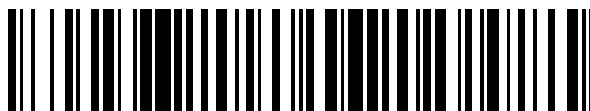


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 638 432**

51 Int. Cl.:

G06F 21/50 (2013.01)

G06F 21/52 (2013.01)

G06F 21/53 (2013.01)

G06F 21/62 (2013.01)

H04M 1/725 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **31.01.2007 PCT/FI2007/050052**

87 Fecha y número de publicación internacional: **18.07.2017 WO08092985**

96 Fecha de presentación y número de la solicitud europea: **31.01.2007 E 07704822 (1)**

97 Fecha y número de publicación de la concesión europea: **19.07.2017 EP 2111597**

54 Título: **Gestión de aplicaciones relacionadas con módulos seguros**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
20.10.2017

73 Titular/es:
NOKIA TECHNOLOGIES OY (100.0%)
KEILALAHDENTIE 4
02150 ESPOO, FI

72 Inventor/es:
SAARISALO, MIKKO

74 Agente/Representante:
VALLEJO LÓPEZ, Juan Pedro

ES 2 638 432 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Gestión de aplicaciones relacionadas con módulos seguros

5 **Campo de la invención**

La presente invención se refiere a la gestión de módulos seguros y aplicaciones de contrapartida de módulos seguros. Más particularmente, pero no exclusivamente, la presente invención se refiere al manejo de aplicaciones de contrapartida que están dedicadas a implementar una determinada función, tal como una interfaz de usuario, para aplicaciones de módulo seguro almacenadas dentro de un elemento o módulo seguro.

Antecedentes de la invención

Tradicionalmente, las aplicaciones de pago y/o venta de entradas residen en un chip seguro incrustado en una tarjeta inteligente de plástico de tamaño de tarjeta de crédito.

Más recientemente, cuando el pago/venta de entradas sin contacto se han vuelto más comunes, se ha comenzado a instalar chips seguros que contienen instrumentos de pago y/o billetes de transporte público en dispositivos móviles, como teléfonos móviles. En una realización a modo de ejemplo, un dispositivo móvil comprende un módulo de tarjeta inteligente y un módulo de comunicación de campo cercano. El módulo de tarjeta inteligente puede ser un módulo seguro que contiene la aplicación de módulo seguro requerida, por ejemplo, la aplicación de pago/venta de entradas. La aplicación de módulo seguro puede ser iniciada por un usuario o basada automáticamente en el contexto y/o la ubicación del dispositivo móvil. Por ejemplo, cuando el dispositivo móvil entra dentro del área de un terminal de punto de ventas, la aplicación de módulo seguro puede iniciarse automáticamente. El módulo de comunicación de campo cercano se activará y posteriormente se podrá realizar una transacción de pago sin contacto.

El término comunicación de campo cercano en este contexto abarca varias técnicas y tecnologías de corto alcance que permiten la comunicación inalámbrica entre dispositivos cuando se tocan juntos o se acercan unos a otros. Por consiguiente, el término comunicación de campo cercano cubre, entre otras cosas, varias tecnologías de conectividad sin contacto cercano al contacto que implican acoplamiento electromagnético y/o electrostático. El término cubre la tecnología RFID (identificación de radio frecuencia), así como la tecnología específica NFC (comunicación de campo cercano) especificada por los siguientes organismos de normalización: NFC Forum, Organización Internacional de Normas (ISO) y ECMA International.

Ahora que los módulos seguros que contienen aplicaciones de módulos seguros se instalan en dispositivos electrónicos, como por ejemplo teléfonos móviles, esto permite una característica conveniente, a saber, la posibilidad de habilitar una interfaz de usuario para proporcionar al usuario del teléfono medios para observar y controlar diversas aplicaciones almacenadas en el módulo seguro. La interfaz de usuario del dispositivo móvil puede utilizarse como una interfaz de usuario para el módulo seguro. Normalmente, esto requiere dos aplicaciones: una primera aplicación (la aplicación de módulo seguro) instalada en el módulo seguro para proporcionar la funcionalidad crítica de seguridad y una segunda aplicación (una aplicación de interfaz de usuario u otra aplicación de contrapartida adecuada) instalada en el teléfono móvil para proporcionar la interfaz de usuario para la primera aplicación y para controlar la primera aplicación en caso de que se proporcione un nivel de seguridad apropiado. Tener dos aplicaciones distintas para proporcionar la funcionalidad total presenta el riesgo de que esos dos se descompongan, destruyendo así el funcionamiento correcto.

En otras palabras, cuando surge una situación en la que el dispositivo móvil por alguna razón no tiene la aplicación de contrapartida requerida (aquí: aplicación de interfaz de usuario), la funcionalidad de interfaz de usuario se desactivará. Esto puede ocurrir, por ejemplo, cuando el módulo seguro se cambia de un dispositivo móvil a otro (si este último no contiene la aplicación requerida) o cuando se está actualizando el software del teléfono.

Como se sugiere en la solicitud de patente internacional PCT/FI2006/050383 del inventor de la presente solicitud, se puede resolver este problema disponiendo un aparato que aloja el módulo seguro para comprobar si está presente una aplicación de contrapartida compatible en el aparato. Esto se puede hacer aprovechando un registro dedicado o una base de datos organizada en el módulo seguro. En el caso de que la aplicación de contrapartida compatible no esté presente, el aparato puede obtener la aplicación de contrapartida compatible de una fuente externa. Sin embargo, cuando se ha actualizado la aplicación de contrapartida compatible, existe el riesgo de que el usuario pueda eliminar o desinstalar intencionadamente o no la aplicación de contrapartida, o arruinar de otro modo el funcionamiento adecuado de la aplicación de contrapartida.

La supresión o eliminación de otra manera puede estar muy bien para algunas aplicaciones como juegos u otras aplicaciones independientes. La supresión o eliminación de una aplicación de contrapartida de módulo seguro, por ejemplo, dicha aplicación de interfaz de usuario, sin embargo, puede causar impactos severos, al menos en la experiencia del usuario. Sin la aplicación de interfaz de usuario, el usuario no puede ver el valor de su ticket de valor, por ejemplo. El usuario puede incluso llegar a la conclusión de que su billete sin contacto se ha perdido, a pesar de que todavía está almacenado de forma segura dentro del módulo seguro.

El documento US2006/0143606 describe un dispositivo de comunicaciones inalámbricas que incluye un entorno de

ejecución de software y un gestor de permisos de software que está asociado con el entorno de ejecución de software. El entorno de ejecución de software define elementos de estado para al menos un paquete instalado de aplicaciones de software instalado en el entorno de ejecución del software. Los elementos de estado especifican acciones de usuario prohibidas con respecto a al menos un paquete de aplicación de software. El dispositivo de comunicaciones inalámbricas incluye además un gestor de paquetes de software que proporciona comunicaciones con al menos un paquete de aplicación de software instalado. El gestor de paquetes de software realiza al menos uno de asegurar, con base en los elementos de estado, una presencia continua de paquetes de aplicaciones de software instalados y hacer cumplir los elementos de estado para un paquete de aplicación de software instalado respectivo.

Sumario

De acuerdo con un primer aspecto de la invención, se proporciona un aparato capaz de alojar un módulo seguro según la reivindicación 1. En un ejemplo, la comprobación de si la aplicación es una aplicación relacionada con el módulo seguro se realiza antes o después de la elección o activación real. En una realización, las aplicaciones relacionadas con el módulo seguro son aplicaciones de contrapartida, tales como aplicaciones de interfaz de usuario de módulo seguro. Sin embargo, está claro que las aplicaciones no están restringidas a las aplicaciones de interfaz de usuario, sino que también son aplicables otras aplicaciones, como las aplicaciones de control o administración. En una realización, una aplicación de contrapartida es una aplicación compatible que reside en el aparato (de alojamiento) fuera del módulo seguro. En una realización, la aplicación de contrapartida es una aplicación que está diseñada para operar junto con la aplicación del elemento seguro. En una realización, la aplicación de contrapartida es una aplicación que proporciona una interfaz de usuario para el módulo seguro en una estación móvil. En una realización, la aplicación de contrapartida es una aplicación de control que controla el funcionamiento del módulo seguro desde el exterior. En otra realización, la aplicación de contrapartida es otra aplicación que gestiona el módulo seguro.

