(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 626 552**

(51) Int. CI.:

G06F 21/51 (2013.01)
G06F 21/62 (2013.01)
G06F 21/60 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.08.2013 PCT/CN2013/082182**

(87) Fecha y número de publicación internacional: **26.02.2015 WO15024253**

(96) Fecha de presentación y número de la solicitud europea: **23.08.2013 E 13886160 (4)**

(97) Fecha y número de publicación de la concesión europea: **12.04.2017 EP 2876568**

(54) Título: **Método y aparato de gestión de permisos y terminal**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.07.2017

(73) Titular/es:

HUAWEI DEVICE CO., LTD. (100.0%)
Building B2 Huawei Industrial Base Bantian
Longgang District Shenzhen
Guangdong 518129, CN

(72) Inventor/es:

HUANG, XI y
WU, HUANGWEI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y aparato de gestión de permisos y terminal

CAMPO DE LA INVENCIÓN

La presente invención se refiere a tecnologías informáticas y en particular, a un método de gestión de permisos, un aparato y un terminal.

ANTECEDENTES DE LA INVENCIÓN

En un sistema operativo de Android, una aplicación puede solicitar diferentes permisos. Después de obtener un permiso requerido mediante solicitud, la aplicación puede solicitar una interfaz API correspondiente o una componente de aplicación para completar una función correspondiente.

En la técnica anterior, en un proceso de utilización de una aplicación que requiere un permiso de ROOT, si no se obtiene el permiso de ROOT, no se puede utilizar normalmente una función que requiere el permiso de ROOT en la aplicación; o si se obtiene el permiso de ROOT, la aplicación se puede ejecutar normalmente, es decir, controlar un sistema, a modo de ejemplo, gestionar y controlar un permiso de una aplicación.

Sin embargo, considerando la seguridad, un desarrollador de un terminal móvil no proporciona el permiso de ROOT para un usuario; por lo tanto, cuando se utiliza el terminal móvil cuyo permiso de ROOT no está disponible para el usuario, el usuario no puede utilizar normalmente una función que corresponde al permiso de ROOT, a modo de ejemplo, el control de, o el acceso a, un sistema del terminal móvil. Las características de seguridad para el sistema operativo Symbian se dan a conocer por el documento de Mark Shackman: “Seguridad de plataforma de Symbian – una descripción técnica (versión 1.2)”; el documento de Andy Harker: “Seguridad de plataforma del sistema operativo de Symbian/08. Instalador de software nativo”; el documento de Craig Heath: “Seguridad de plataforma del sistema operativo de Symbian/01. ¿Por qué una plataforma segura?”; y el documento de Geoff Preston: “Seguridad de plataforma del sistema operativo de Symbian/09. Habilitación de la seguridad de la plataforma”, siendo todos los artículos publicaciones de Internet.

El documento US 20060200668 A1 da a conocer un método para asegurar la ejecución de un programa de aplicación en un teléfono móvil inteligente. Cada aplicación se identifica por un identificador y una tabla de derechos está asociada con cada recurso en el teléfono móvil. Por intermedio de una tabla de derechos, los derechos de acceso al recurso pueden asociarse con un identificador de aplicación. Lo que antecede hace posible gestionar, para cada recurso, las aplicaciones que se permiten para solicitar el recurso. Además, los derechos asociados con un recurso solamente pueden modificarse por el propietario del recurso.

SUMARIO DE LA INVENCIÓN

Formas de realización de la presente invención dan a conocer un método de gestión de permisos, un aparato y un terminal, que se utilizan para realizar el control de, o el acceso a, un sistema de un terminal móvil por un usuario.

De conformidad con un primer aspecto de la idea inventiva, se da a conocer un método de gestión de permisos, que incluye:

obtener un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación incluye un primer certificado e información de demanda de permiso del primer programa de aplicación;

determinar, en conformidad con la información de demanda de permiso, un primer permiso que el primer programa de aplicación requiere durante su ejecución, en donde el primer permiso es un permiso de administrador de sistemas de un sistema; la concesión del primer permiso al primer programa de aplicación de conformidad con el primer certificado del primer programa de aplicación.

La concesión del primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación incluye:

determinar si un segundo certificado está memorizado, o no, en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra en la lista de certificados dignos de confianza utilizando la información de índice en el primer certificado, y al menos un certificado que permite la concesión a un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y

si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; o

si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza,

conceder un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que se abre para el primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

En una primera manera posible de puesta en práctica del primer aspecto de la idea inventiva, después de la determinación de que el segundo certificado está memorizado en la lista de certificados dignos de confianza, el método incluye, además: determinar si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza incluye el primer permiso; y

si la respuesta es positiva, la concesión del primer permiso al primer programa de aplicación; o

si la respuesta es negativa, conceder el segundo permiso al primer programa de aplicación.

En una segunda manera de puesta en práctica posible del primer aspecto de la idea inventiva, la concesión del primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación incluye:

determinar si un segundo certificado está memorizado en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra utilizando información de índice en un certificado de nivel superior del primer certificado, y al menos un certificado que permite la concesión a un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y

si la respuesta es positiva, conceder el primer permiso al primer programa de aplicación; o

si la respuesta es negativa, conceder un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que se abre para el primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

Con referencia a la primera manera de puesta en práctica posible del primer aspecto de la idea inventiva o la segunda manera puesta en práctica posible del primer aspecto, en una tercera manera de puesta en práctica posible del primer aspecto, antes de la concesión del primer permiso al primer programa de aplicación, el método incluye, además:

determinar, en conformidad con el segundo certificado y la información de signatura en el primer programa de aplicación, si el paquete de instalación del primer programa de aplicación está completo o no lo está; y

si el paquete de instalación del primer programa de aplicación no está completo, terminar todas las operaciones; o

si el paquete de instalación del primer programa de aplicación está completo, conceder el primer permiso al primer programa de aplicación.

Con referencia a cualquier manera de puesta en práctica posible del primer aspecto, en una cuarta manera de puesta en práctica posible del primer aspecto de la idea inventiva, después de la concesión del primer permiso al primer programa de aplicación, el método incluye, además:

recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un índice de un tercer certificado, un tercer permiso configurado en el tercer certificado y una instrucción de operación, utilizándose la instrucción de operación para suprimir o añadir el tercer permiso correspondiente al tercer certificado, y el tercer certificado ha sido establecido en la lista de certificados dignos de confianza;

suprimir o añadir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza; y

si el tercer certificado correspondiente al tercer certificado en la lista de certificados dignos de confianza se suprime en conformidad con la información de actualización, realizar un salto operativo de la concesión del tercer permiso a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado; o

si el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza se añade en conformidad con la información de actualización, conceder el tercer permiso a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

Con referencia a cualquier manera de puesta en práctica posible del primer aspecto de la idea inventiva, en una quinta manera de puesta en práctica posible del primer aspecto, después de la concesión del primer permiso al primer programa de aplicación, el método incluye, además:

recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un tercer certificado y una instrucción de operación, y la instrucción de operación se utiliza para añadir el tercer certificado a, o suprimir el tercer certificado de la lista de certificados dignos de confianza;

en conformidad con la información de actualización, añadir el tercer certificado a la lista de certificados dignos de confianza, o suprimir el tercer certificado desde la lista de certificados dignos de confianza; y

si el tercer certificado se añade a la lista de certificados dignos de confianza, conceder un permiso correspondiente al tercer certificado a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado; o

si el tercer certificado se suprime desde la lista de certificados dignos de confianza, realizar un salto operativo de la concesión de un permiso correspondiente al tercer certificado para un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

En conformidad con un segundo aspecto de la idea inventiva, se da a conocer un terminal, que incluye: un receptor y un procesador conectado al receptor, en donde:

el receptor está configurado para obtener un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación incluye un primer certificado e información de demanda de permiso del primer programa de aplicación; y

el procesador está configurado para: determinar, en conformidad con la información de demanda de permiso, un primer permiso que el primer programa de aplicación requiere durante su ejecución, en donde el primer permiso es un permiso de administrador de sistemas de un sistema; y conceder el primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación.

El procesador está específicamente configurado para: determina si un segundo certificado está memorizado en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra en la lista de certificados dignos de confianza utilizando una información de índice en el primer certificado, y al menos un identificador que permite la concesión para un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; o si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que se abre para el primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles, o solicitar a un usuario que guarde el segundo certificado en una lista de certificados dignos de confianza, y después de que el usuario guarde el segundo certificado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación, en donde un certificado al que se asigna confianza por el usuario se memoriza en la lista de certificados dignos de confianza.

En una primera manera de puesta en práctica posible del segundo aspecto de la idea inventiva, el procesador está configurado, además, para: determinar si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza incluye el primer permiso; y si se determina que la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza incluye el primer permiso, conceder el primer permiso al primer programa de aplicación; o si se determina que la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza no incluye el primer permiso, conceder el segundo permiso al primer programa de aplicación.

En una segunda manera de puesta en práctica posible del segundo aspecto de la idea inventiva, el procesador está configurado, además, para: determinar si un segundo certificado está memorizado en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra utilizando información de índice en un certificado de nivel superior del primer certificado, y al menos un certificado que permite la concesión a un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y si se determinar que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; o si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que se abre para el primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

Con referencia a la primera manera de puesta en práctica posible del segundo aspecto de la idea inventiva o a la segunda manera de puesta en práctica posible del segundo aspecto, en una tercera manera de puesta en práctica posible del tercer aspecto, el procesador está configurado, además, para: determinar, en conformidad con el segundo certificado y la información de signatura en el primer programa de aplicación, si el paquete de instalación

del primer programa de aplicación está completo, o no lo está; y el módulo de determinación determina que el paquete de instalación del primer programa de aplicación no está completo, terminar todas las operaciones; o si el módulo de determinación determina que el paquete de instalación del primer programa de aplicación está completo, conceder el primer permiso al primer programa de aplicación.

Con referencia a cualquier manera de puesta en práctica posible del segundo aspecto de la idea inventiva, en una cuarta manera de puesta en práctica posible del segundo aspecto, el receptor está configurado para recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un índice de un tercer certificado, un tercer permiso configurado en el tercer certificado, y una instrucción de operación, utilizándose la instrucción de operación para indicar la supresión o adición del tercer permiso que corresponde al tercer certificado, y el tercer certificado ha sido establecido en la lista de certificados dignos de confianza;

el procesador está configurado, además, para suprimir o añadir la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza; o

el procesador está configurado, además, para: suprimir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza, y realizar un salto operativo de la concesión del tercer permiso a un segundo programa de aplicación; o añadir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza, y conceder el tercer permiso a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

Con referencia a cualquier manera de puesta en práctica posible del segundo aspecto de la idea inventiva, en una quinta manera de puesta en práctica posible del tercer aspecto, el receptor está configurado para recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un tercer certificado y una instrucción de operación, y la instrucción de operación se utiliza para añadir el tercer certificado a, o suprimir el tercer certificado desde la lista de certificados dignos de confianza; y el procesador está configurado, además, para: en conformidad con la información de actualización, añadir el tercer certificado a la lista de certificados dignos de confianza, o suprimir el tercer certificado de la lista de certificados dignos de confianza; o

el procesador está configurado, además, para: después de que el tercer certificado se añada a la lista de certificados dignos de confianza, la concesión de un permiso correspondiente al tercer certificado a un segundo programa de aplicación; o después de que el tercer certificado se suprima de la lista de certificados dignos de confianza, realizar un salto operativo de la concesión de un permiso correspondiente al tercer certificado para un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

En el método de gestión de permisos y el terminal dados a conocer por las formas de realización de la presente invención, se obtiene un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación incluye un primer certificado e información de demanda de permiso del primer programa de aplicación; un primer permiso que el primer programa de aplicación requiere durante su ejecución se determina en conformidad con la información de demanda de permisos, en donde el primer permiso es un permiso del administrador de sistemas de un sistema; y el primer permiso se concede al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación, de modo que el primer permiso que el primer programa de aplicación requiere durante su ejecución se concede al primer programa de aplicación. De este modo, se puede poner en práctica el control de, o el acceso a, un sistema de un terminal móvil por un usuario.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir las soluciones técnicas en las formas de realización de la presente invención o en la técnica anterior con mayor claridad, a continuación se describen, de forma concisa, los dibujos adjuntos requeridos para describir las formas de realización o la técnica anterior. Evidentemente, los dibujos adjuntos en la descripción siguiente ilustran solamente algunas formas de realización de la presente invención y los expertos en esta técnica pueden derivar otros dibujos a partir de estos dibujos adjuntos sin necesidad de esfuerzos creativos.

