO17067722**

(96) Fecha de presentación y número de la solicitud europea: **15.09.2016 E 16769946 (1)**

(97) Fecha y número de publicación de la concesión europea: **30.10.2019 EP 3366049**

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

(30) Prioridad:

19.10.2015 EP 15306669

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.06.2020

(73) Titular/es:

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

(72) Inventor/es:

SAAD, HELMI;
GLEIZE, VALÉRIE y
COURTIADE, FABIEN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para gestionar aplicaciones en un elemento seguro

(Campo de la invención)

La presente invención se refiere a métodos de gestión de aplicaciones en elementos seguros. Se refiere particularmente a métodos relacionados con cómo se lleva a cabo la selección de una aplicación.

(Antecedentes de la invención)

Un elemento seguro es un dispositivo resistente a la manipulación que está destinado a ser alojado en una máquina como un teléfono móvil, un dispositivo conectado o cualquier máquina anfitriona que requiera un cálculo seguro. Un elemento seguro puede ser extraíble como una tarjeta de circuito integrado universal (UICC) o una tarjeta de memoria segura. Un elemento seguro es generalmente un componente basado en hardware. Un elemento seguro puede estar soldado a su máquina anfitriona. Un elemento seguro asociado permanentemente con su dispositivo anfitrión se denomina elemento seguro incorporado. Un elemento seguro puede contener una aplicación destinada a ser llamada por la máquina anfitriona conectada o por una máquina distante. Un elemento seguro puede contener medios informáticos (como servicios criptográficos) o un medio de almacenamiento seguro destinado a ser utilizado por la máquina anfitriona conectada.

Un elemento seguro puede comprender varias aplicaciones. Para simplificar el acceso a las aplicaciones, se ha definido el principio de selección implícita. Cuando una aplicación se selecciona implícitamente en una interfaz de comunicación, un dispositivo externo puede enviar comandos directamente a la aplicación, sin seleccionar explícitamente la aplicación de destino. Por ejemplo, muchos lectores sin contacto desplegados en el dominio de transporte suponen que la aplicación pertinente ya está activa y seleccionada al iniciar una transacción con una aplicación incorporada en un elemento seguro.

Las especificaciones de la tarjeta GlobalPlatform v2.2 definen el "parámetro de selección implícita" (etiqueta 'CF' definida en §11.1.7) que permite declarar una aplicación como seleccionada implícitamente para una interfaz sin contacto. Sin embargo, el estándar GP 2.2 - Enmienda C v1.1.1 especifica que solo se puede instalar una aplicación con el "parámetro de selección implícita" para una interfaz de comunicación.

Puede suceder que un usuario necesite tener varias aplicaciones del mismo tipo en un elemento seguro. Por ejemplo, cuando el usuario viaja de la ciudad A a la ciudad B, debe desinstalar/cancelar manualmente la aplicación de transporte actual correspondiente a la Ciudad A antes de instalar la aplicación de transporte pertinente para acceder a la red de transporte urbano de la Ciudad B con ajustes de selección implícitos. Tales operaciones de desinstalación/instalación son largas y pueden ser complejas. No son prácticas para un usuario.

Existe la necesidad de facilitar la gestión de aplicaciones para aplicaciones que necesitan ser seleccionadas e instaladas implícitamente.

El documento US 2014/0188713 A1 describe un método para ejecutar una transacción NFC.

(Compendio de la invención)

Un objeto de la invención es resolver el problema técnico mencionado anteriormente. La invención está definida por las reivindicaciones 1 y 5.

Un objeto de la presente invención es un elemento seguro que comprende un sistema operativo y una interfaz de comunicación. El sistema operativo está configurado para gestionar una pluralidad de aplicaciones que están presentes e instaladas simultáneamente en el elemento seguro y que están configuradas individualmente para ser seleccionadas implícitamente en la interfaz de comunicación.

Ventajosamente, cada una de dichas aplicaciones puede activarse individualmente y el sistema operativo puede configurarse para denegar una solicitud de activación de una de dichas aplicaciones si otra de dichas aplicaciones ya está activada.

Ventajosamente, el sistema operativo puede ser capaz de manejar un comando que solicita tanto la instalación de una nueva aplicación configurada para ser seleccionada implícitamente en dicha interfaz de comunicación como la activación de dicha nueva aplicación. El sistema operativo puede estar adaptado para instalar dicha nueva aplicación, para configurar dicha nueva aplicación de modo que se seleccione implícitamente en dicha interfaz de comunicación y para negar la activación de dicha nueva aplicación si una aplicación de dicha pluralidad de aplicaciones ya está activada.