En un ejemplo, un registro de aplicación de interfaz de usuario se implementa en un elemento de tarjeta inteligente seguro que contiene una entrada para cada aplicación segura almacenada en el elemento de tarjeta inteligente segura. En un ejemplo de supresión, la protección de los midlets relativos a la tarjeta inteligente segura se implementa marcando los midlets relativos a la tarjeta inteligente segura usando el registro/directorio de la aplicación del elemento de tarjeta inteligente segura.

En un ejemplo, los midlets que actúan como interfaz de usuario para aplicaciones de módulo de tarjeta inteligente segura son manejados por el dispositivo de alojamiento de manera diferente a las aplicaciones regulares o midlets.

En un ejemplo, un módulo seguro es alimentado durante la operación de alimentación de terminal y un procesador de un módulo de alojamiento seguro recibe información desde el módulo seguro durante este tiempo. El procesador crea una especie de archivo virtual que almacena esta información, en la que la información de archivo virtual se actualiza cuando el módulo seguro está alimentado. Entonces, siempre que se accede a un midlet relativo al elemento seguro, un puntero al archivo virtual indica si el midlet puede modificarse a través de la interfaz de usuario del terminal o no.

En una realización, un aparato de alojamiento, tal como un terminal móvil o teléfono, implementa una instalación o clase de aplicación separada para aquellas aplicaciones residentes en el aparato de alojamiento, que actúan como aplicaciones de interfaz de usuario de aplicación de módulo seguro o aplicaciones de gestión. De esta forma, las aplicaciones relacionadas con el módulo seguro (como la interfaz de usuario o los midlets de administración) se pueden separar de las aplicaciones habituales. Basado en la separación, las medidas de restricción pueden ser dirigidas a las aplicaciones que comprende en la instalación separada o clase de aplicación.

Otro ejemplo está dirigido a la protección adicional de la aplicación basada en el dominio de seguridad. Los midlets que acceden al elemento de seguridad interna del teléfono móvil pueden requerir tener una firma específica de Java Security Domain. Normalmente, el teléfono móvil reconoce los dominios de seguridad de fabricantes, operadores, terceros y no fiables. Los tres primeros requieren una cadena de certificados reconocible que coincida con los certificados raíz residentes del teléfono móvil. Cuando el midlet ha sido firmado por un titular de certificado reconocido, el teléfono puede conceder permisos específicos para el midlet. En un ejemplo, un aparato móvil o teléfono móvil implementa un dominio de seguridad adicional basado en el certificado raíz residente en el aparato o módulo seguro. Si el midlet tiene una firma que coincide con este dominio de seguridad, en un ejemplo, el aparato está adaptado para aplicar medidas de restricción de derechos de usuario basadas únicamente en esta firma.

De acuerdo con un segundo aspecto de la invención, se proporciona un método, según la reivindicación 5. Según un tercer aspecto de la invención, se proporciona un programa informático (o software) almacenado en un medio legible por ordenador, comprendiendo el programa de ordenador un código de programa ejecutable por ordenador adaptado para hacer que un aparato realice el método del segundo aspecto.

Varias realizaciones de la presente invención se han ilustrado solo con referencia a ciertos aspectos de la invención. Debe apreciarse que las realizaciones correspondientes pueden aplicarse también a otros aspectos.

Breve descripción de los dibujos

La invención se describirá, a modo de ejemplo solamente, con referencia a los dibujos adjuntos, en los que:

- 5 La figura 1 muestra un aparato capaz de alojar un módulo seguro de acuerdo con una realización de la invención;
- La figura 2a ilustra un aspecto superficial de una interfaz de usuario de acuerdo con una realización de la invención;
- La figura 2b ilustra otra apariencia superficial de una interfaz de usuario de acuerdo con una realización de la invención;
- 10 La figura 3 muestra un aparato de acuerdo con otra realización de la invención;
- La figura 4 ilustra una tabla de registro de acuerdo con una realización de la invención;
- La figura 5 muestra un aparato de acuerdo con otra realización de la invención;
- La figura 6 muestra un aparato de acuerdo con otra realización de la invención;
- 15 La figura 7 muestra diferentes vías de comunicación para un aparato de acuerdo con una realización de la invención; y
- La figura 8 muestra un diagrama de flujo de acuerdo con una realización de la invención.

Memoria detallada

20 La figura 1 muestra un aparato capaz de alojar un módulo seguro fijo o que se puede fijar de forma separable de acuerdo con una realización de la invención. El aparato 100 comprende un procesador 101, una memoria 120 y un software almacenado en la memoria 120. El software comprende código de programa que contiene instrucciones que el procesador 101 ejecuta para controlar el funcionamiento del aparato 100. El software comprende un sistema operativo o firmware 123 y aplicaciones 122. En una realización, el aparato 100 es un terminal móvil o teléfono móvil.

El aparato 100 puede comprender una interfaz de usuario 102 acoplada al procesador 101. La interfaz de usuario 102 comprende normalmente al menos un teclado y una pantalla.

30 El aparato 100 comprende además un módulo o elemento seguro 110 que comprende un procesador 131, una memoria 130 y un software almacenado en la memoria 130. El software comprende un sistema operativo 133 y una o más aplicaciones de módulo seguro 132. En una realización, el módulo seguro 110 es una tarjeta inteligente o chip integrado permanentemente, montado de forma desmontable o montado de forma desmontable en el aparato 100.

35 El módulo seguro puede ser una tarjeta Java (con sistema operativo Java). En el caso de las tarjetas Java, las aplicaciones 132 de módulos seguros pueden denominarse applets. En una realización, el aparato comprende una ranura de tarjeta inteligente en la que puede alimentarse el módulo seguro 110. En una realización, el módulo seguro 110 es un módulo de identidad de abonado (SIM). Normalmente, cualquier módulo seguro 110 debe ser inviolable.

40 El aparato de alojamiento de módulo seguro 100 está configurado para proporcionar conectividad al módulo seguro 110. En la práctica, el aparato 100 puede incluir una interfaz de tarjeta inteligente o módulo de interfaz (no mostrado) que está en contacto con los conectores de clavija físicos del módulo seguro. La interfaz puede acoplarse al procesador 101 a través de un bus de datos (no mostrado). El módulo seguro 110 puede definir niveles de seguridad diferentes para la información diferente contenida en el módulo seguro 110. El aparato 100 puede solicitar información a través de la interfaz desde el módulo seguro 110. Dependiendo de cuál sea el nivel de seguridad de la información solicitada, el módulo seguro 110 entrega la información solicitada al aparato de alojamiento 100. Con este fin, el módulo de seguridad 110 puede comprender, por ejemplo, un módulo de comprobación de seguridad o una función correspondiente (no mostrada). Este módulo puede ser implementado por software o una combinación adecuada de software y hardware. Clasifica información diferente en diferentes niveles de seguridad y comprueba si un solicitante (por ejemplo, el aparato de alojamiento 100 o el software de aparatos) tiene derechos apropiados para recibir información solicitada del módulo seguro 110. De acuerdo con una realización, la verificación de seguridad es implementada por el sistema operativo 133 del módulo seguro 110.

55 La(s) aplicación(es) de módulo seguro 132 pueden comprender, por ejemplo, una aplicación de pago o una aplicación de venta de billetes. Es ejecutado por el procesador de módulo seguro 21. El módulo seguro 110 comprende una interfaz para permitir el acceso al módulo seguro (normalmente pasivo) desde el exterior. Esta interfaz puede proporcionarse mediante disposiciones adecuadas utilizando software y/o hardware y/o disposiciones físicas, tales como conectores de clavija.