La Figura 1 es un diagrama de flujo de una forma de realización de un método de gestión de permisos en conformidad con la presente invención;

La Figura 2 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad con la presente invención;

La Figura 3 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad con la presente invención;

La Figura 4 es un diagrama esquemático de una lista de revocación de certificados en el método de gestión de

permisos en conformidad con la presente invención;

La Figura 5 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad transacción la presente invención;

La Figura 6 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad con la presente invención;

La Figura 7 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad con la presente invención;

La Figura 8 es un diagrama estructural esquemático de una forma de realización de un aparato de gestión de permisos en conformidad con la presente invención;

La Figura 9 es un diagrama estructural esquemático de otra forma de realización de un aparato de gestión de permisos en conformidad con la presente invención; y

La Figura 10 es un diagrama estructural esquemático de una forma de realización de un terminal en conformidad con la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

Para hacer más claros los objetivos, las soluciones técnicas y las ventajas de las formas de realización de la presente invención, a continuación se describe, de forma clara y completa, las soluciones técnicas en las formas de realización de la presente invención haciendo referencia a los dibujos adjuntos en dichas formas de realización de la presente invención. Evidentemente, las formas de realización descritas son una parte y no la totalidad de las formas de realización de la presente invención. Todas las demás formas de realización obtenidas por expertos en esta técnica sobre la base de las formas de realización de la presente invención sin necesidad de esfuerzos creativos, deberán caer dentro del alcance de protección de la presente invención.

Un método de gestión de permisos que se da a conocer por las formas de realización de la presente invención puede aplicarse a la instalación de un programa de aplicación de terceros en un terminal móvil, en donde el terminal móvil puede ser un teléfono inteligente, o dispositivo similar. El método de gestión de permisos dado a conocer por las formas de realización puede realizarse mediante un aparato de gestión de permisos, en donde el aparato de gestión de permisos puede estar integrado en el terminal móvil y el aparato de gestión de permisos puede ponerse en práctica utilizando software y/o hardware. A continuación se describe, en detalle, el método de gestión de permisos y el aparato dados a conocer por las formas de realización.

La Figura 1 es un diagrama de flujo de una forma de realización de un método de gestión permisos en conformidad con la presente invención. Según se ilustra en la Figura 1, el método en esta forma de realización puede incluir:

Etapa 101: Obtener un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación incluye un primer certificado e información de demanda de permisos del primer programa de aplicación.

En esta forma de realización, el primer certificado puede ser un certificado que se utilice cuando un desarrollador de aplicaciones de terceros suscriba el primer programa de aplicación. El primer certificado puede incluir una clave pública del primer certificado, un índice del primer certificado, información de propietario del primer certificado, un algoritmo de encriptación del primer certificado y elementos similares. El desarrollador de aplicaciones de terceros puede ser un desarrollador de aplicaciones con la excepción de un desarrollador de sistemas y un fabricante de terminales móviles.

La información de demanda de permiso en esta forma de realización, puede ser información de permiso que necesite solicitarse cuando se ejecute el primer programa de aplicación; y en general, la información de demanda de permiso se establece en un fichero de configuración del paquete de instalación, a modo de ejemplo, cuando el fichero de configuración es un fichero AndroidManifest.xml, el fichero de configuración incluye al menos la información de demanda de permiso y un nombre del primer programa de aplicación.

Etapa 102: Determinar, en conformidad con la información de demanda de permiso, un primer permiso que el primer programa de aplicación requiere durante su ejecución.

En esta forma de realización, un terminal puede determinar, en conformidad con la información de demanda de permiso, un permiso que el primer programa de aplicación requiere durante su ejecución; es decir, el primer programa de aplicación puede solicitar una interfaz API correspondiente o un componente de aplicación solamente cuando tenga un permiso requerido, con el fin de completar una función correspondiente, en donde el permiso que el primer programa de aplicación requiere durante su ejecución puede incluir el primer permiso y/o un segundo permiso.

El primer permiso es un permiso del administrador de sistemas de un sistema. El permiso del administrador de sistemas del sistema puede ser un permiso ROOT_PERMISSION.

A modo de ejemplo, el permiso del administrador de sistemas del sistema puede utilizarse para memorizar información de audio y de vídeo e información de configuración en el sistema, ejecutar un programa de aplicación en el sistema u operación similar.

El segundo permiso puede ser un permiso común, que es un permiso que se abre a un programa de aplicación de terceros por un desarrollador de sistemas y un fabricante de terminales móviles. A modo de ejemplo, en un sistema operativo Android, pueden solicitarse 134 tipos de permisos comunes y estos permisos comunes se memorizan en un fichero AndroidManifest.xml.

Etapa 103: Conceder el primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación.

En esta forma de realización, el primer certificado es un certificado para firmar el primer programa de aplicación, y el primer permiso se concede al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación en al menos dos maneras de puesta en práctica.

En una primera manera de puesta en práctica, se determina, en conformidad con el primer certificado del primer programa de aplicación, que la información del primer certificado se memoriza en una lista de certificados dignos de confianza, y a continuación, el primer permiso se concede al primer programa de aplicación.

Más concretamente, se determina si un segundo certificado está memorizado, o no, en la lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra en la lista de certificados dignos de confianza utilizando información de índice en el primer certificado, al menos un certificado que permite la concesión para un programa de aplicación está memorizado en la lista de certificados dignos de confianza, y un fabricante de terminales móviles configura la lista de certificados dignos de confianza. Conviene señalar que, el segundo certificado es un certificado que se encuentra en la lista de certificados dignos de confianza utilizando la información de índice en el primer certificado; y en este caso, el segundo certificado es el primer certificado y la información de índice en el primer certificado no está manipulada indebidamente. Después de que se memorice la información de índice del primer certificado con, un certificado que se encuentre en la lista de certificados dignos de confianza utilizando la información de índice en el primer certificado no es el primer certificado, y en este caso, el segundo certificado es diferente del primer certificado.

Si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, el primer permiso se concede al primer programa de aplicación; o

si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, un segundo permiso se concede al primer programa de aplicación, o se solicita a un usuario que guarde el segundo certificado en una lista de certificados dignos de confianza del usuario, y después de que el usuario guarde el segundo certificado en la lista de certificados dignos de confianza del usuario, el primer permiso se concede al primer programa de aplicación, en donde un certificado digno de confianza por el usuario se memoriza en la lista de certificados dignos de confianza del usuario. La lista de certificados dignos de confianza del usuario puede incluir certificado que merece confianza por el usuario y mantenido por el propio usuario. Después de que el usuario guarde el certificado en la lista de certificados dignos de confianza del usuario, un permiso correspondiente al certificado puede concederse a un programa de aplicación.

Sin importar si el segundo certificado está memorizado originalmente en la lista de certificados dignos de confianza o el usuario guarda el segundo certificado en la lista de certificados dignos de confianza después de ser solicitado, es decir, después de que se determine que el segundo certificado está memorizado en la lista de certificados dignos de confianza, además, puede determinarse si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza incluye el primer permiso; y

si la respuesta es afirmativa, el primer permiso se concede al primer programa de aplicación; o

si la respuesta es negativa, el segundo permiso se concede al primer programa de aplicación, en donde el segundo permiso que se abre para el primer programa de aplicación por un desarrollador de sistemas y un fabricante de terminales móviles.

En una segunda manera de puesta en práctica, se determina, en conformidad con el primer certificado del primer programa de aplicación, que un certificado de nivel superior del primer certificado está memorizado en una lista de certificados dignos de confianza, y el primer permiso se concede al primer programa de aplicación.

Más concretamente, se determina si un segundo certificado está memorizado en la lista de certificados dignos de

confianza, en donde el segundo certificado es un certificado que se encuentra utilizando información de índice en el certificado de nivel superior del primer certificado, y al menos un certificado que permita la concesión para un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y

si la respuesta es afirmativa, el primer permiso se concede al primer programa de aplicación; o

si la respuesta es negativa, un segundo permiso se concede al primer programa de aplicación.

En esta forma de realización, se obtiene el paquete de instalación del primer programa de aplicación, en donde el paquete de instalación incluye el primer certificado y la información de demanda de permiso del primer programa de aplicación; el primer permiso que el primer programa de aplicación requiere durante su ejecución se determina en conformidad con la información de demanda de permiso, en donde el primer permiso es el permiso del administrador de sistemas del sistema; y luego, el primer permiso se concede al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación. El primer permiso que el primer programa de aplicación requiere durante su ejecución se concede al primer programa de aplicación y de este modo, el acceso a un sistema de un terminal móvil por un usuario puede realizarse a este respecto.

Conviene señalar que, en la forma de realización anterior, en la etapa 103, antes de la concesión del primer permiso al primer programa de aplicación, el método puede incluir, además:

determinar, de conformidad con el segundo certificado y la información de signatura en el primer programa de aplicación, si el primer certificado de instalación del primer programa de aplicación está completo, o no lo está; y

si el paquete de instalación del primer programa de aplicación no está completo, terminar todas las operaciones; o

si el paquete de instalación del primer programa de aplicación está completo, conceder el primer permiso al primer programa de aplicación.

A modo de ejemplo, utilizando la información del primer certificado del primer programa de aplicación, tal como un algoritmo de *hash* registrado en un fichero CERT.RSA, el cálculo de *hash* se realiza en un fichero en el paquete de instalación en el primer programa de aplicación para obtener un valor de hash H1. A continuación, una signatura del primer programa de aplicación, tal como una información de signatura en CERT.SF es objeto de desencriptación utilizando una clave pública registrada en el segundo certificado, para obtener un valor de has H2. H1 se compara con H2. Si H1 es igual H2, se determina que el paquete de instalación del primer programa de aplicación está completo; de no ser así, el paquete de instalación no está completo y se terminan todas las operaciones.

Sobre la base de la forma de realización anterior, la lista de certificados dignos de confianza puede situarse en el terminal móvil o en un servidor.

Además, sobre la base de la forma de realización anterior, el terminal puede recibir, además, información de actualización enviada por el fabricante de terminales móviles, y más concretamente, puede existir al menos dos escenarios operativos aplicables.