Ventajosamente, el sistema operativo puede estar adaptado para enviar, en respuesta a dicho comando, un código de advertencia que refleje el cumplimiento parcial de dicho comando cuando la nueva aplicación se haya instalado sin activación.

Ventajosamente, dicha interfaz de comunicación puede estar dedicada a la comunicación dirigida a un dispositivo sin contacto.

Otro objeto de la presente invención es un método para gestionar aplicaciones en un elemento seguro que comprende una interfaz de comunicación. Se instala una primera aplicación en el elemento seguro y se configura para ser seleccionada implícitamente en dicha interfaz de comunicación. El método comprende las etapas:

- el elemento seguro recibe un primer comando que solicita la instalación de una segunda aplicación configurada para ser seleccionada implícitamente en la dicha interfaz de comunicación,

- al recibir dicho primer comando, el elemento seguro instala dicha segunda aplicación, configura dicha segunda aplicación para que sea seleccionada implícitamente en dicha interfaz de comunicación y mantiene dicha primera aplicación sin cambios.

Ventajosamente, dichas primera y segunda aplicaciones pueden activarse individualmente y dicho método puede comprender la etapa adicional:

- el elemento seguro rechaza una solicitud de activación de una de dichas aplicaciones si otra de dichas aplicaciones ya está activada.

Ventajosamente, dicho método puede comprender las etapas adicionales:

- el elemento seguro recibe un segundo comando que solicita tanto la instalación de una tercera aplicación configurada para ser seleccionada implícitamente en dicha interfaz de comunicación como la activación de dicha tercera aplicación, y

- al recibir dicho segundo comando, el elemento seguro instala dicha tercera aplicación, configura dicha tercera aplicación para que sea seleccionada implícitamente en dicha interfaz de comunicación y deniega la activación de dicha tercera aplicación si una aplicación configurada para ser seleccionada implícitamente en dicha interfaz de comunicación ya está activada.

(Breve descripción de los dibujos)

Otras características y ventajas de la presente invención surgirán más claramente de una lectura de la siguiente descripción de una serie de realizaciones preferidas de la invención con referencia al dibujo adjunto correspondiente en el que:

- La Figura 1 representa un sistema que comprende un elemento seguro según la invención.

(Descripción detallada de las realizaciones preferidas)

La invención puede aplicarse a cualquier tipo de elemento seguro. En particular, la invención se aplica a elementos seguros extraíbles y elementos seguros soldados a dispositivos anfitriones. La invención se aplica a elementos seguros configurados para ser accesibles a través de un canal NFC (Near Field Communication - comunicación de campo cercano). La invención es adecuada para aplicaciones en el dominio de tránsito.

La Figura 1 ilustra la arquitectura de un elemento seguro según la invención.

El dispositivo anfitrión 11 es un dispositivo habilitado para NFC (como un teléfono móvil o un dispositivo portátil, por ejemplo) que comprende un controlador NFC (denominado CLF) capaz de establecer una conexión NFC (mostrada como una línea de puntos) con el dispositivo externo 80. El dispositivo externo 80 puede ser un lector NFC. El dispositivo anfitrión 11 también comprende un componente de comunicación 81 capaz de establecer una sesión OTA (Over-the-air - durante la comunicación) o HTTPS con una máquina remota, como un MNO (Mobile Network Operator - operador de red móvil) TSM (Trusted Service Manager - gestor de servicios de confianza) o SEI (Secure Element Issuer - expedidor de elemento seguro) TSM.

Alternativamente, el controlador NFC puede reemplazarse con un encaminador RF.

El elemento seguro 10 está incorporado en el dispositivo anfitrión 11. El elemento seguro 10 incluye varias interfaces de comunicación. La primera interfaz de comunicación 20 está conectada al controlador NFC (o al encaminador RF) a través de un solo cable y puede intercambiar datos con el CLF a través del protocolo SWP (Single Wire Protocol - protocolo de un solo cable) según lo definido por ETSI TS 102 613 Versión 7 y Superior. La interfaz de comunicación 20 puede considerarse como dedicada a la comunicación dirigida a un dispositivo sin contacto porque está vinculada al controlador NFC. La segunda interfaz de comunicación 21 está conectada al componente de comunicación 81. El elemento seguro 10 está configurado para intercambiar datos con el componente de comunicación 81 utilizando SPI (Serial Peripheral interface - interfaz periférica en serie) a través de la interfaz de comunicación 21. En otro ejemplo, el elemento seguro 10 puede estar configurado para comunicarse según las especificaciones ISO7816 a través de la interfaz de comunicación 21.