60 El usuario del aparato 100 puede interactuar con aplicaciones de módulo seguro 132 utilizando una aplicación de contrapartida dedicada (aplicación de interfaz de usuario) que está incluida dentro de las aplicaciones 122 y es ejecutada por el procesador 101. En el caso de que la aplicación de módulo seguro 132 correspondiente pueda denominarse un applet, la aplicación de contrapartida 122 puede denominarse midlet. Un applet aquí generalmente significa una aplicación personalizada instalada, residente y que se ejecutará en un módulo seguro. Un applet puede ser un applet de tarjeta Java. Un midlet aquí generalmente significa una pequeña aplicación que se instalará en un

dispositivo electrónico. Un midlet puede ser una pequeña aplicación Java. La aplicación de interfaz de usuario 122 implementa una interfaz de usuario para la correspondiente aplicación de módulo seguro 132. De esta manera, la interfaz de usuario 102 (normalmente un teclado y una pantalla) del aparato 100 puede utilizarse como una interfaz de usuario para la aplicación de módulo seguro 132 en cuestión. Mediante la aplicación de interfaz de usuario 122 el usuario puede controlar generalmente la correspondiente al menos una aplicación de módulo seguro 132 que reside en el módulo seguro 110. Con la ayuda de la aplicación de interfaz de usuario 122, el usuario puede, por ejemplo, activar la al menos una aplicación de módulo seguro 132, usar la al menos una aplicación de módulo seguro 132 y/o cerrar la al menos una aplicación de módulo seguro 132 después de su uso.

El aparato 100 puede comprender además un módulo de comunicación de campo cercano 104 con una antena. El módulo de comunicación de campo cercano 104 está conectado al procesador 101 y al módulo de seguridad 110. En una realización, el módulo de comunicación de campo cercano 104 es un módulo de comunicación RFID, tal como, por ejemplo, un lector de RFID. Un dispositivo externo, tal como un terminal de punto de venta o un lector sin contacto (no mostrado en la figura 1), puede comunicarse con el módulo seguro 110 a través del módulo de comunicación de campo cercano 104. El módulo de comunicación de campo cercano 104 puede funcionar en un modo activo o pasivo. En un modo activo, el módulo de comunicación de campo cercano 104 y otro módulo de comunicación de campo cercano activo generan sus propios campos de radiofrecuencia para transferir datos. En un modo pasivo, solo uno de los módulos de comunicación de campo cercano genera el campo de radiofrecuencia. El otro módulo de comunicación de campo cercano funciona como un "módulo de solo lectura", una etiqueta que no transmite activamente.

Este modo también se puede llamar un modo de etiqueta. Para la comunicación con una red de telecomunicaciones celulares, el aparato 100 puede comprender además un transceptor de radio celular 105 con una antena. El transceptor de radio celular 105 está acoplado al procesador 101. El aparato 100 puede comprender además interfaz (es) 106 para comunicaciones de corto alcance, distinta de la comunicación de campo cercano descrita en el anterior, tal como Bluetooth, WLAN (red de área local inalámbrica), UWB (banda ultra ancha) y/o comunicaciones infrarrojas.

En un ejemplo, se ha observado que las aplicaciones de contrapartida de elemento seguro 122 (tales como aplicaciones de interfaz de usuario y otras aplicaciones críticas para gestionar el módulo de seguridad) deben manejarse de manera diferente que otras aplicaciones o midlets 122 comprendidos en la memoria de aparato 120 son manejados. Mediante la implementación de esto, como ejemplo, la eliminación no intencional de las aplicaciones de contrapartida 122 por el usuario se puede evitar en muchos casos.

De acuerdo con una realización, el aparato de alojamiento 100 maneja aplicaciones de interfaz de usuario (o midlets) 122 y otras aplicaciones de contrapartida de manera diferente a las aplicaciones regulares. En esta realización, el aparato 100 maneja diferentes aplicaciones sobre la base de diferentes clases de instalación o aplicación. El aparato 100 implementa una clase de instalación o de aplicación independiente para aplicaciones de contrapartida de módulo seguro (de las cuales la aplicación de interfaz de usuario presenta un ejemplo). Basado en la clase, el software del aparato de hosting marca cualquier aplicación de contraparte. Si el usuario intenta borrar, mover o enmendar la aplicación de contraparte, el software del dispositivo de alojamiento lo impide. De acuerdo con una realización de la invención, el usuario no tiene ningún control sobre la aplicación de contrapartida que no sea usarla.

Dependiendo de la implementación, se puede indicar al usuario qué aplicaciones pertenecen a la clase de aplicación independiente que contiene aplicaciones relacionadas con el módulo seguro. La figura 2a ilustra un aspecto superficial de la interfaz de usuario 102, en la que el usuario ve una lista de aplicaciones presentes en el aparato de alojamiento 100. Este puede ser el contenido de una carpeta visible (carpeta "colecciones" o similar) que comprende diferentes midlets. Las aplicaciones relacionadas con el módulo seguro o midlets se indican con la ayuda de un símbolo de bloqueo en la lista. La figura 2b ilustra otra apariencia superficial de la interfaz de usuario 102. En este ejemplo, los midlets pertenecientes a la clase de aplicación relacionada con el módulo seguro se muestran en una lista que está separada de la lista que muestra midlets regulares. En otra implementación, las aplicaciones relacionadas con el módulo seguro pueden estar ocultas del usuario definiéndolas como archivos ocultos. Ahora, si el usuario, por ejemplo, intenta eliminar una de las aplicaciones relacionadas con el módulo seguro, el software del aparato no deja que suceda automáticamente. En su lugar, puede, por ejemplo, solicitar al usuario un mensaje en la interfaz de usuario (visualización), el mensaje que indica que la supresión del archivo que contiene la aplicación no está permitida. En una realización alternativa, se puede conceder al usuario el permiso para eliminar la aplicación, sin embargo, no directamente sino solo después de un paso o etapas adicionales. El propósito del siguiente paso es asegurar que el usuario no accidentalmente (o sin querer) eliminar la aplicación. La etapa adicional puede comprender la interacción con el usuario. Por ejemplo, el usuario puede ser advertido primero por un mensaje de advertencia, que se muestra en la interfaz de usuario, informando al usuario de la consecuencia de su eliminación y solicitando al usuario que confirme que la aplicación realmente debe eliminarse y que dicha operación no se recomienda. La aplicación se suprime solo después de que se reciba una confirmación del usuario y solo después de que se cumpla cualquier otra condición adicional especificada, como por ejemplo solicitar al usuario realizar ciertos pasos adicionales para obtener el permiso final para eliminar la aplicación, tal como solicitar, por ejemplo, un código PIN de autenticación de usuario o similar del usuario.

La figura 3 muestra un aparato de acuerdo con otra realización de la invención. El aparato 300 corresponde al

aparato 100 en la mayor parte de sus aspectos técnicos. Se han utilizado los mismos números de referencia para indicar partes o funciones similares.

El aparato mostrado en la figura 3 hace uso del registro o base de datos 335 dispuesto en la memoria 130 del módulo seguro 110. Uno de tales registros se ha descrito en la solicitud de patente internacional PCT/FI2006/050383 del inventor de la presente solicitud.

El módulo seguro 110 tiene la tabla de registro o base de datos 335. El registro 335 puede implementarse como una aplicación independiente en un chip de elemento seguro. Alternativamente, la funcionalidad puede implementarse en el sistema operativo de módulo seguro 133. En el registro se mantiene información sobre las aplicaciones de módulo seguro instaladas 132 y las aplicaciones de contrapartida 122. Para cada aplicación de módulo seguro 132, el registro contiene información que identifica la aplicación de contrapartida 122 que se requiere que esté presente en el aparato de alojamiento 300. Esta información puede presentarse de varias maneras. Por ejemplo, esta información puede comprender el nombre (o algún otro identificador) y el número de versión de la solicitud de contrapartida requerida 122. En una realización alternativa, el registro 335 contiene información tanto del nombre como del proveedor. En una realización alternativa, el registro 335 contiene instrucciones sobre cómo instalar/actualizar la aplicación de contrapartida 122 requerida. Si el aparato no tiene la aplicación de contrapartida requerida 122 o la versión requerida de la aplicación, puede realizarse una instalación o actualización siguiendo las instrucciones. Dichas instrucciones pueden comprender, por ejemplo, la dirección de un recurso de red desde el que se puede descargar la aplicación o actualización. Esta dirección puede tener la forma de una URL (localizador de fuente uniforme).