En un primer escenario aplicable, se realiza una operación correspondiente sobre un tercer permiso configurado en un tercer certificado que ha sido memorizado en la lista de certificados dignos de confianza, en donde el tercer permiso puede ser un permiso que se abre para un programa de aplicación por un desarrollador de aplicaciones, con la excepción del desarrollador de sistemas y el fabricante de terminales móviles, o el tercer permiso puede ser también un permiso que esté abierto para un programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

Más concretamente, se recibe la información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un índice del tercer certificado, el tercer permiso configurado en el tercer certificado y una instrucción de operación, utilizándose la instrucción de operación para suprimir o añadir el primer certificado correspondiente al tercer certificado, y el tercer certificado ha sido establecido en la lista de certificados dignos de confianza;

la lista de certificados dignos de confianza se actualiza en conformidad con la información de actualización, y el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza se suprime o añade; o

si el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza se suprime en conformidad con la información de actualización, el tercer permiso no se concede a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado; o

si el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza se añade en

conformidad con la información de actualización, el tercer permiso se concede a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

En un segundo escenario aplicable, se realiza una operación correspondiente en un tercer certificado que ha sido memorizado en la lista de certificados dignos de confianza.

Más concretamente, el terminal recibe la información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye el tercer certificado y una instrucción de operación, utilizándose la instrucción de operación para añadir el tercer certificado a, o suprimir el tercer certificado de la lista de certificados dignos de confianza, y conviene señalar que, después de que el tercer certificado se añada a la lista de certificados dignos de confianza, puede añadirse, en consecuencia, un permiso correspondiente al tercer certificado;

en conformidad con la información de actualización, el tercer certificado se añade a la lista de certificados dignos de confianza, o el tercer certificado se suprime desde la lista de certificados dignos de confianza; y

si el tercer certificado se añade a la lista de certificados dignos de confianza, un permiso correspondiente al tercer certificado se concede a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado; o

si el tercer certificado se suprime desde la lista de certificados dignos de confianza, un permiso correspondiente al tercer certificado no se concede a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando un tercer certificado.

La Figura 2 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos, en conformidad con la presente invención. Según se ilustra en la Figura 2, el método en esta forma de realización puede incluir:

Etapa 201: Obtener un paquete de instalación de un primer programa de aplicación.

Más concretamente, cuando el primer programa de aplicación se instala en un terminal móvil, puede obtenerse el paquete de instalación del primer programa de aplicación, y un primer certificado y una información de demanda de permiso del primer programa de aplicación se obtiene a partir del paquete de instalación, es decir, un fichero .apk. A modo de ejemplo, el primer certificado puede incluir una clave pública del primer certificado, información de propietario del primer certificado, un algoritmo de encriptación del primer certificado y elementos similares.

Conviene señalar que, un desarrollador de aplicaciones de terceros puede suscribir un primer programa de aplicación S utilizando el primer certificado A, y un método de signatura puede ser un método de signatura general. A modo de ejemplo, en primer lugar, puede realizarse un cálculo de *hash* sobre todo el contenido del primer programa de aplicación para obtener un valor H de *hash*; a continuación, un algoritmo de encriptación correspondiente al primer certificado A, es decir, una clave privada se utiliza para encriptar el valor de hash H, es decir, el valor de *hash* H es objeto de signatura y se obtiene un valor de signatura; y luego, el primer certificado A y el valor de signatura se añaden al primer programa de aplicación y el primer programa de aplicación es objeto de compresión y empaquetado en el paquete de instalación, es decir, el fichero .apk.

Etapa 202: Determinar si la información de índice de un primer certificado se memoriza, o no, en el paquete de instalación del primer programa de aplicación.

Conviene señalar que, un segundo certificado es un certificado que se encuentra en una lista de certificados dignos de confianza utilizando la información de índice en el primer certificado y en este caso, el segundo certificado es el primer certificado.

Más concretamente, en primer lugar, se determina si un primer certificado de un primer programa de aplicación S incluye información de índice del primer certificado, en donde la información de índice del primer certificado es información que puede identificar, de forma única, el primer certificado. A modo de ejemplo, la información de índice del primer certificado puede ser información de clave pública del primer certificado, y puede ser también información del número del primer certificado, u otra información que pueda identificar, de forma única, al certificado, tal como un número de serie del certificado.

Si se determina que la información de índice del primer certificado está memorizada en el paquete de instalación del primer programa de aplicación, se ejecuta la etapa 203; o si se determina que la información de índice del primer certificado no está memorizada en el paquete de instalación del primer programa de aplicación, se ejecuta la etapa 206.

Etapa 203: Determinar, en conformidad con la información de índice del primer certificado, si un segundo certificado está memorizado, o no, en una lista de certificados dignos de confianza que se coloca en un terminal móvil.

Más concretamente, si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza en el terminal móvil, se ejecuta la etapa 204 y el segundo certificado es el primer certificado.

Si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza en el terminal móvil, se ejecuta la etapa 206.

Además, sobre la base de la forma de realización anterior, si el segundo certificado no se encuentra en la lista de certificados dignos de confianza en conformidad con la información de índice del primer certificado, una información de indicación puede enviarse a un usuario que utilice el terminal móvil, en donde la información de indicación puede solicitar al usuario que añada el primer certificado incluido en el paquete de instalación del primer programa de aplicación a una lista de certificados dignos de confianza del usuario, y configurar un permiso requerido por el primer programa de aplicación, que incluye el primer certificado, tal como un permiso ROOT_PERMISSION. Si el usuario añade el primer certificado a la lista de certificados dignos de confianza, se ejecuta la etapa 204, o si el usuario se niega a añadir el primer certificado a la lista de certificados dignos de confianza que se confía por el usuario, se ejecuta la etapa 206.

Conviene señalar que la lista de certificados dignos de confianza puede colocarse en el terminal móvil por un fabricante de terminales móviles por anticipado, y puede crearse también de forma adicional por el usuario. Además, la lista de certificados dignos de confianza puede memorizarse en una memoria de solamente lectura (Read-Only Memory, ROM en forma abreviada) del terminal móvil; una puesta en práctica específica no está limitada y cualquier soporte de memorización en el terminal móvil puede utilizarse a este respecto. Además, el fabricante de terminales móviles puede encriptar, además, y memorizar la lista de certificados dignos de confianza, con el fin de impedir, mediante encriptación, que sea manipulada indebidamente la lista de certificados dignos de confianza.

En esta forma de realización, existen al menos dos maneras de puesta en práctica específicas para la lista de certificados dignos de confianza. En una primera manera de puesta en práctica, la lista de certificados dignos de confianza se coloca, por separado, en el terminal móvil y un permiso correspondiente a un certificado memorizado en la lista de certificados dignos de confianza es objeto de búsqueda en una lista de permisos utilizando un método de indexación. En una segunda manera de puesta en práctica, una lista de permisos y la lista de certificados dignos de confianza se combinan en una entidad, es decir, en la lista de permisos, se configura una información de permiso correspondiente después de que cada cado memorizado en la lista de certificados dignos de confianza.

Etapa 204: Determinar, en conformidad con el segundo certificado y la información de signatura en el primer programa de aplicación, que el paquete de instalación del primer programa de aplicación está completo.

A modo de ejemplo, un método para determinar que el paquete de instalación del primer programa de aplicación está completo puede ser: en primer lugar, realizar un cálculo de hash en un fichero en el paquete de instalación de un primer programa de aplicación S utilizando un primer certificado del primer programa de aplicación, tal como un algoritmo de hash registrado en un fichero CERT.RSA, se realiza para obtener un valor de hash H1; a continuación, se desencripta una signatura del primer programa de aplicación, tal como una información de signatura en CERT.SF, utilizando una clave pública memorizada en el segundo certificado, con el fin de obtener un valor de hash H2; y luego, comparando H1 con H2. Si H1 no es igual a H2, el paquete de instalación no está completo y por lo tanto, se termina cualquier operación; o si H1 es igual a H2, el paquete de instalación está completo y por lo tanto, se ejecuta la etapa 205.

Etapa 205: Si el paquete de instalación del primer programa de aplicación está completo, conceder un permiso requerido por el primer programa de aplicación para dicho primer programa de aplicación.

Conviene señalar que el permiso requerido por el primer programa de aplicación puede incluir un primer permiso y un segundo permiso, en donde el primer permiso es un permiso del administrador de sistemas de un sistema, a modo de ejemplo, el permiso del administrador de sistemas del sistema puede utilizarse para memorizar información de audio e información de vídeo y la información de configuración en el sistema, ejecutar un programa de aplicación en el sistema o una operación similar. El segundo permiso es un permiso que se desarrolla conjuntamente por un desarrollador de sistemas y un fabricante de terminales móviles para un programa de aplicación de terceros. El permiso del administrador de sistemas del sistema es un permiso ROOT_PERMISSION.

Más concretamente, un método para conceder el primer permiso al primer programa de aplicación puede ser: determinar que una lista de permisos correspondiente al segundo certificado memorizado en la lista de certificados dignos de confianza incluye el primer permiso, y por lo tanto, añadir el primer permiso a una lista de permisos del primer programa de aplicación. Al mismo tiempo, el segundo permiso puede concederse, además, al primer programa de aplicación.

Etapa 206: Determinar, en conformidad con el primer certificado y la información de signatura en el primer programa de aplicación, que el paquete de instalación del primer programa de aplicación está completo.

A modo de ejemplo, un método para determinar que el paquete de instalación está completo puede ser concretamente: en primer lugar, realizar un cálculo de hash en todos los ficheros con la excepción de un fichero de signatura en el paquete de instalación de un primer programa de aplicación S utilizando la información del primer certificado registrada en el primer programa de aplicación, tal como un algoritmo de hash registrado en un fichero CERT.RSA, con el fin de obtener un valor de hash H1; a continuación desencriptar los datos de signatura, tal como una información de signatura en CERT.SF utilizando una clave pública en el fichero de signatura CERT.RSA del primer programa de aplicación, con el fin de obtener un valor de hash H2; y luego, comparar H1 con H2. Si H1 es igual a H2, el paquete de instalación está completo y se ejecuta la etapa 207 posterior; de no ser así, el paquete de instalación no está completo y se termina cualquier operación.

Etapa 207: Conceder, al primer programa de aplicación, un segundo permiso que se solicita para el primer programa de aplicación.

En esta forma de realización, el segundo permiso es un permiso que se abre para el primer programa de aplicación por un desarrollador de sistemas y un fabricante de terminales móviles.

Etapa 208: Registrar la información de instalación del primer programa de aplicación y completar la instalación del primer programa.

En esta forma de realización, después de que se conceda al primer programa de aplicación el primer permiso y/o el segundo permiso, se registra información sobre un primer programa de aplicación S en fichero de registro de información de aplicación packages.xml, en donde la información registrada en el fichero de registro de información de aplicación packages.xml, que incluye un nombre del primer programa de aplicación S, información sobre un permiso concedido al primer programa de aplicación S e información similar.

Conviene señalar que, sobre la base de la forma de realización anterior, antes de la etapa 201, el primer permiso puede añadirse a un sistema primero, a modo de ejemplo, un permiso ROOT_PERMISSION se añade a un sistema Android.

Además, otra manera de puesta en práctica de esta forma de realización es básicamente similar a la forma de realización anterior ilustrada en la Figura 2 y una diferencia es que la lista de certificados dignos de confianza se coloca en un servidor.

Conviene señalar que una lista de certificados dignos de confianza del usuario puede colocarse en el terminal móvil.

La Figura 3 ilustra un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad con la presente invención y la Figura 4 es un diagrama esquemático de una lista de revocación de certificados en un método de gestión de permisos en conformidad con la presente invención. Según se ilustra en la Figura 3, el método en esta forma de realización puede incluir:

Etapa 301: Obtener un paquete de instalación de un primer programa de aplicación.