En otro ejemplo, el elemento seguro 10 puede tener una interfaz de comunicación única.

El elemento seguro 10 comprende un sistema operativo 30. Dos aplicaciones de transporte 40 y 50 están instaladas en el elemento seguro 10. El sistema operativo 30 está diseñado para permitir la instalación de varias aplicaciones que son seleccionadas implícitamente en la misma interfaz de comunicación. Por ejemplo, las aplicaciones 40 y 50 están configuradas individualmente para ser seleccionadas implícitamente en la primera interfaz de comunicación 20.

Estas aplicaciones 40 y 50 se pueden activar individualmente. Cuando está activada, una aplicación puede recibir un comando, tratar el comando y generar una respuesta. Cuando está deshabilitada (es decir, no activada), una aplicación no se puede activar ni tratar ningún comando.

El sistema operativo 30 está diseñado para permitir la activación de aplicaciones. Más específicamente, el sistema operativo 30 está configurado para denegar una solicitud de activación de una aplicación que fue seleccionada implícitamente en una interfaz de comunicación dada si ya está activada otra aplicación que fue seleccionada implícitamente en la misma interfaz de comunicación.

Por ejemplo, si la aplicación 40 ya está activada, una solicitud para activar la aplicación 50 es rechazada por el sistema operativo 30. Es necesario deshabilitar la aplicación 40 antes de activar con éxito la aplicación 50.

En otro ejemplo, si no hay ninguna aplicación ya activada, una solicitud para activar la aplicación 50 es realizada con éxito por el sistema operativo 30. Por ejemplo, la etiqueta "CF" asignada a la aplicación 50 se tiene en cuenta en la secuencia de instalación/activación asociada en consecuencia.

Cabe señalar que la activación de la aplicación se puede solicitar a través del CRS (Contactless Registry Service - servicio de registro sin contacto) según lo definido por GlobalPlatform Enmienda C v1.1.1.

Como se muestra (en línea discontinua) en la Figura 1, el sistema operativo 30 puede manejar un comando 61 que solicita tanto la instalación de una nueva aplicación 60 configurada para ser seleccionada implícitamente en la interfaz de comunicación especificada como la activación de esta nueva aplicación 60. El sistema operativo 30 está adaptado para instalar la aplicación 60 y configurar la aplicación 60 para que sea seleccionada implícitamente en la interfaz de comunicación de destino. El sistema operativo 30 también está configurado para denegar la activación de la aplicación 60 si otra aplicación está seleccionada implícitamente en la misma interfaz de comunicación y ya está activada.

Por ejemplo, supongamos que la aplicación 40 ya está activada y que el comando 61 solicita tanto la instalación de la aplicación 60 con ajustes que especifican la selección implícita en la interfaz de comunicación 20 como la activación de la aplicación 60. El sistema operativo 30 instalará la aplicación 60 y deniega la activación de la aplicación 60. En este caso, el sistema operativo 30 está configurado para enviar un código de advertencia 62 en respuesta al comando 61. Este código de advertencia 62 refleja el cumplimiento parcial del comando 61. Por ejemplo, el código de advertencia 62 puede contener el valor 0x6200.

La invención proporciona una forma de gestionar posibles conflictos debido al hecho de que solo una aplicación, que es seleccionada implícitamente en una interfaz dada, puede activarse a la vez.

Cabe señalar que dos aplicaciones pueden estar activas simultáneamente en la misma interfaz: una aplicación con el parámetro seleccionado por defecto y la otra sin el parámetro seleccionado por defecto.

Ventajosamente, el elemento seguro puede comprender una aplicación representante (no dibujada) que es el único punto de entrada asociado con una interfaz de comunicación. En este caso, la aplicación representante se encarga de reenviar los comandos entrantes a la aplicación de destino. En este caso, las aplicaciones accesibles a través de la aplicación representante se gestionan según la invención.