La figura 4 ilustra una realización del registro 335. En esta realización, el registro 335 contiene para cada aplicación de módulo seguro 132 (identificada por ejemplo por un identificador de aplicación y de versión) información que identifica la aplicación de contrapartida 122 exacta y exacta (nombre y versión) y el sitio de red desde el cual esta aplicación o actualización puede ser descargado.

En una realización, el sistema operativo o firmware 123 del aparato de alojamiento 300 (figura 3) recupera la información contenida en el registro 335 y almacena esta información en la memoria 120. En una realización, esta información contiene información que indica la correspondencia de aplicaciones de módulo seguro y aplicaciones de contrapartida. En una realización, una réplica 325 del registro 335 se escribe en la memoria 120 del aparato de alojamiento 300. El firmware 123 del aparato de alojamiento 300 puede comprobar de vez en cuando el contenido del registro 335 y actualizar su réplica 325 en consecuencia. Las situaciones típicas de comprobación y actualización son las puestas en marcha de aparatos y las situaciones en las que el módulo seguro 110 se activa para diferentes propósitos, tales como para pagos y/o billetes. Si la energía del módulo seguro 110 ha estado inactiva durante un largo tiempo, el firmware 123 puede estar configurado para alimentar el módulo 110 y comprobar el contenido del registro 335. Esto puede hacerse ocasionalmente, por ejemplo, en varias horas de intervalo. Utilizando la información procedente del registro 335, el software de aparatos alojadores aplica medidas de restricción especiales a las aplicaciones de contrapartida de módulo seguro o midlets 122. Para este fin, la existencia de datos en el registro 335 que enlaza una aplicación de módulo seguro 132 y una correspondiente aplicación de contrapartida 122 en sí misma puede ser interpretada por el aparato de alojamiento como una indicación para aplicar dichas medidas de restricción. Adicionalmente, el registro 335 puede contener datos adicionales (por ejemplo, una columna adicional o conjunto de parámetros) que indiquen directa o indirectamente que deben aplicarse medidas de restricción de derechos de usuario con respecto a la solicitud de contrapartida. En una realización, el registro puede contener una indicación expresa en el registro o la tabla (por ejemplo, un indicador, patrón de bits, parámetro o valor de atributo o texto) que indica que la solicitud de contrapartida debe ser tratada como "no editable" o similar.

Éstas pueden incluir varias medidas de seguridad, medidas de protección de supresión y restricciones de instalación o actualización. Si la aplicación de contrapartida es, por ejemplo, una aplicación de interfaz de usuario, el software de aparatos de alojamiento puede impedir que el usuario elimine involuntariamente la aplicación de contraparte.

La figura 5 muestra un aparato de acuerdo con otro ejemplo más. El aparato 500 corresponde a los aparatos 100 y 300 en la mayor parte de sus aspectos técnicos. Se han utilizado los mismos números de referencia para indicar partes o funciones similares.

El aparato mostrado en la figura 5 hace uso de dominios de seguridad. Normalmente, los aparatos móviles reconocen un conjunto de dominios de seguridad. En el caso de aparatos móviles, éstos pueden implicar un dominio de fabricante, un dominio de operador, un dominio de terceros de confianza y dominio(s) de seguridad no fiable(s). Los tres primeros (fabricantes, operadores y dominios de terceros de confianza) requieren una cadena de certificados reconocible que coincida con los certificados raíz residentes del equipo. Un aparato puede conceder permisos específicos para una aplicación si la solicitud está firmada por un titular de certificado reconocible.

En un ejemplo, el acceso al módulo seguro 110 se controla utilizando un dominio de seguridad de terceros de confianza definido (denominado dominio de acceso de módulo seguro). En un ejemplo, un certificado raíz 537 del dominio de acceso de módulo seguro puede almacenarse dentro de la memoria de módulo seguro 130. Dependiendo de la implementación, el certificado raíz 537 se puede almacenar alternativamente en la memoria general 120 del aparato anfitrión o en ambos lugares. En una realización, es una condición para una aplicación que reside fuera del módulo seguro 110 que, para acceder al módulo seguro 110, la aplicación debe tener una firma que

coincida con el dominio de acceso al módulo seguro. En otras palabras, se permite a una aplicación de contrapartida de módulo seguro 522 acceder al módulo seguro 110 si la solicitud de contrapartida 522 está firmada por una firma de dominio de seguridad que coincide con el dominio de acceso de módulo seguro (o tiene una cadena de certificados reconocible al certificado raíz 537). Para estos fines, se puede utilizar una firma de dominio de seguridad Java, por ejemplo.

Si la aplicación de contrapartida de elemento seguro 522 tiene una firma que coincide con el dominio de seguridad de elemento seguro, el aparato de alojamiento puede aplicar medidas de seguridad basadas en la firma. Basándose en el hecho de que el midlet tiene una firma coincidente, el software de aparatos de alojamiento puede marcar cualquier aplicación de contrapartida. Si el usuario intenta borrar, mover o enmendar la aplicación de contraparte, el software del dispositivo de alojamiento lo impide. En su lugar, puede, por ejemplo, solicitar al usuario un mensaje en la interfaz de usuario (visualización), el mensaje indica que no se permite modificar el archivo en cuestión. En una realización alternativa, se puede conceder al usuario permiso para eliminar la solicitud, no sin embargo directamente, sino solo después de que se ha tomado una o más etapas adicionales y/o se ha cumplido una condición adicional similar a lo que se ha descrito en la anterior.

Las realizaciones y ejemplos presentados en relación con las figuras 1, 3 y 5 pueden considerarse independientes entre sí. Sin embargo, también pueden utilizarse en cualquier combinación adecuada. En la figura 6 se muestra una combinación a modo de ejemplo. El aparato 600 implementa el dominio de seguridad adicional para restringir los derechos de acceso de los midlets 522 que acceden al elemento seguro 110 residente del aparato. El certificado raíz 537 se almacena en la memoria de elementos seguros 130. El software de aparatos contenido en la memoria 120 gestiona los midlets 522 de manera que imponga reglas del dominio de seguridad adicional para acceder al módulo seguro desde un midlet 522. El elemento seguro 110 tiene el registro 335 que contiene datos de aplicaciones de módulo seguro 132 y sus correspondientes aplicaciones de contraparte o midlets 522. El software del aparato supervisa el registro de módulo seguro 335. Cuando se instala una aplicación de módulo seguro 132 y la instalación ha realizado un registro en el registro 335, el aparato de alojamiento 600 solicita al usuario que instale la aplicación de contrapartida compatible 522, y con permiso, realiza la instalación. De forma similar, cuando se actualiza una aplicación de módulo seguro 132 y la actualización ha realizado un registro en el registro 335, el aparato de alojamiento 600 solicita al usuario que actualice la aplicación de contrapartida compatible 522, y con permiso, realiza la actualización. El software de aparato escribe una réplica 325 del registro 335 en la memoria 120 del aparato de alojamiento 600, u obtiene de otro modo información de aplicaciones de módulo seguro 132 y las correspondientes aplicaciones de contrapartida 522. Utilizando la información procedente del registro 335, el software del aparato aplica medidas de restricción especiales (por ejemplo, protección contra delección) a las aplicaciones de contrapartida de módulo seguro o a los midlets 522. Cuando se elimina una aplicación de módulo seguro 132 el software del aparato suprime la aplicación de contrapartida 522 en consecuencia. De manera similar, cuando una aplicación de módulo seguro 132 es invalidada, por el emisor de la tarjeta o emisor de la aplicación, el software del aparato suprime o invalida la aplicación de contrapartida 522 en consecuencia.

De acuerdo con una realización, el usuario no proporciona substancialmente ningún otro control a la aplicación de contrapartida o midlet 522 sino para usarlo. La gestión de dichas aplicaciones de contraparte o midlets 522 está dispuesta para seguir la misma lógica que la gestión de las correspondientes aplicaciones 132 de elementos seguros.