Un principio de puesta en práctica de la etapa 301 en esta forma de realización es similar al de la etapa 201 ilustrada en la Figura 2, por lo que no se describe aquí de nuevo.

Etapa 302: Determinar, en conformidad con un primer certificado y una información de signatura en el primer programa de aplicación, si el paquete de instalación del primer programa de aplicación está completo.

A modo de ejemplo, un método para determinar que el paquete de instalación del primer programa de aplicación está completo puede ser: realizar un cálculo de hash sobre un fichero en un paquete de instalación de un primer programa de aplicación S utilizando un primer certificado en el primer programa de aplicación, tal como un algoritmo de hash registrado en un fichero CERT.RSA, con el fin de obtener un valor de hash H1; a continuación, desencriptar una signatura del primer programa de aplicación, tal como una información de signatura en CERT.SF, utilizando una clave pública en el primer programa de aplicación, con el fin de obtener un valor de hash H2; y luego, comparar H1 con H2. Si H1 es igual a H2, el paquete de instalación no está completo y por lo tanto, se termina cualquier operación; o si H1 es igual a H2, el paquete de instalación está completo.

Etapa 303: Determinar si el primer programa de aplicación necesita solicitar un primer permiso.

Un permiso que el primer programa de aplicación necesita solicitar en esta forma de realización incluye el primer permiso y un segundo permiso, en donde el primer permiso es un permiso del administrador de sistemas de un sistema, y el permiso del administrador de sistemas del sistema es un permiso ROOT_PERMISSION. A modo de ejemplo, el permiso del administrador de sistemas del sistema puede utilizarse para memorizar información de audio y de vídeo e información de configuración en el sistema, ejecutar un programa de aplicación en el sistema, o funciones similares. El segundo permiso puede ser un permiso que se desarrolla conjuntamente por el desarrollador de sistemas y un fabricante de terminales móviles para un programa de aplicación de terceros.

Más concretamente, si el primer programa de aplicación necesita solicitar el primer permiso, se ejecuta la etapa 304; o si el primer programa de aplicación no necesita solicitar el primer permiso, se ejecuta la etapa 306.

Etapa 304: Determinar si un segundo certificado está memorizado en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado de nivel superior del primer certificado, y la lista de certificados dignos de confianza se coloca en un terminal móvil.

En esta forma de realización, el segundo certificado es el certificado de nivel superior del primer certificado en el primer programa de aplicación, es decir, el segundo certificado es un certificado que se encuentra utilizando información de índice en el certificado de nivel superior del primer certificado.

Además, para cómo determinar si la instalación está completa o no, se puede utilizar la manera siguiente: en primer lugar, se realiza un cálculo de hash sobre el primer certificado utilizando un algoritmo de hash que se utiliza cuando el primer certificado es objeto de signatura, con el fin de obtener un valor de hash H1; a continuación, una signatura en el primer certificado, tal como una información de signatura en el fichero CERT.SF, se desencripta utilizando una clave pública memorizada en el segundo certificado, con el fin de obtener un valor de hash H2 y luego, H1 se compara con H2. Si H1 es igual a H2, puede determinarse, utilizando el segundo certificado, que el paquete de instalación del primer programa de aplicación está completo, es decir, se determina que el segundo certificado correspondiente al primer certificado se memoriza en la lista de certificados dignos de confianza y se ejecuta la etapa 305. Si H1 no es igual a H2, se ejecuta la etapa 306; o cuando se determina que H1 no es igual a H2, se solicita a un usuario que añada el primer certificado a una lista de certificados dignos de confianza del usuario. Si el usuario añade el primer certificado a la lista de certificados dignos de confianza del usuario, se ejecuta la etapa 305; de no ser así, se ejecuta la etapa 306.

Además, antes que se realice el cálculo de *hash* sobre el primer certificado para obtener el valor de *hash* H1, puede determinarse si el primer certificado ha sido revocado o no. A modo de ejemplo, se determina, en conformidad con la lista de revocación de certificados ilustrada en la Figura 4, si el primer certificado está memorizado, o no, en el primer certificado, en donde la información sobre un certificado revocado se memoriza en la lista de revocación de certificados, y la lista de revocación de certificados se coloca en el terminal móvil. Si se determina que el primer certificado está memorizado en la lista de revocación de certificados, a modo de ejemplo, el primer certificado está numerado como C00001 y está memorizado en la lista ilustrada en la Figura 4, y luego se confirma que el primer certificado ha sido revocado, y una operación de concesión del primer permiso al primer programa de aplicación se termina; o si se determina que el primer certificado no está memorizado en la lista de revocación de certificados, se confirma que el primer certificado no ha sido revocado y luego, puede realizarse un cálculo de hash sobre el primer certificado con el fin de obtener el valor de hash H1.

Conviene señalar que un fabricante de terminales móviles puede generar, utilizando un segundo certificado del fabricante de terminales móviles un sub-certificado del segundo certificado, es decir, el primer certificado, para desarrollador de aplicaciones que es objeto de confianza por el fabricante de terminales móviles. Un proceso de generación es un proceso de generación de sub-certificados general; y a modo de ejemplo, se obtiene un abstracto utilizando el algoritmo de hash sobre la información sobre el primer certificado, el abstracto de la información sobre el primer certificado es encriptada utilizando una clave privada correspondiente a una clave pública en el segundo certificado, para generar una signatura y la signatura se memoriza en el primer certificado.

Etapa 305: Conceder un permiso requerido por el primer programa de aplicación al primer programa de aplicación.

Un principio de puesta en práctica de la etapa 305 en esta forma de realización es similar al de la etapa 205 que se ilustra en la Figura 2, por lo que no se describirá aquí de nuevo.

Etapa 306: Conceder, al primer programa de aplicación, un segundo permiso que se solicita por el primer programa de aplicación.

Etapa 307: Registrar información de instalación del primer programa de aplicación y completar la instalación del primer programa.

Los principios de puesta en práctica de la etapa 306 y de la etapa 307 en esta forma de realización son similares a las de las etapas 207 y 208 ilustradas en la Figura 2, respectivamente, por lo que no se describirán aquí de nuevo.

Conviene señalar que, sobre la base de las formas de realización anteriores, antes de la etapa 301, el primer permiso puede añadir a un sistema en primer lugar, a modo de ejemplo, un permiso ROOT_PERMISSION se añade a un sistema Android.

Además, otra manera de puesta en práctica de esta forma de realización es básicamente similar a la forma de realización anterior ilustrada en la Figura 3 y una diferencia es que la lista de certificados dignos de confianza se coloca en un servidor.

Conviene señalar que en la etapa 304, el primer certificado está memorizado en una lista de certificados dignos de confianza del usuario, en donde la lista de certificados dignos de confianza del usuario se coloca también en el terminal móvil, según se ilustra en la Figura 2.

La Figura 5 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad con la presente invención. Según se ilustra en la Figura 5, el método en esta forma de realización puede incluir:

Etapa 501: Obtener un paquete de instalación de un primer programa de aplicación.

Etapa 502: Determinar, en conformidad con un primer certificado e información de signatura en el primer programa de aplicación, que el paquete de instalación del primer programa de aplicación está completo.

Los principios de puesta en práctica de la etapa 501 y de la etapa 502 en esta forma de realización son similares a los de la etapa 301 y la etapa 302 ilustradas en la Figura 3, respectivamente, por lo que no se describirán aquí de nuevo.

Etapa 503: Determinar que el primer programa de aplicación necesita solicitar un identificador de usuario que sea el mismo que el de un sistema.

En esta forma de realización, un terminal puede realizar un análisis sintáctico de la información del identificador de usuario compartido (sharedUserId) de una aplicación y tener conocimiento de que el primer programa de aplicación necesita compartir un identificador de usuario userId con un usuario del sistema.

Etapa 504: Determinar si un segundo certificado está memorizado, o no, en un terminal móvil, en donde el segundo certificado es un certificado de nivel superior del primer certificado.

En esta forma de realización, si el segundo certificado está memorizado en el terminal móvil, se ejecuta la etapa 505; de no ser así, se ejecuta la etapa 506.

Más concretamente, un fabricante de terminales móviles puede colocar el segundo certificado en el terminal móvil por anticipado; y puede ser también que, cuando un programa de aplicación se instale en el terminal móvil, un segundo certificado incluido en el programa de aplicación se memorice en el terminal móvil, en donde el segundo certificado es el certificado de nivel superior del primer certificado.

Etapa 505: Permitir que el primer programa de aplicación comparta un identificador de usuario con el sistema.

Más concretamente, la información compartida correspondiente puede registrarse packages.xml y una forma de registro es como sigue:

<nombre del paquete=" com.M.S."

codePath="/system/app/S.apk" nativeLibraryPach="/data/data/com.M.S./lib"

indicadores = "1" ft="137c481b198" it="137c481b198"

ut="137c481b198" versión="1" sharedUserId= "1000">

<sigs count= "1">

<cert index= "0"/>

</signaturas>

</paquete>;

Etapa 506: Conceder, a una primera aplicación en conformidad con una regla de concesión de permisos, un permiso que se solicita.

Más concretamente, si el segundo certificado no está memorizado en el terminal móvil, el permiso que se solicita puede concederse a la primera aplicación de conformidad con una regla de concesión de permisos en la que la primera aplicación no comparte un identificador de usuario con el sistema; y si el primer programa de aplicación comparte un identificador de usuario con el sistema, el permiso que se solicita puede ser concedido a la primera aplicación de conformidad con una regla de concesión de permisos en la que la primera aplicación comparte un identificador de usuario con el sistema.

Conviene señalar que, si se determina que el primer programa de aplicación necesita solicitar un identificador de usuario que no es el mismo que el del sistema, puede concederse un segundo permiso para el primer programa de aplicación.

La Figura 6 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad con la presente invención, según se ilustra en la Figura 6.

Etapa 601: Obtener un paquete de instalación de un primer programa de aplicación.

Etapa 602: Determinar, en conformidad con un primer certificado e información de signatura en el primer programa de aplicación, que el paquete de instalación del primer programa de aplicación está completo.

Los principios de puesta en práctica de la etapa 601 y de la etapa 602 en esta forma de realización son similares a los de la etapa 301 y la etapa 302 ilustradas en la Figura 3, respectivamente, por lo que no se describirán aquí de nuevo.

Etapa 603: Determinar, en conformidad con la información de índice del primer certificado, si un segundo certificado está memorizado, o no, en una lista de certificados dignos de confianza que se coloca en un terminal móvil.

Un principio de puesta en práctica de la etapa 603 en esta forma de realización es similar al de la etapa 203 ilustrada en la Figura 2, por lo que no se describirá aquí de nuevo.

Conviene señalar que, si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza en el terminal móvil, se ejecuta la etapa 604.

Si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza en el terminal móvil, se ejecuta la etapa 605.

Etapa 604: Conceder un permiso solicitado por el primer programa de aplicación para el primer programa de aplicación.

Etapa 605: Conceder, al primer programa de aplicación, un segundo permiso que se solicita por el primer programa de aplicación.

Etapa 606: Registrar la información de instalación del primer programa de aplicación y completar la instalación del primer programa.

Los principios de puesta en práctica de la etapa 604, la etapa 605 y la etapa 606 en esta forma de realización son similares a los de la etapa 205, etapa 207 y la etapa 208 ilustradas en la Figura 2, respectivamente, por lo que no se repetirán aquí de nuevo.

Conviene señalar que, sobre la base de las formas de realización anteriores, antes de la etapa 601, un primer permiso puede añadirse un primer permiso a un sistema en primer lugar, a modo de ejemplo, un permiso de ROOT_PERMISSIOIN se añade a un sistema Android.