El caso de la aplicación Cabecera/Miembro se gestionará como se define en las especificaciones de GlobalPlatform frente al mecanismo de activación y desactivación. Por lo tanto, la aplicación Cabecera/Miembro, como se define en las especificaciones de GlobalPlatform, se tiene en cuenta en lo que se refiere a la etiqueta Multi CF.

Gracias a la invención, un usuario solo tiene que desactivar la aplicación seleccionada por defecto actualmente y activar la pertinente para acceder al servicio necesario. Esta activación/desactivación se puede realizar a través del CRS convencional (Contactless Registry Service - servicio de registro sin contacto) y CREL (Contactless Registry Event Listener - oyente de eventos de registro sin contacto) que se definen en las especificaciones de GlobalPlatform. Ya no es necesario desinstalar/reinstalar la aplicación.

Gracias a la invención, se pueden instalar varias aplicaciones en un elemento seguro con la selección implícita en la misma interfaz de comunicación. No se solicita ningún cambio en las flotas desplegadas de lectores sin contacto.

Debe entenderse, dentro del alcance de la invención, que las realizaciones descritas anteriormente se proporcionan como ejemplos no limitativos. En particular, la aplicación puede aplicarse a cualquier dominio como pago, lealtad, identidad o acceso al servicio. Puede aplicarse a aplicaciones correspondientes a varios países, varios mercados o varios modelos de negocio. El elemento seguro puede contener cualquier cantidad de aplicaciones instaladas.

La invención no se limita a la interfaz de comunicación NFC y puede aplicarse a cualquier interfaz de comunicación RF posible.

El dispositivo anfitrión puede ser cualquier dispositivo capaz de incorporar un elemento seguro. Por ejemplo, el dispositivo anfitrión puede ser una tableta, un automóvil, un ordenador portátil, un reloj inteligente, un dispositivo portátil o un ordenador.

REIVINDICACIONES

1. Un elemento seguro (10) que comprende un sistema operativo (30) y una interfaz de comunicación (20), en donde el sistema operativo (30) está adaptado para gestionar una pluralidad de aplicaciones (40, 50) que están presentes e instaladas simultáneamente en el elemento seguro (10) y que están configurados individualmente para ser seleccionados implícitamente en dicha interfaz de comunicación (20), en donde cada una de dichas aplicaciones (40, 50) puede ser activada individualmente, el elemento seguro **caracterizado por que** el sistema operativo (30) está adaptado para denegar una solicitud de activación de una de dichas aplicaciones (40, 50) si otra de dichas aplicaciones (40, 50) ya está activada y realizar la activación si ninguna de dichas aplicaciones (40, 50) ya está activada, por que el sistema operativo (30) puede manejar un comando (61) que solicita tanto la instalación de una nueva aplicación (60) configurada para ser seleccionada implícitamente en dicha interfaz de comunicación (20) como la activación de dicha nueva aplicación (60), y por que el sistema operativo (30) está adaptado para instalar dicha nueva aplicación (60), para configurar dicha nueva aplicación (60) de modo que sea seleccionada implícitamente en dicha interfaz de comunicación (20) y para denegar la activación de dicha nueva aplicación (60) si una aplicación de dicha pluralidad de aplicaciones (40, 50) ya está activada y realizar dicha activación si ninguna de dicha pluralidad de aplicaciones (40, 50) ya está activada.

2. Un elemento seguro (10) según la reivindicación 1, en donde el sistema operativo (30) está adaptado para enviar, en respuesta a dicho comando (61), un código de advertencia (62) que refleja el cumplimiento parcial de dicho comando (61) cuando la nueva aplicación (60) ha sido instalada sin activación.

3. Un elemento seguro (10) según la reivindicación 1, en donde dicha interfaz de comunicación (20) está dedicada a comunicación dirigida a un dispositivo sin contacto (80).

4. Un elemento seguro (10) según la reivindicación 1, en donde dicha solicitud de activación se realiza a través de un servicio de registro sin contacto como se define en GlobalPlatform Enmienda C v1.1.1.