En un ejemplo alternativo, está dispuesto que el registro de módulo seguro permita (directa o indirectamente) una elección entre múltiples aplicaciones de contraparte (por ejemplo, aplicaciones de interfaz de usuario). El usuario puede tener la opción de elegir una o más de una (o incluso todas) aplicaciones de contraparte que se instalarán. En un ejemplo, el software de aparatos de alojamiento está dispuesto para manejar todos los que se describen en el anterior. En otro ejemplo, el software del aparato está dispuesto para tratar el conjunto de aplicaciones de contrapartida alternativas como se ha descrito en el anterior, pero para permitir al usuario instalar y eliminar midlets individuales siempre que haya al menos un midlet compatible disponible para actuar como contraparte Para cada aplicación de módulo seguro. La figura 7 muestra diferentes rutas de instalación y/o actualización de aplicaciones en un aparato de acuerdo con un ejemplo. Según una alternativa, se instala una aplicación de módulo seguro o actualización de aplicación mediante un método sin contacto que utiliza un enlace de comunicación de campo cercano. El archivo o comandos de aplicación y/o instalación se transfieren desde un lector sin contacto 50 sobre el enlace de comunicación de campo cercano al módulo de comunicación de campo cercano 104 y desde allí al elemento de seguridad 110 en el que se lleva a cabo la instalación. Según otra alternativa, la aplicación de módulo seguro o actualización de aplicación se instala mediante el método de instalación en el aire (OTA). En esta alternativa, el archivo o comandos de aplicación y/o instalación se transfieren desde un servidor en vivo seguro 750 a través de la red de comunicaciones 740 al aparato 600 utilizando un servicio de comunicaciones orientado a conexión o sin conexión de red de telefonía celular. El archivo o comandos de aplicación y/o instalación son recibidos por el transceptor de radio celular 105 que los pone adelante para la instalación segura de la aplicación del módulo.

Con más detalle, la instalación mediante el método OTA puede implementarse, por ejemplo, de acuerdo con la siguiente realización a modo de ejemplo. En primer lugar, se establece una conexión segura (asegurada por una clave secreta, por ejemplo) entre el módulo seguro 110 y el servidor seguro 750. Después del establecimiento de la conexión, el servidor seguro 750 emite comandos de instalación de la aplicación para controlar la instalación del módulo seguro (132) (o la actualización). La aplicación de módulo seguro 132 se instala (o se actualiza) sobre la base de los comandos de instalación. En caso de que exista el registro (o directorio) 335 en el módulo seguro 110, el

registro 335 se actualiza con la información de instalación mediante comandos OTA o implícitamente por el sistema operativo de módulo seguro 133.

5 Posteriormente, se instala (o actualiza) una correspondiente aplicación de contrapartida 122, 522 en el aparato de alojamiento en respuesta a instrucción(es)/comando(s) recibidos desde el servidor 750. Alternativamente, como se describe en la solicitud de patente internacional PCT/FI2006/050383, El aparato de alojamiento puede comprobar desde el módulo seguro 110 si se necesita una instalación (o actualización) y realizar la instalación (o actualización) en consecuencia. En una realización, el registro 335 identifica la o las aplicaciones de contrapartida 522 para la o las aplicaciones de módulo seguro 132. El registro 335 de esa manera proporciona al aparato de alojamiento una
10 indicación de qué aplicaciones o intermedios 522 el dispositivo de alojamiento debe tratar como aplicaciones relacionadas con el módulo seguro (por ejemplo, a qué aplicaciones el software de aparatos de alojamiento debe aplicar las medidas de restricción especial mencionadas en los párrafos anteriores).

15 En el caso de que no exista ningún registro que enlace las aplicaciones de módulo seguro 132 y las aplicaciones de contrapartida 522 conjuntamente, el servidor 750 puede asignar las aplicaciones de contrapartida 522 durante la instalación (o actualización) de modo que el aparato de alojamiento comprenda que dichas aplicaciones son aplicaciones relacionadas con el módulo seguro al que deben aplicar las medidas especiales de restricción.

20 La figura 8 muestra un diagrama de flujo a modo de ejemplo de acuerdo con una realización de la invención. En la etapa 810 el usuario del aparato elige una aplicación residente del aparato anfitrión 122 a través de la interfaz de usuario 102 o activa la aplicación 122 a través de la interfaz de usuario 102 (por ejemplo, realiza cualquier intento de manipulación para eliminar o modificar la aplicación 122 de modo que la aplicación 122 ya no funcionaría correctamente después de tal manipulación). En la etapa 820, el procesador 101 comprueba si la aplicación 122 es una aplicación relacionada con un módulo seguro (es decir, una aplicación de contrapartida o similar). Esto se puede
25 comprobar, dependiendo de la implementación, desde la réplica del registro 325, o de lo contrario de la memoria 120 si la aplicación ha sido marcada en la memoria 120 de acuerdo con las realizaciones presentadas en la descripción anterior. Si SÍ, el procesador 101 aplica medidas de restricción (por ejemplo, protección contra borrado) en la etapa 830 para restringir los derechos del usuario. Si NO, las medidas de restricción no se aplican.

30 Se han presentado diversas realizaciones de la invención. Debe apreciarse que, en este documento, las palabras comprenden, incluyen y contienen cada una de ellas se utilizan como expresiones abiertas sin ninguna exclusividad.

35 La descripción anterior ha proporcionado a modo de ejemplos no limitativos de implementaciones y realizaciones particulares de la invención una descripción completa e informativa del mejor método y aparato actualmente contemplado por los inventores para llevar a cabo la invención. Sin embargo, es evidente para un experto en la técnica que la invención no está restringida a detalles de las realizaciones presentadas anteriormente, sino que puede implementarse en otras realizaciones usando medios equivalentes sin desviarse de las características de la invención.

40 Además, algunas de las características de las realizaciones descritas anteriormente de esta invención podrían usarse ventajosamente sin el uso correspondiente de otras características. Como tal, la descripción anterior debe considerarse meramente ilustrativa de los principios de la presente invención, y no en limitación de la misma. Por lo tanto, el alcance de la invención solo está restringido por las reivindicaciones de la patente adjuntas.

REIVINDICACIONES

1. Un aparato (100) capaz de alojar un módulo seguro (110), comprendiendo el aparato:

5 medios de memoria (120) para almacenar al menos una aplicación (122); y
 medios de procesamiento (101) configurados para comprobar si la al menos una aplicación (122) es una
 aplicación de contrapartida para una aplicación (132) que reside en el módulo seguro (110) alojado por el aparato
 (100), en donde la aplicación de contrapartida está configurada para permitir que un usuario interactúe con la
 10 aplicación correspondiente (132) que reside en el módulo seguro (110), y en donde la comprobación se basa en
 información recibida del módulo seguro (110), indicando dicha información la correspondencia de las
 aplicaciones (132) que residen en el módulo seguro y las aplicaciones de contrapartida,
 en donde el medio de procesamiento (101) está configurado además para, al determinar que una aplicación
 elegida o activada por el usuario del aparato es una aplicación de contrapartida para una aplicación (132) que
 reside en el módulo seguro (110) alojado por el aparato (100), restringir los derechos de usuario relativos a dicha
 15 aplicación de contraparte (122).

2. Un aparato según la reivindicación 1, en el que la aplicación de contrapartida (122) es una aplicación de interfaz
 de usuario de módulo seguro u otra aplicación de gestión de módulo seguro.

20 3. Un aparato según la reivindicación 1 o la reivindicación 2, en el que los medios de procesamiento (101) están
 configurados para restringir derechos de usuario aplicando al menos uno de medidas de seguridad, protección
 contra borrado o restricción de instalación o de actualización.

4. Un aparato según cualquiera de las reivindicaciones anteriores, en el que los medios de procesamiento (101)
 25 están configurados para restringir los derechos de usuario implementando una clase de aplicación independiente
 para aplicaciones relacionadas con el módulo seguro.

5. Un método para restringir derechos de usuario, que comprende:

30 verificar (820) mediante un aparato (100) capaz de alojar un módulo seguro (110) si una aplicación almacenada
 elegida o activada por un usuario del aparato es una aplicación de contrapartida (122) para una aplicación (132)
 que reside en el módulo seguro alojado por el aparato, en donde la aplicación de contrapartida está configurada
 para permitir que un usuario interactúe con la aplicación correspondiente (132) que reside en el módulo seguro
 (110), y en donde la comprobación se basa en información recibida del módulo seguro (110), indicando dicha
 35 información la correspondencia de las aplicaciones (132) que residen en el módulo seguro y las aplicaciones de
 contrapartida; y
 al determinar que la aplicación elegida o activada por un usuario del aparato es una aplicación de contrapartida
 (122) para una aplicación (132) que reside en el módulo seguro (110) alojado por el aparato (100), restringir
 (830) derechos de usuario relativos a dicha aplicación de contrapartida (122).