Además, otra manera de puesta en práctica de esta forma de realización es básicamente similar a la forma de realización anterior ilustrada en la Figura 6 y una diferencia es que la lista de certificados dignos de confianza se coloca en un servidor.

La Figura 7 es un diagrama de flujo de otra forma de realización de un método de gestión de permisos en conformidad con la presente invención. Según se ilustra en la Figura 7, sobre la base de las formas de realización anteriores, después de que se complete la instalación de un primer programa, el método puede incluir, además:

Etapa 701: Recibir información de actualización para actualizar una lista de certificados dignos de confianza.

Más concretamente, existen al menos dos escenarios aplicables en los que un terminal puede recibir la información de actualización para actualizar la lista de certificados dignos de confianza.

En un primer escenario aplicable, se recibe la información de actualización enviada por un fabricante de terminales móviles, en donde la información de actualización incluye un índice de un tercer certificado, un tercer permiso configurado en el tercer certificado y una instrucción de operación, utilizándose la instrucción de operación para suprimir o añadir el tercer permiso correspondiente al tercer certificado, y un tercer certificado ha sido establecido en la lista de certificados dignos de confianza, en donde el tercer permiso puede ser un permiso del administrador de sistemas de un sistema, o el tercer permiso puede ser también un permiso que se abre para un programa de aplicación por un desarrollador de sistemas y el fabricante de terminales móviles.

En un segundo escenario aplicable, se recibe la información de actualización enviada por un fabricante de terminales móviles, en donde la información de actualización incluye un tercer certificado y una instrucción de operación, y la instrucción de operación se utiliza para añadir el tercer certificado a, o suprimir el tercer certificado desde, la lista de certificados dignos de confianza, en donde un tercer permiso puede ser un permiso del administrador de sistemas de un sistema, o el tercer permiso puede ser también un permiso que se abre para un programa de aplicación por un desarrollador de sistemas y el fabricante de terminales móviles.

Conviene señalar que, el fabricante de terminales móviles puede enviar un mensaje de actualización a un aparato de gestión de permisos en una manera de OTA u otra manera, y el aparato de gestión de permisos recibe el mensaje de actualización en la manera OTA u otra manera; y una manera en la que el aparato de gestión de permisos obtiene el mensaje de actualización no está limitado aquí a este respecto.

Etapa 702: Actualizar la lista de certificados dignos de confianza en conformidad con la información de actualización recibida.

En esta forma de realización, correspondiente a los escenarios de aplicación de la etapa 701, la actualización de la lista de certificados dignos de confianza en conformidad con la información de actualización recibida, es concretamente que:

en el primer escenario aplicable, el terminal puede actualizar la lista de certificados dignos de confianza de conformidad con la información de actualización, con el fin de suprimir o añadir el tercer permiso correspondiente al tercer certificado; y realizar un salto operativo de la concesión o conceder el tercer permiso a un segundo programa de aplicación en conformidad con la lista de certificados dignos de confianza actualizada, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado; y

en el segundo escenario aplicable, el terminal puede actualizar la lista de certificados dignos de confianza en conformidad con la información de actualización, y saltar operativamente o conceder el tercer permiso al segundo programa de aplicación en conformidad con la lista de certificados dignos de confianza actualiza, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

La Figura 8 es un diagrama estructural esquemático de una forma de realización de un aparato de gestión de permisos en conformidad con la presente invención. Según se ilustra en la Figura 8, el aparato de gestión de permisos puede establecerse en un terminal móvil, y puede ser también establecido con independencia, en donde el aparato de gestión de permisos incluye un módulo de obtención 801, un módulo de determinación 802 y un módulo de concesión 803, en donde:

el módulo de obtención 801 está configurado para obtener un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación incluye un primer certificado e información de demanda de permiso del primer programa de aplicación;

el módulo de determinación 802 está configurado para determinar, en conformidad con la información de demanda de permiso, un primer permiso que el primer programa de aplicación requiere durante su ejecución, en donde el primer permiso es un permiso del administrador de sistemas de un sistema; y

el módulo de concesión 803 está configurado para conceder el primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación.

En esta forma de realización, se obtiene el paquete de instalación del primer programa de aplicación, en donde el paquete de instalación incluye el primer certificado y la información de demanda de permiso del primer programa de aplicación; el primer permiso que el primer programa de aplicación requiere durante su ejecución se determina en conformidad con la información de demanda de permiso; y el primer permiso se concede al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación. El primer permiso que el primer programa de aplicación requiere cuando se instala o se ejecuta se concede al primer programa de aplicación, y de este modo, puede realizarse el control de, o el acceso a, un sistema del terminal móvil por un usuario.

Conviene señalar que, el primer permiso es el permiso del administrador de sistemas del sistema. El permiso del administrador de sistemas del sistema es un permiso ROOT_PERMISSION. A modo de ejemplo, el permiso del administrador de sistemas del sistema puede utilizarse para memorizar información de audio y de vídeo e información de configuración en el sistema, ejecutar un programa de aplicación en el sistema, o funciones similares.

Sobre la base de las formas de realización anteriores, el módulo de determinación 802 está configurado específicamente para determinar si un segundo certificado está memorizado, o no, en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra en la lista de certificados dignos de confianza utilizando información de índice en el primer certificado y al menos un certificado que permite la

concesión a un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y

el módulo de concesión 803 está configurado específicamente para: si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; o si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que se abre para el primer programa de aplicación por un desarrollador de sistemas y un fabricante de terminales móviles, o solicitar a un usuario que guarde el segundo certificado en una lista de certificados dignos de confianza del usuario, y después de que el usuario guarde el segundo certificado en la lista de certificados dignos de confianza del usuario, conceder el primer permiso al primer programa de aplicación, en donde un certificado objeto de confianza por el usuario se memoriza en la lista de certificados dignos de confianza del usuario.

Además, el módulo de determinación 802 está configurado, además, para determinar si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza incluye el primer permiso; y

el módulo de concesión 803 está configurado, además, para: si se determina que la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza incluye el primer permiso, conceder el primer permiso al primer programa de aplicación; o si se determina que la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza no incluye el primer permiso, conceder el segundo permiso al primer programa de aplicación.

Sobre la base de las formas de realización anteriores, el módulo de determinación 802 está configurado, además, para determinar si un segundo certificado está memorizado, o no, en la lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra utilizando información de índice en un certificado de nivel superior del primer certificado, y al menos un certificado que permite la concesión a un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y

el módulo de concesión 803 está configurado, además, para: si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; o si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder el segundo permiso al primer programa de aplicación, en donde el segundo permiso es el permiso que se abre para el primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

Además, el módulo de determinación 802 está configurado, además, para determinar, en conformidad con el segundo certificado e información de signatura en el primer programa de aplicación, en donde el paquete de instalación del primer programa de aplicación está completo; y

el módulo de concesión 803 está configurado, además, para: si el módulo de determinación 802 determina que el paquete de instalación del primer programa de aplicación no está completo, terminar todas las operaciones; o si el módulo de determinación 802 determina que el paquete de instalación en el primer programa de aplicación está completo, conceder el primer permiso al primer programa de aplicación.

Conviene señalar que la lista de certificados dignos de confianza se coloca en el terminal móvil o en un servidor.

La Figura 9 es un diagrama estructural esquemático de otra forma de realización de un aparato de gestión de permisos en conformidad con al presente invención. Según se ilustra en la Figura 9, para el aparato de gestión de permisos, sobre la base de las formas de realización anteriores, el aparato puede incluir, además: un módulo de establecimiento 804, configurado para establecer el primer permiso en el sistema.

Sobre la base de las formas de realización anteriores, el aparato puede incluir, además: un módulo de recepción 805, configurado para recibir información de actualización enviada por un fabricante de terminales móviles, en donde la información de actualización incluye un índice de un tercer certificado, un tercer certificado configurado en el tercer certificado y una instrucción de operación, utilizándose la instrucción de operación para indicar la supresión o adición del tercer permiso correspondiente al tercer certificado, y el tercer certificado ha sido establecido en la lista de certificados dignos de confianza;

un módulo de actualización 806, configurado para suprimir o añadir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza; y

un módulo de procesamiento 807 configurado para: suprimir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza, y realizar un salto operativo de la concesión del tercer permiso a un segundo programa de aplicación; o añadir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza, y conceder el tercer permiso a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

De modo opcional, el módulo de recepción 805 está configurado para recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un tercer certificado y una instrucción de operación, y la instrucción de operación se utiliza para añadir el tercer certificado a, o suprimir el tercer certificado desde, la lista de certificados dignos de confianza;

el módulo de actualización 806 está configurado, además, para: en conformidad con la información de actualización, añadir el tercer certificado a la lista de certificados dignos de confianza, o suprimir el tercer certificado desde la lista de certificados dignos de confianza; y

el módulo de procesamiento 807 está configurado, además, para: después de que el módulo de actualización añada el tercer certificado a la lista de certificados dignos de confianza, conceder un permiso correspondiente al tercer certificado a un segundo programa de aplicación; o después de que el módulo de actualización suprima el tercer certificado desde la lista de certificados dignos de confianza, realizar un salto operativo de la concesión de un permiso correspondiente al tercer certificado para un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

Por lo tanto, si el primer permiso no está abierto, el primer permiso que el primer programa de aplicación requiere cuando se está instalando o en su ejecución, se concede al primer programa de aplicación, con lo que se asegura que el sistema sea seguro y estable.

La Figura 10 es un diagrama estructural esquemático de una forma de realización de un terminal en conformidad con la presente invención. Según se ilustra en la Figura 10, el terminal incluye: un receptor 1001, y un procesador 1002 conectado al procesador 1001, en donde:

el receptor 1001 está configurado para obtener un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación incluye un primer certificado e información de demanda de permiso del primer programa de aplicación; y

el procesador 1002 está configurado para: determinar, en conformidad con la información de demanda de permiso, un primer permiso que el primer programa de aplicación requiere cuando se está instalando o en su ejecución, en donde el primer permiso es un permiso del administrador de sistemas de un sistema; y conceder el primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación, en donde el primer certificado es un certificado para la signatura del primer programa de aplicación.

En esta forma de realización, se obtiene el paquete de instalación del primer programa de aplicación, en donde el paquete de instalación incluye el primer certificado y la información de demanda de permiso del primer programa de aplicación; el primer permiso que el primer programa de aplicación requiere cuando se está instalando o en su ejecución, se determina en conformidad con la información de demanda de permiso, en donde el primer permiso es un permiso de acceso o función del recursos del sistema que el primer programa de aplicación es incapaz de obtener, y el primer programa de aplicación es un programa de aplicación que se desarrolla por un desarrollador de aplicaciones, exceptuado un desarrollador de sistemas y un fabricante de terminales móviles; y el primer permiso se concede al primer programa de aplicación de conformidad con el primer certificado del primer programa de aplicación. El primer permiso que el primer programa de aplicación requiere cuando se está instalando o en su ejecución, se concede al primer programa de aplicación; y de este modo, puede realizarse un control de, o acceso a, un sistema de un terminal móvil por un usuario.