5. Un método para gestionar aplicaciones en un elemento seguro (10) que comprende un sistema operativo (30) y una interfaz de comunicación (20), en donde el sistema operativo (30) está adaptado para gestionar una pluralidad de aplicaciones (40, 50) que están presentes e instaladas simultáneamente en el elemento seguro (10) y que están configuradas individualmente para ser seleccionadas implícitamente en dicha interfaz de comunicación (20), en donde cada una de dichas aplicaciones (40, 50) puede ser activada individualmente, **caracterizado por que** dicho método comprende las etapas:

- el sistema operativo (30) recibe un comando (61) que solicita tanto la instalación de una nueva aplicación (60) configurada para ser seleccionada implícitamente en dicha interfaz de comunicación (20) como la activación de dicha nueva aplicación (60),

- el sistema operativo (30) instala dicha nueva aplicación (60), configura dicha nueva aplicación (60) para que sea seleccionada implícitamente en dicha interfaz de comunicación (20) y deniega la activación de dicha nueva aplicación (60) si una aplicación de dicha pluralidad de aplicaciones (40, 50) ya está activada y realiza la activación si ninguna de dicha pluralidad de aplicaciones (40, 50) ya está activada.

6. Un método según la reivindicación 5, en donde dicho método comprende la etapa adicional:

- el elemento seguro (10) rechaza una solicitud de activación de una de dichas aplicaciones (40, 50, 60) si otra de dichas aplicaciones (40, 50, 60) ya está activada y realiza la activación si ninguna de dichas aplicaciones (40, 50, 60) ya está activada.

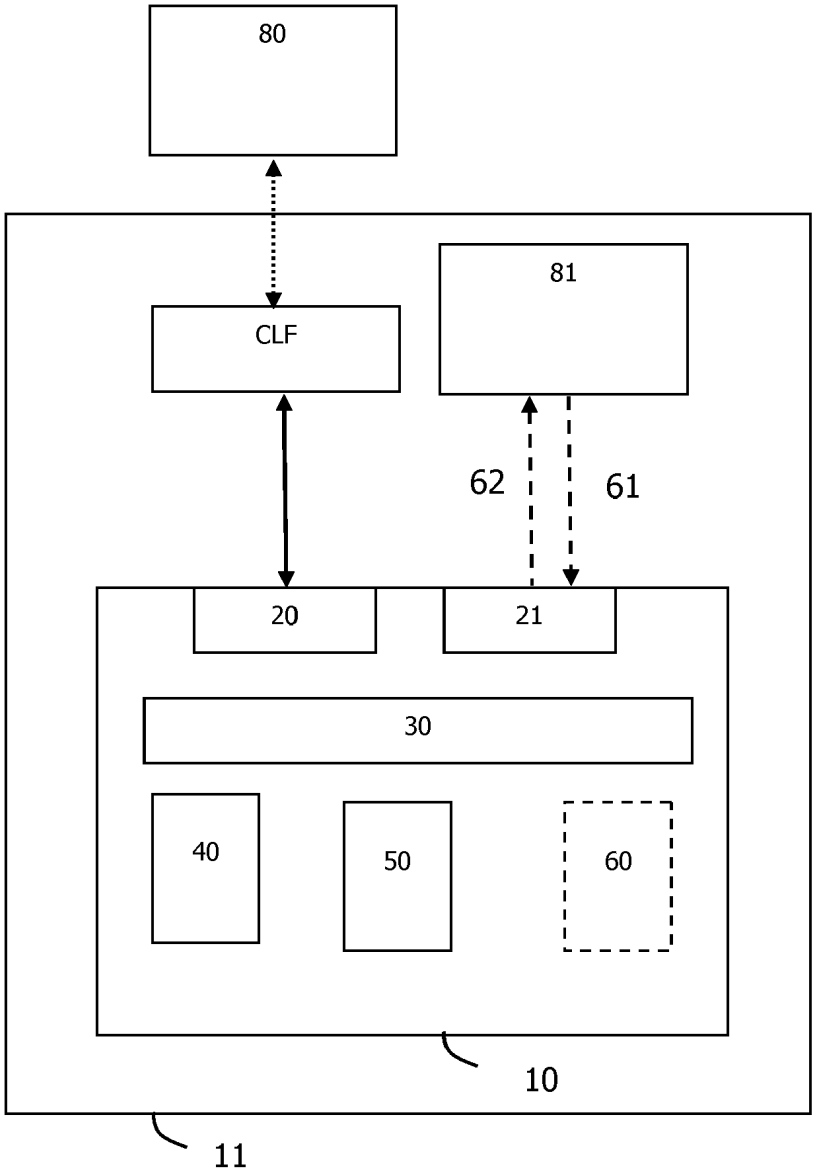

FIG. 1