40 6. Un método según la reivindicación 5, en el que la aplicación de contrapartida (122) es una aplicación de interfaz
 de usuario de módulo seguro u otra aplicación de gestión de módulo seguro.

7. Un método según la reivindicación 5 o la reivindicación 6, en donde el método comprende restringir derechos de
 45 usuario aplicando al menos uno de medidas de seguridad, protección contra eliminación o restricción de instalación
 o de actualización.

8. Un método según cualquiera de las reivindicaciones 5 a 7, en donde el método comprende restringir derechos de
 usuario utilizando una clase de aplicación independiente para aplicaciones relacionadas con el módulo seguro.

50 9. Un método según cualquiera de las reivindicaciones 5 a 8, en donde el método comprende:

escribir datos desde una réplica de un registro residente de módulo seguro (335) en una memoria de aparato de
 alojamiento (120), y
 55 usar dichos datos o réplica en dicha comprobación si una aplicación es una aplicación relacionada con un
 módulo seguro (122).

10. Un programa informático que comprende un código adaptado para hacer que un aparato realice el método de
 cualquiera de las reivindicaciones anteriores 5 a 9, cuando el programa de ordenador se ejecuta en un procesador.

60 11. Un producto de programa informático que comprende un programa de ordenador según la reivindicación 10, en
 donde el producto de programa de ordenador comprende un medio de lectura informática portador de código de
 programa informático incorporado en el mismo para uso con un ordenador.