En esta forma de realización, el procesador 1002 está configurado específicamente para: determinar si un segundo certificado está memorizado, o no, en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra en la lista de certificados dignos de confianza utilizando información de índice en el primer certificado, al menos un identificador que permite la concesión a un programa de aplicación está memorizado en la lista de certificados dignos de confianza y el fabricante de terminales móviles configura la lista de certificados dignos de confianza; y si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; o si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder un segundo permiso al primer programa de aplicación, o solicitar al usuario que guarde el segundo certificado en una lista de certificados dignos de confianza del usuario, y después de que el usuario guarde el segundo certificado en la lista de certificados dignos de confianza del usuario, conceder el primer permiso al primer programa de aplicación, en donde un certificado objeto de confianza por el usuario se memoriza en la lista de certificados dignos de confianza del usuario y el segundo permiso es un permiso que se abre para el primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

Sobre la base de las formas de realización anteriores, el procesador 1002 está configurado, además, para: determinar si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza incluye el primer permiso; y si se determina que la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza incluye el primer permiso, conceder el primer permiso al

primer programa de aplicación; o si se determina que la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza no incluye el primer permiso, conceder el segundo permiso al primer programa de aplicación.

De modo opcional, en esta forma de realización, el procesador 1002 está configurado, además, para: determinar si un segundo certificado está memorizado, o no, en la lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra utilizando información de índice en un certificado de nivel superior del primer certificado; y si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; o si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder el segundo permiso al primer programa de aplicación.

Sobre la base de las formas de realización anteriores, el procesador 1002 está configurado, además, para: determinar, en conformidad con el segundo certificado y la información de signatura en el primer programa de aplicación, si el paquete de instalación del primer programa de aplicación está completo o no lo está; y si se determina que el paquete del primer programa de aplicación no está completo, terminar todas las operaciones; o si se determina que el paquete de instalación del primer programa de aplicación está completo, conceder el primer permiso para el primer programa de aplicación.

Además, sobre la base de las formas de realización anteriores, el procesador 1002 está configurado específicamente para: realizar un cálculo de hash sobre el primer programa de aplicación utilizando información del primer certificado del primer programa de aplicación, con el fin de obtener un primer valor de hash; y realizar un cálculo de hash sobre el primer programa de aplicación utilizando la desencriptación de clave pública registrada en el segundo certificado, con el fin de obtener un segundo valor de hash. Si el primer valor de hash es igual al segundo valor de hash, el paquete de instalación está completo; o si el primer valor de hash no es igual al segundo valor de hash, el paquete de instalación no está completo.

Sobre la base de las formas de realización anteriores, la lista de certificados dignos de confianza se coloca en un terminal móvil o en un servidor.

Sobre la base de las formas de realización anteriores, el procesador 1002 está configurado, además, para establecer el primer permiso en el sistema.

El receptor 1001 está configurado, además, para recibir información de actualización enviada por el fabricante de terminales móviles; en donde la información de actualización incluye un índice de un tercer certificado, un tercer permiso configurado en el tercer certificado, y una instrucción de operación, utilizándose la instrucción de operación para indicar la supresión o adición del tercer permiso correspondiente al tercer certificado, y el tercer certificado ha sido establecido en la lista de certificados dignos de confianza; y

el procesador 1002 está configurado, además, para suprimir o añadir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza; o

el procesador 1002 está configurado, además, para: suprimir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza, y realizar un salto operativo de la concesión del tercer permiso a un segundo programa de aplicación; o añadir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza, y conceder el tercer permiso a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

Además, el receptor 1001 está configurado, además, para recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un tercer certificado y una instrucción de operación, y la instrucción de operación se utiliza para añadir el tercer certificado a, o suprimir el tercer certificado desde, la lista de certificados dignos de confianza; y

el procesador 1002 está configurado, además, para: en conformidad con la información de actualización, añadir el tercer certificado a la lista de certificados dignos de confianza, o suprimir el tercer certificado desde la lista de certificados dignos de confianza; o

el procesador 1002 está configurado, además, para: después de que el tercer certificado se añada a la lista de certificados dignos de confianza, conceder un permiso correspondiente al tercer certificado a un segundo programa de aplicación; o después de que el tercer certificado se suprima desde la lista de certificados dignos de confianza, realizar un salto operativo de la concesión de un permiso correspondiente al tercer certificado a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

En esta forma de realización, se obtiene el paquete de instalación del primer programa de aplicación, en donde el

paquete de instalación incluye el primer certificado y la información de demanda de permiso del primer programa de aplicación; el primer premiso que el primer programa de aplicación requiere cuando se está instalando o en ejecución, se determina en conformidad con la información de demanda de permiso; y el primer permiso se concede al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación.

Los expertos en esta técnica pueden entender que la totalidad o una parte de las etapas de las formas de realización del método pueden ponerse en práctica por un programa informático que proporcione instrucciones a un hardware pertinente. El programa puede memorizarse en un soporte de memorización legible por ordenador. Cuando se ejecuta el programa, se ejecutan las etapas de las formas de realización del método. El soporte de memorización anterior incluye: cualquier soporte que pueda memorizar un código de programa, tal como una memoria ROM, una memoria RAM, un disco magnético o un disco óptico.

Por último, conviene señalar que las formas de realización anteriores están simplemente previstas para describir las soluciones técnicas de la presente invención pero no para limitar el alcance de la presente invención. Aunque la presente invención se describe en detalle haciendo referencia a las formas de realización anteriores, los expertos en esta técnica deben entender que pueden realizar todavía modificaciones a las soluciones técnicas descritas en las formas de realización anteriores o realizar sustituciones equivalentes a algunas o la totalidad de sus características técnicas, en tanto que dichas modificaciones o sustituciones no causen soluciones técnicas correspondientes que se desvíen del alcance de las soluciones técnicas de las formas de realización de la presente invención.

REIVINDICACIONES

1. Un método de gestión de permisos, que comprende:

obtener (101) un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación contiene un primer certificado e información de demanda de permiso del primer programa de aplicación;

determinar (102), en conformidad con la información de demanda de permiso, un primer permiso que el primer programa de aplicación requiere durante su ejecución, en donde el primer permiso es un permiso de administrador del sistema de un sistema; y

conceder (103) el primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación;

en donde la concesión del primer permiso al primer programa de aplicación, de conformidad con el primer certificado del primer programa de aplicación, comprende:

determinar (203, 304), si un segundo certificado se memoriza en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra en la lista de certificados dignos de confianza utilizando información de índice en el primer certificado, y al menos un certificado que permite su concesión a un programa de aplicación siendo memorizado en la lista de certificados dignos de confianza; y

si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder (205, 305) el primer permiso para el primer programa de aplicación;

si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder (207, 306) un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que es abierto para el primer programa de aplicación por un desarrollador de sistemas y un fabricante de terminales móviles.

2. El método según la reivindicación 1, después de la determinación de que el segundo certificado se memoriza en la lista de certificados dignos de confianza, que comprende, además:

determinar si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza comprende el primer permiso; y

si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza comprende el primer permiso, conceder el primer permiso al primer programa de aplicación;

si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza no comprende el primer permiso, conceder el segundo permiso al primer programa de aplicación.

3. El método según la reivindicación 1, en donde la concesión del primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación, comprende:

determinar si un segundo certificado está memorizado en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra utilizando la información de índice en un certificado de nivel superior del primer certificado, y al menos un certificado que permite la concesión a un programa de aplicación que está memorizado en la lista de certificados dignos de confianza; y si el segundo certificado está memorizado en una lista de certificados dignos de confianza, la concesión del primer permiso al primer programa de aplicación;

si el segundo certificado no está memorizado en una lista de certificados dignos de confianza, la concesión de un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que se abre al primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

4. El método según cualquiera de las reivindicaciones 1 a 3, antes de la concesión del primer permiso al primer programa de aplicación, que comprende, además:

determinar, en conformidad con el segundo certificado y la información de signatura en el primer programa de aplicación, si el paquete de instalación del primer programa de aplicación está completo, o no lo está; y

si el paquete de instalación del primer programa de aplicación no está completo, terminar todas las operaciones;

si el paquete de instalación del primer programa de aplicación está completo, conceder el primer permiso al primer programa de aplicación.

5. El método según cualquiera de las reivindicaciones 1 a 4, después de la concesión del primer permiso al primer programa de aplicación, que comprende, además:

recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un índice de un tercer certificado, un tercer permiso configurado en el tercer certificado, y una instrucción de operación, que se utiliza para suprimir o añadir el tercer permiso correspondiente al tercer certificado, y el tercer certificado se ha establecido en la lista de certificados dignos de confianza;

suprimir o añadir, en conformidad con la información de actualización, el tercer permiso que corresponde al tercer certificado en la lista de certificados dignos de confianza; y

si el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza se suprime en conformidad con la información de actualización, realizar un salto operativo de la concesión del primer permiso a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado;

si el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza se añade en conformidad con la información de actualización, conceder el tercer permiso a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

6. El método según cualquiera de las reivindicaciones 1 a 5, después de la concesión del primer permiso al primer programa de aplicación, que comprende, además:

recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un tercer certificado y una instrucción de operación, y la instrucción de operación se utiliza para añadir el tercer certificado a, o suprimir el tercer certificado desde, la lista de certificados dignos de confianza;

en conformidad con la información de actualización, añadir el tercer certificado a la lista de certificados dignos de confianza, o suprimir el tercer certificado desde la lista de certificados dignos de confianza; y

si el tercer certificado se añade a la lista de certificados dignos de confianza, conceder un permiso correspondiente al tercer certificado a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado;

si el tercer certificado se suprime de la lista de certificados dignos de confianza, realizar un salto operativo de la concesión de un permiso correspondiente al tercer certificado para un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

7. Un terminal que comprende: un receptor y un procesador conectado al receptor, en donde:

el receptor (1001) está configurado para obtener un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación incluye un primer certificado e información de demanda de permiso del primer programa de aplicación; y

el procesador (1002) está configurado para: determinar, en conformidad con la información de demanda de permiso, un primer permiso que el primer programa de aplicación requiere durante su ejecución, en donde el primer permiso es un permiso de administrador de sistemas de un sistema;

y conceder el primer permiso al primer programa de aplicación en conformidad con el primer certificado del primer programa de aplicación;

en donde el procesador está específicamente configurado para: determinar si un segundo certificado está memorizado en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra en la lista de certificados dignos de confianza utilizando una información de índice en el primer certificado, y al menos un certificado que permite que se conceda a un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que se abre para el primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

8. El terminal según la reivindicación 7, en donde el procesador está configurado, además, para: determinar si la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza comprende el primer permiso; y si se determina que la información de permiso correspondiente al segundo

certificado en la lista de certificados dignos de confianza comprende el primer permiso, conceder el primer permiso al primer programa de aplicación; si se determina que la información de permiso correspondiente al segundo certificado en la lista de certificados dignos de confianza no comprende el primer permiso, conceder el segundo permiso al primer programa de aplicación.

9. El terminal según la reivindicación 7, en donde el procesador está configurado, además, para: determinar si un segundo certificado está memorizado en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado que se encuentra utilizando información de índice en un certificado de nivel superior del primer certificado, y al menos un certificado que permite su concesión a un programa de aplicación está memorizado en la lista de certificados dignos de confianza; y si se determina que el segundo certificado está memorizado en la lista de certificados dignos de confianza, conceder el primer permiso al primer programa de aplicación; si se determina que el segundo certificado no está memorizado en la lista de certificados dignos de confianza, conceder un segundo permiso al primer programa de aplicación, en donde el segundo permiso es un permiso que se abre para el primer programa de aplicación por el desarrollador de sistemas y el fabricante de terminales móviles.