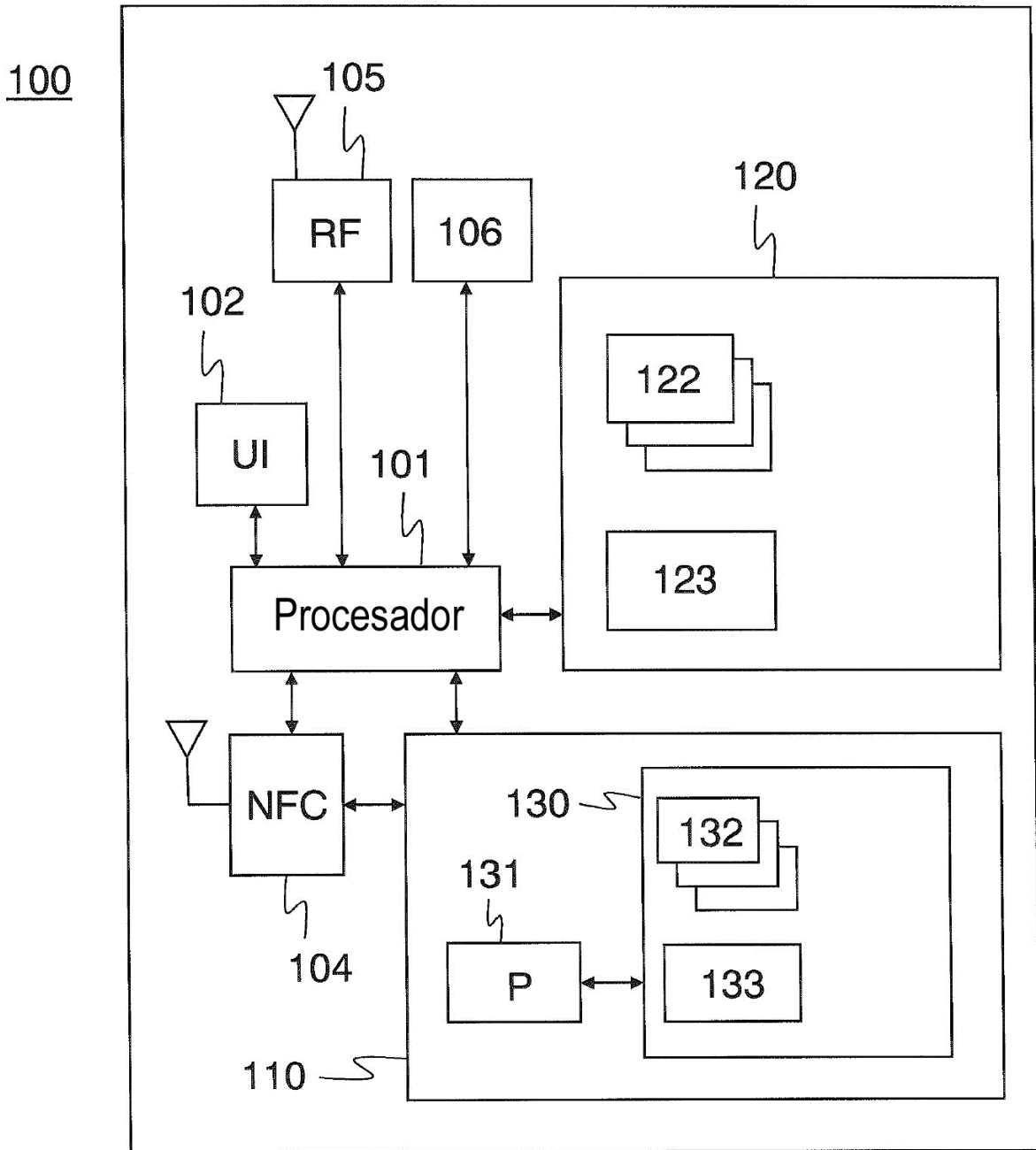


Fig. 1

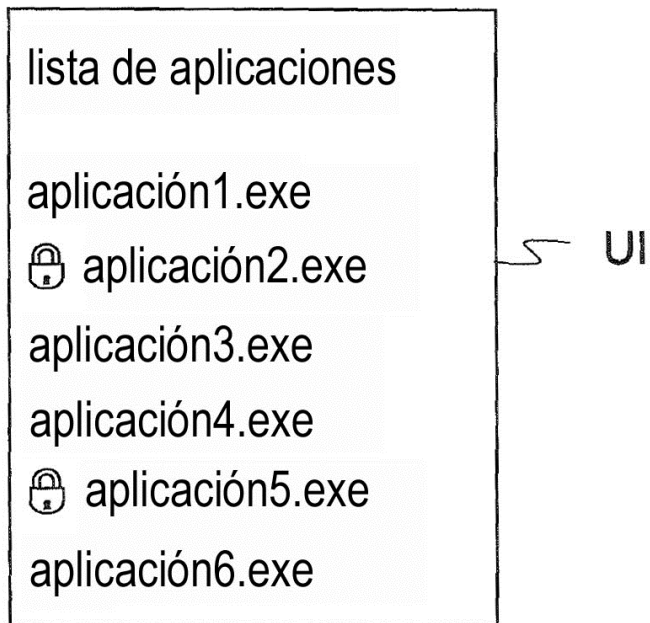


Fig. 2a

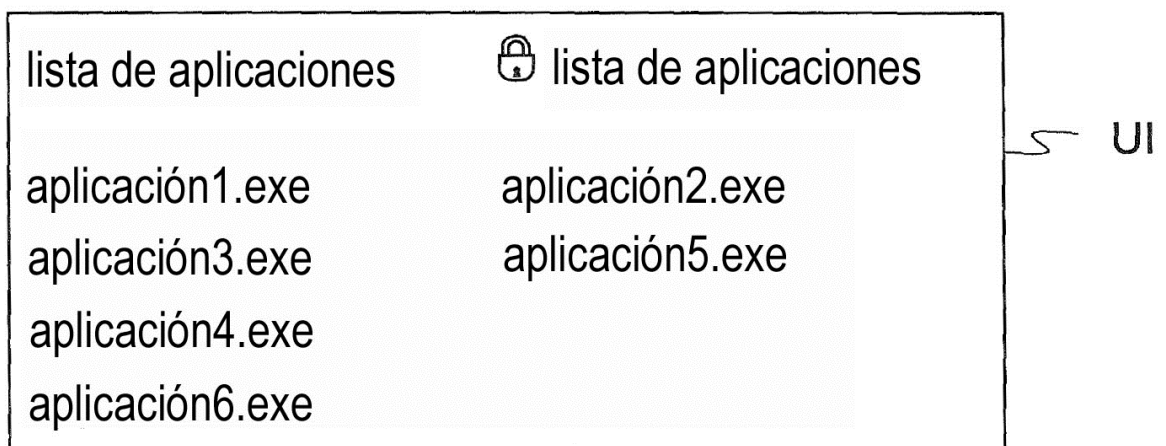


Fig. 2b

300

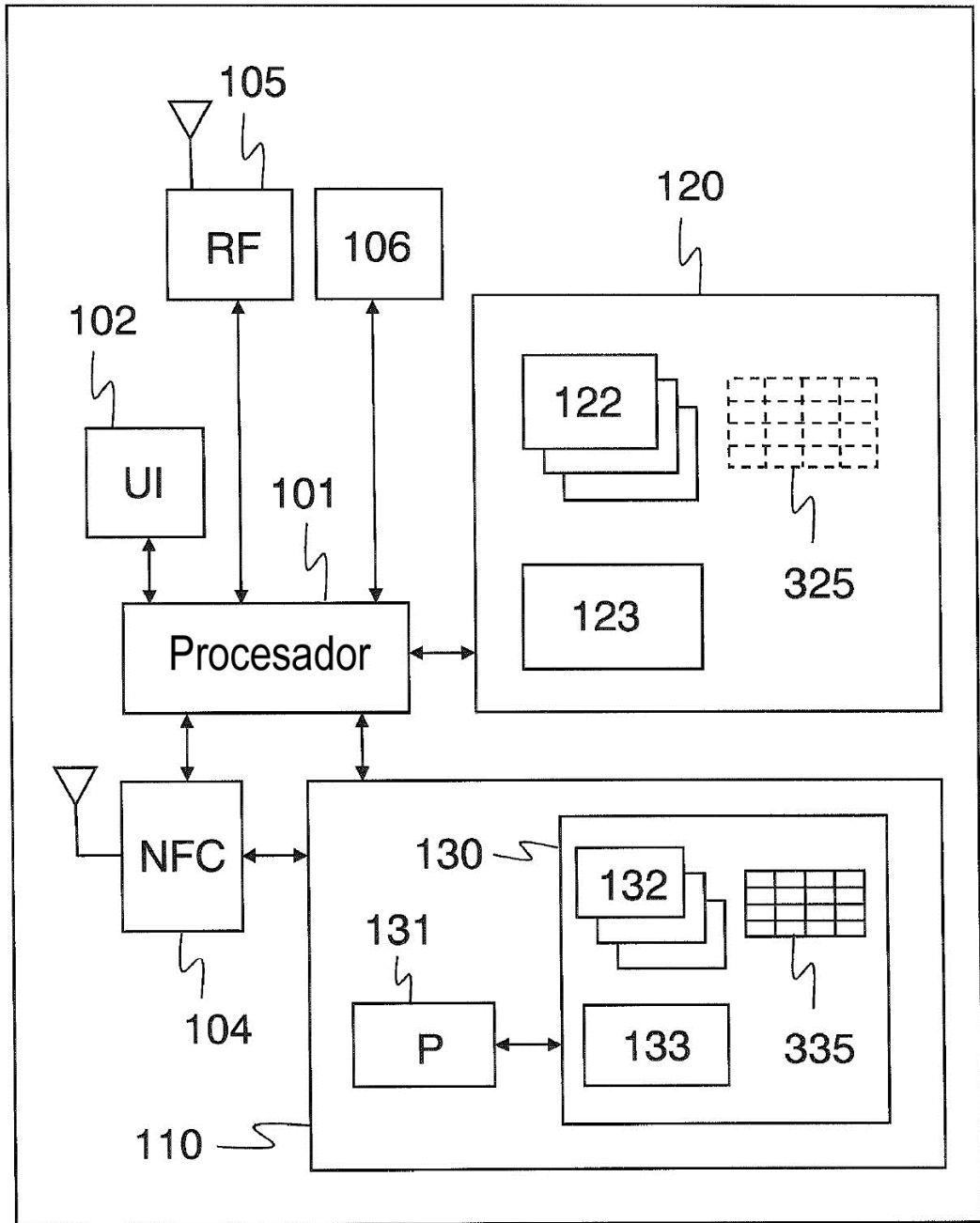


Fig. 3

335

4

ID aplicación SE	nombre/ID aplicación UI	versión aplicación UI	sitio/URL aplicación UI
##### ## #	##### ## #	##### ## #	##### ## #
##### ## #	##### ## #	##### ## #	##### ## #
##### ## #	##### ## #	##### ## #	##### ## #

Fig. 4

500

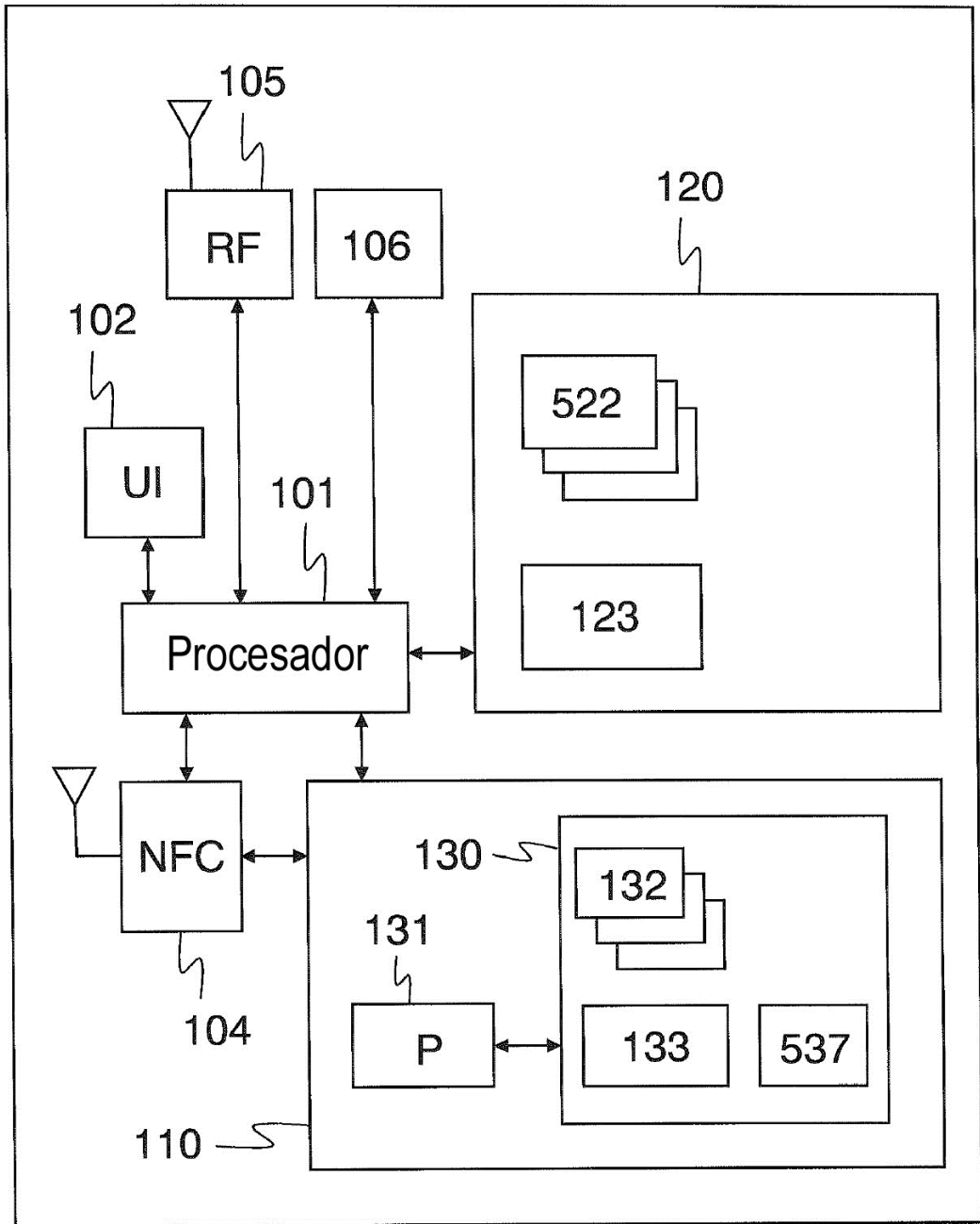


Fig. 5

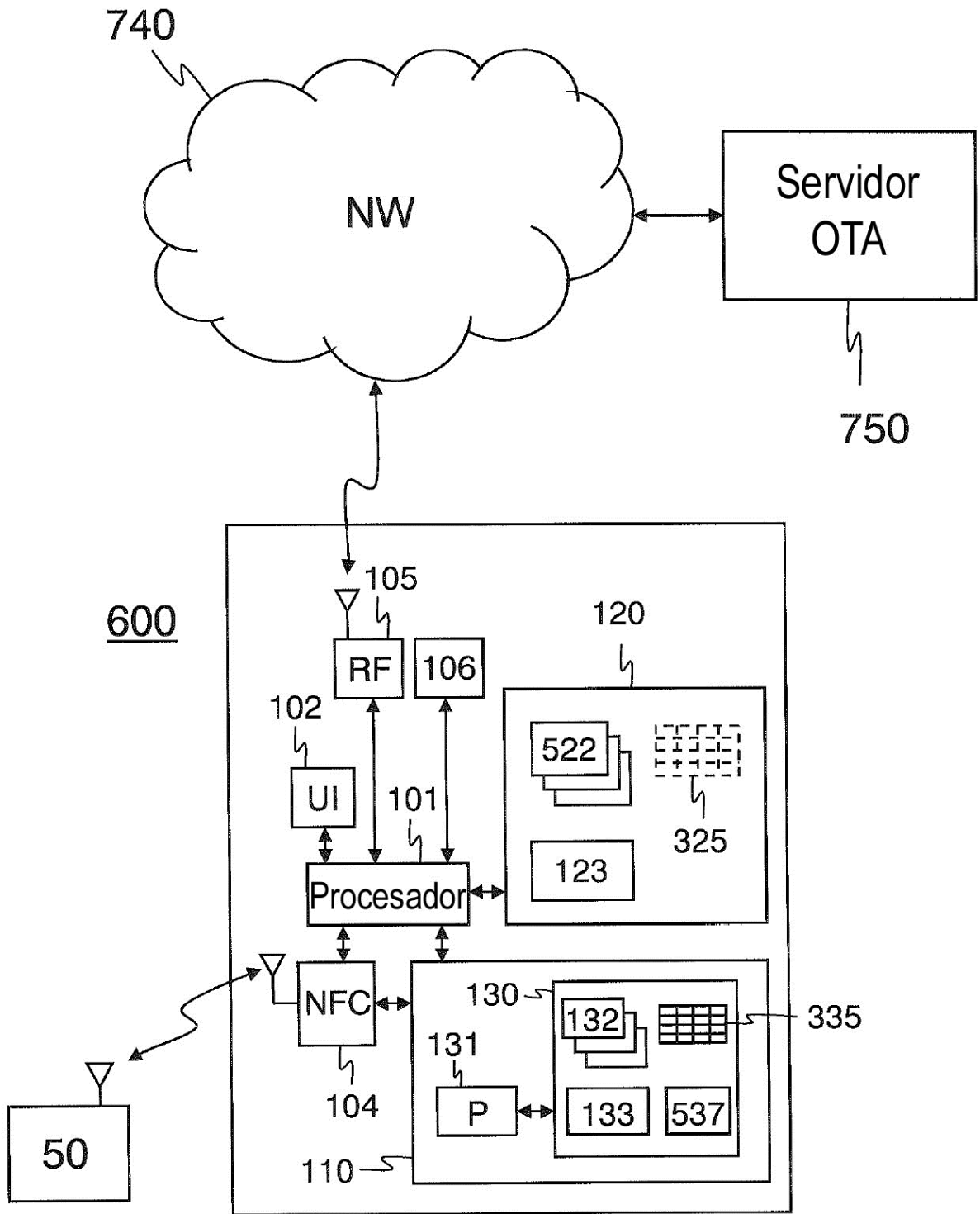


Fig. 7

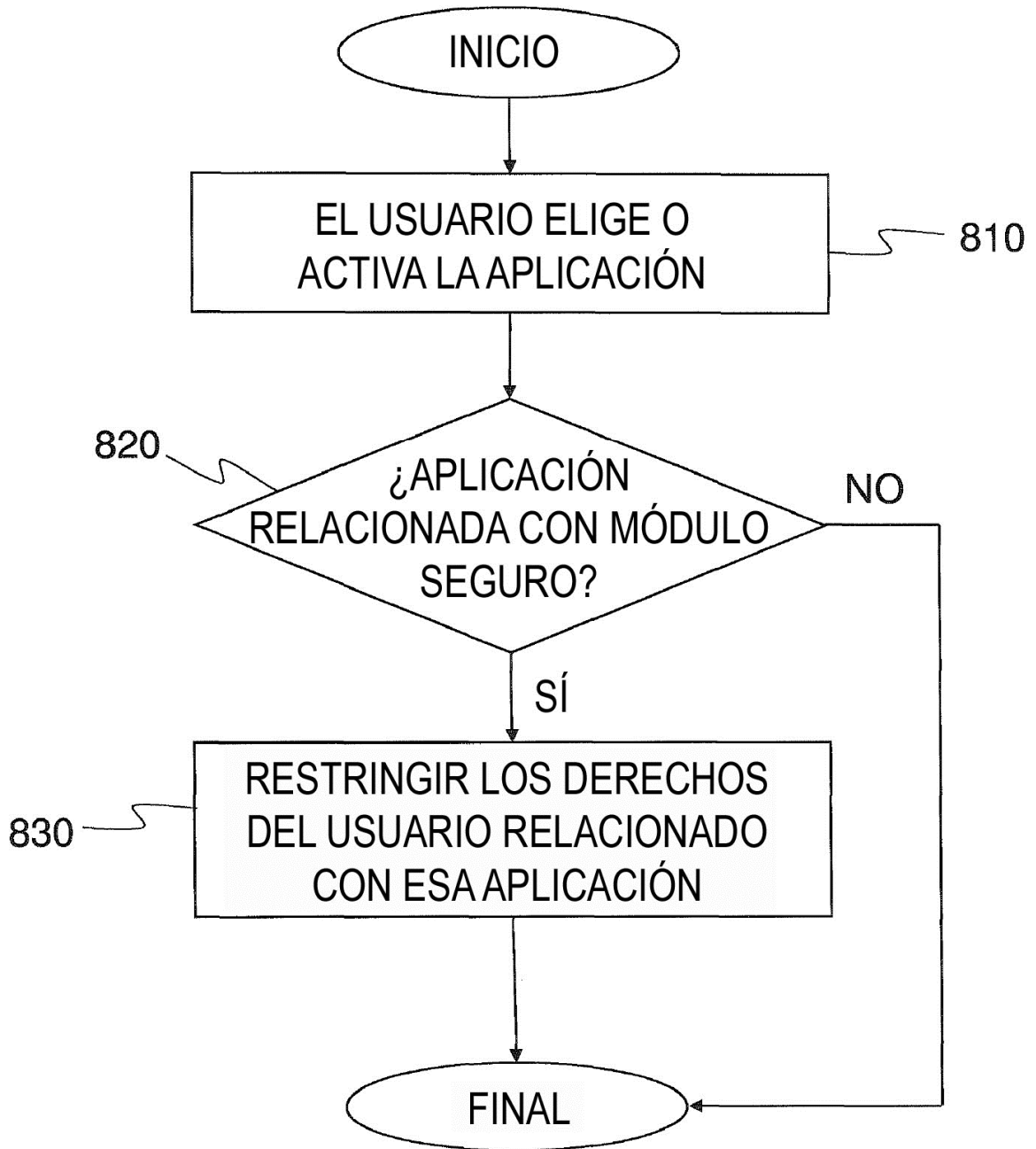


Fig. 8