10. El terminal según la reivindicación 7, 8 o 9, en donde el procesador está configurado, además, para: determinar, en conformidad con el segundo certificado y una información de signatura en el primer programa de aplicación, si el paquete de instalación del primer programa de aplicación está completo, o no lo está; y si el módulo de determinación determina que el paquete de instalación del primer programa de aplicación no está completo, terminar todas las operaciones; si el módulo de determinación determina que el paquete de instalación del primer programa de aplicación está completo, conceder el primer permiso al primer programa de aplicación.

11. El terminal según cualquiera de las reivindicaciones 7 a 10, en donde el receptor está configurado, además, para recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un índice de un tercer certificado, un tercer permiso configurado en el tercer certificado, y una instrucción de operación, utilizándose la instrucción de operación para suprimir o añadir el tercer permiso correspondiente al tercer certificado, y el tercer certificado se ha establecido en la lista de certificados dignos de confianza; y el procesador está configurado, además, para suprimir o añadir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza;

el procesador está configurado, además, para: suprimir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza, y realizar un salto operativo de la concesión del tercer permiso a un segundo programa de aplicación; o añadir, en conformidad con la información de actualización, el tercer permiso correspondiente al tercer certificado en la lista de certificados dignos de confianza, y conceder el tercer permiso a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

12. El terminal según cualquiera de las reivindicaciones 7 a 10, en donde el receptor está configurado para recibir información de actualización enviada por el fabricante de terminales móviles, en donde la información de actualización incluye un tercer certificado y una instrucción de operación, y la instrucción de operación se utiliza para añadir el tercer certificado a, o suprimir el tercer certificado de, la lista de certificados dignos de confianza;

el procesador está configurado, además, para: en conformidad con la información de actualización, añadir el tercer certificado a la lista de certificados dignos de confianza, o suprimir el tercer certificado desde la lista de certificados dignos de confianza;

el procesador está configurado, además, para: después de que el tercer certificado se añada a la lista de certificados dignos de confianza, conceder un permiso correspondiente al tercer certificado a un segundo programa de aplicación; o bien, después de que el tercer certificado se suprima desde la lista de certificados dignos de confianza, realizar un salto operativo de la concesión de un permiso correspondiente al tercer certificado a un segundo programa de aplicación, en donde el segundo programa de aplicación es un programa de aplicación que es objeto de signatura utilizando el tercer certificado.

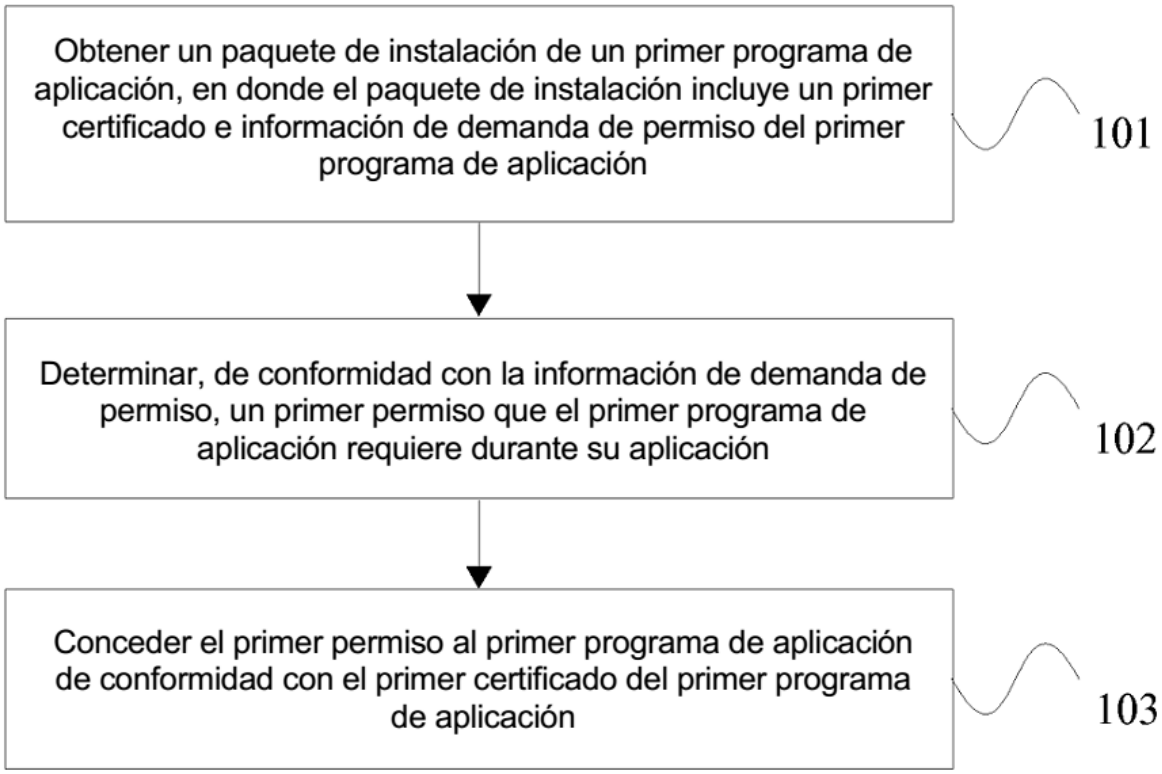
Obtener un paquete de instalación de un primer programa de aplicación, en donde el paquete de instalación incluye un primer certificado e información de demanda de permiso del primer programa de aplicación
101
Determinar, de conformidad con la información de demanda de permiso, un primer permiso que el primer programa de aplicación requiere durante su aplicación
102
Conceder el primer permiso al primer programa de aplicación de conformidad con el primer certificado del primer programa de aplicación
103

FIG. 1

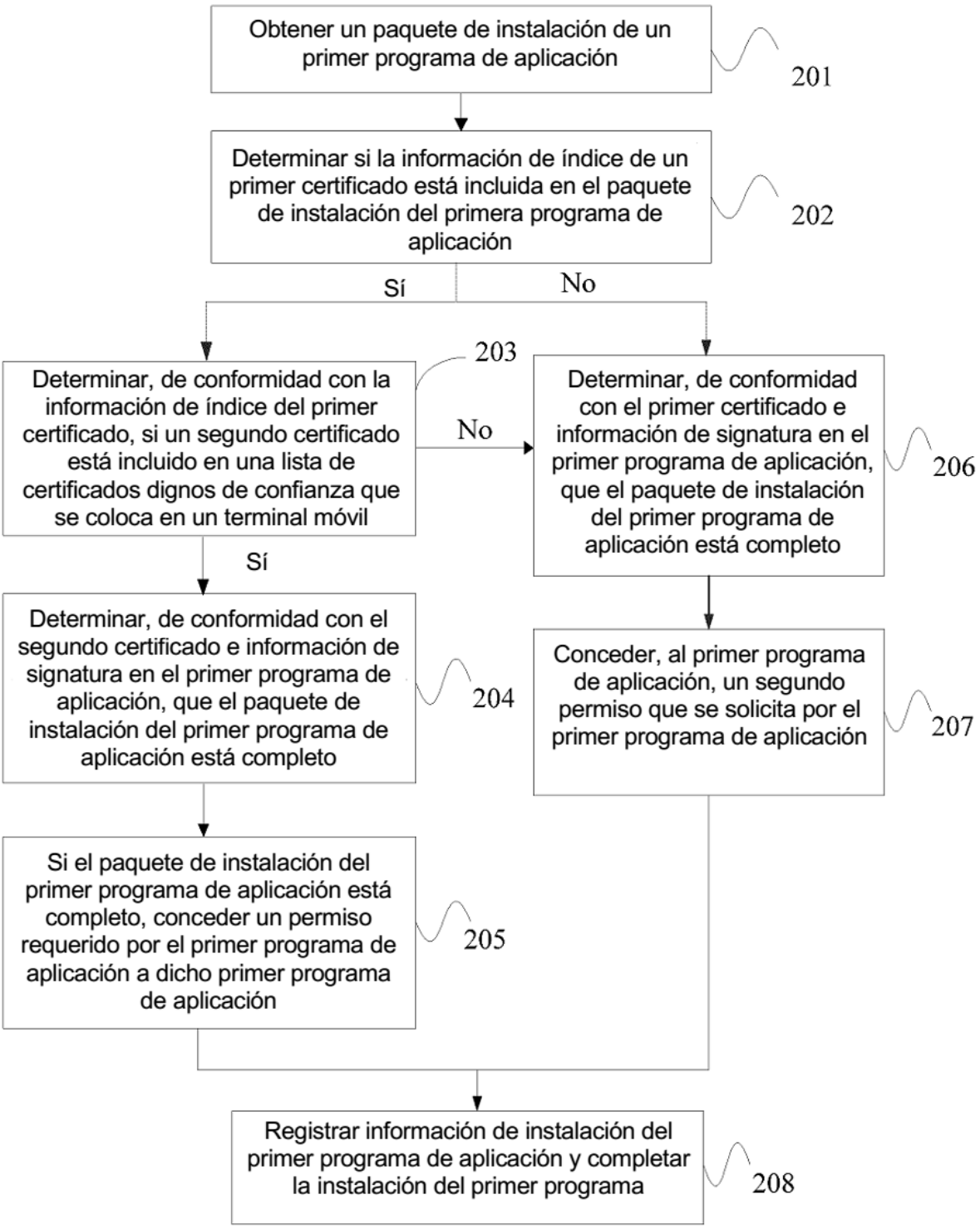
Obtener un paquete de instalación de un primer programa de aplicación
201
Determinar si la información de índice de un primer certificado está incluida en el paquete de instalación del primera programa de aplicación
202
Sí
No
203
Determinar, de conformidad con la información de índice del primer certificado, si un segundo certificado está incluido en una lista de certificados dignos de confianza que se coloca en un terminal móvil
No
Sí
Determinar, de conformidad con el primer certificado e información de signatura en el primer programa de aplicación, que el paquete de instalación del primer programa de aplicación está completo
206
Determinar, de conformidad con el segundo certificado e información de signatura en el primer programa de aplicación, que el paquete de instalación del primer programa de aplicación está completo
204
Conceder, al primer programa de aplicación, un segundo permiso que se solicita por el primer programa de aplicación
207
Si el paquete de instalación del primer programa de aplicación está completo, conceder un permiso requerido por el primer programa de aplicación a dicho primer programa de aplicación
205
Registrar información de instalación del primer programa de aplicación y completar la instalación del primer programa
208

FIG. 2

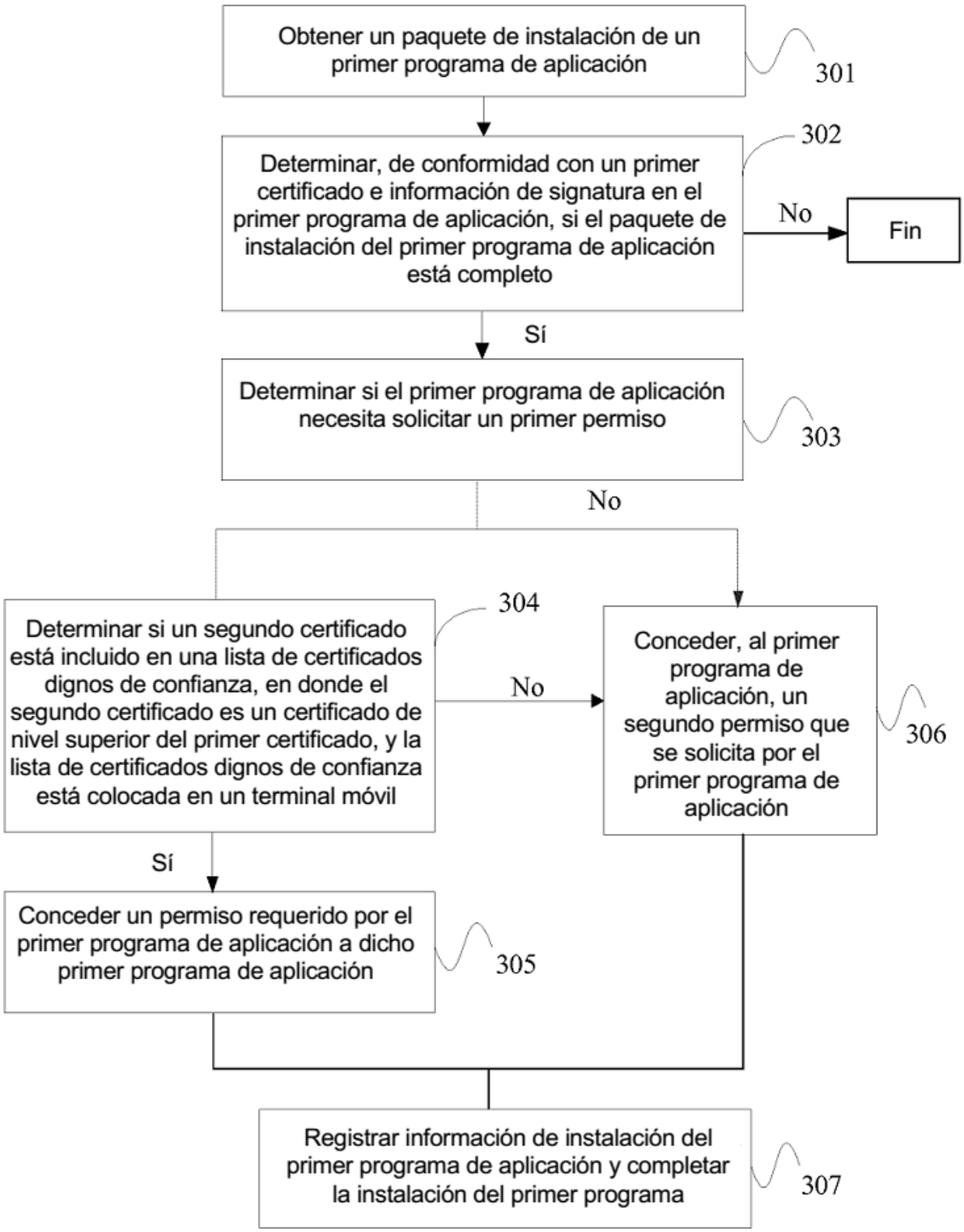
Obtener un paquete de instalación de un primer programa de aplicación
301
Determinar, de conformidad con un primer certificado e información de signatura en el primer programa de aplicación, si el paquete de instalación del primer programa de aplicación está completo
302
No
Fin
Sí
Determinar si el primer programa de aplicación necesita solicitar un primer permiso
303
No
Determinar si un segundo certificado está incluido en una lista de certificados dignos de confianza, en donde el segundo certificado es un certificado de nivel superior del primer certificado, y la lista de certificados dignos de confianza está colocada en un terminal móvil
304
No
Conceder, al primer programa de aplicación, un segundo permiso que se solicita por el primer programa de aplicación
306
Sí
Conceder un permiso requerido por el primer programa de aplicación a dicho primer programa de aplicación
305
Registrar información de instalación del primer programa de aplicación y completar la instalación del primer programa
307

FIG. 3

Número del certificado	Estado	Motivo	Tiempo de validez	Propietario del certificado
C00001	Revocado	El servicio está terminado	2/3/2013	M empresa informática
D00002	Revocado	El certificado caduca	6/4/2013	X sociedad de ciencias y tecnología

FIG. 4

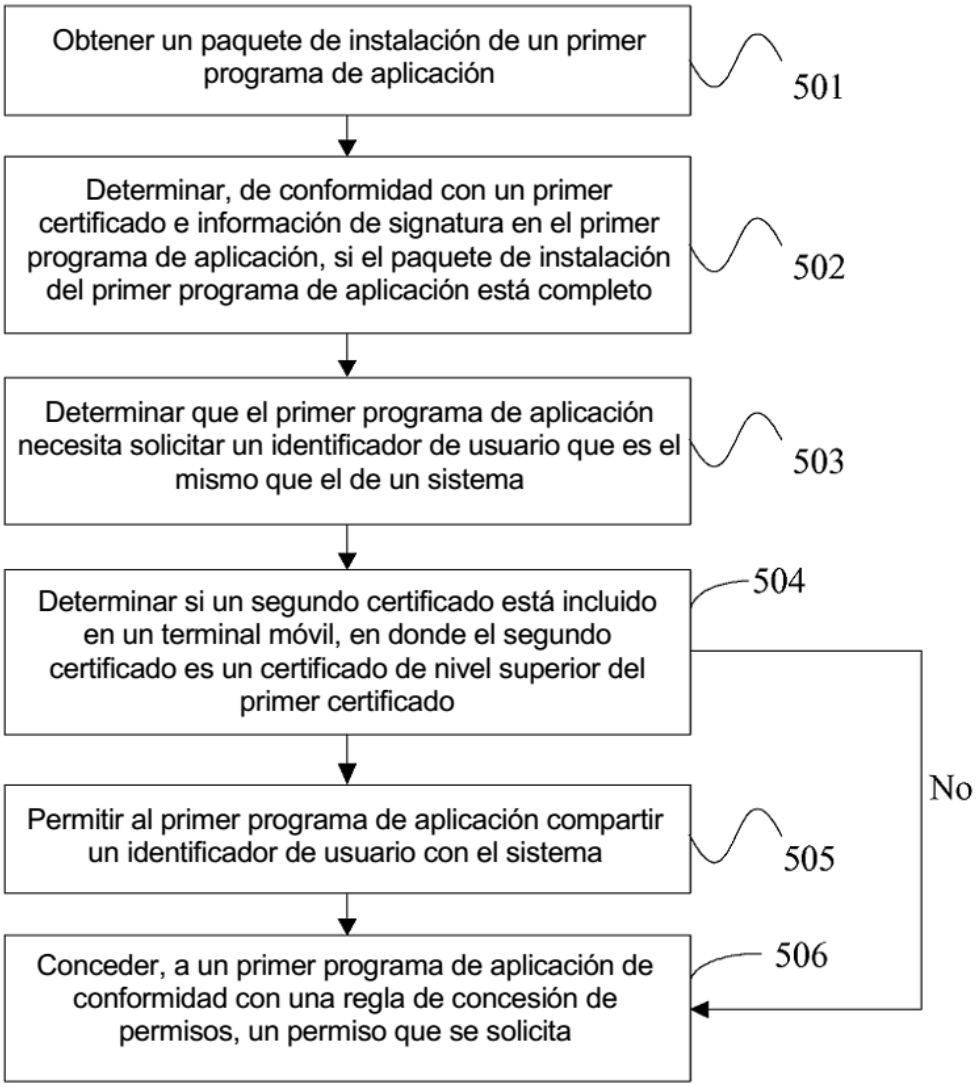

FIG. 5

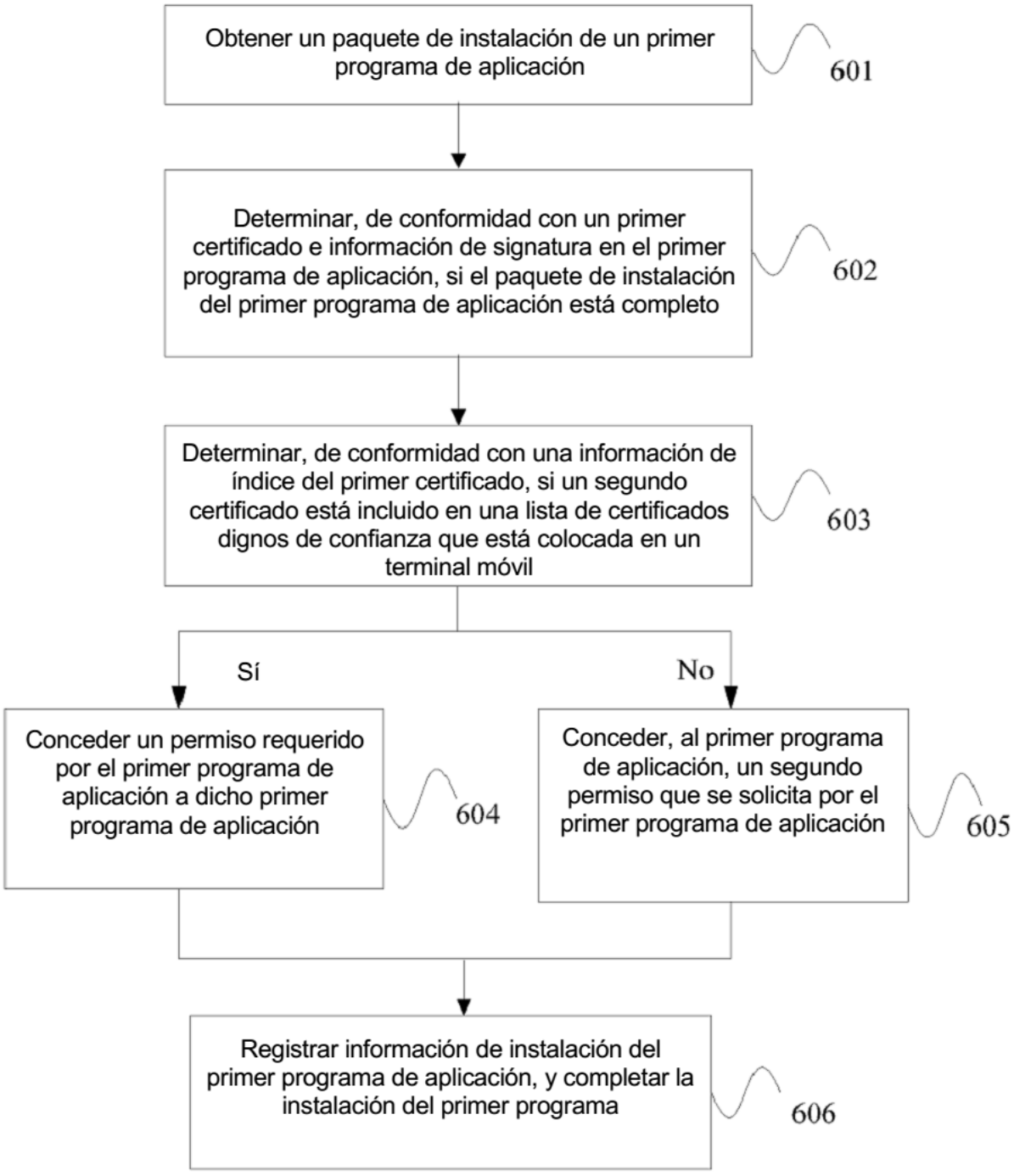
Obtener un paquete de instalación de un primer programa de aplicación
601
Determinar, de conformidad con un primer certificado e información de signatura en el primer programa de aplicación, si el paquete de instalación del primer programa de aplicación está completo
602
Determinar, de conformidad con una información de índice del primer certificado, si un segundo certificado está incluido en una lista de certificados dignos de confianza que está colocada en un terminal móvil
603
Sí
No
Conceder un permiso requerido por el primer programa de aplicación a dicho primer programa de aplicación
604
Conceder, al primer programa de aplicación, un segundo permiso que se solicita por el primer programa de aplicación
605
Registrar información de instalación del primer programa de aplicación, y completar la instalación del primer programa
606

FIG. 6

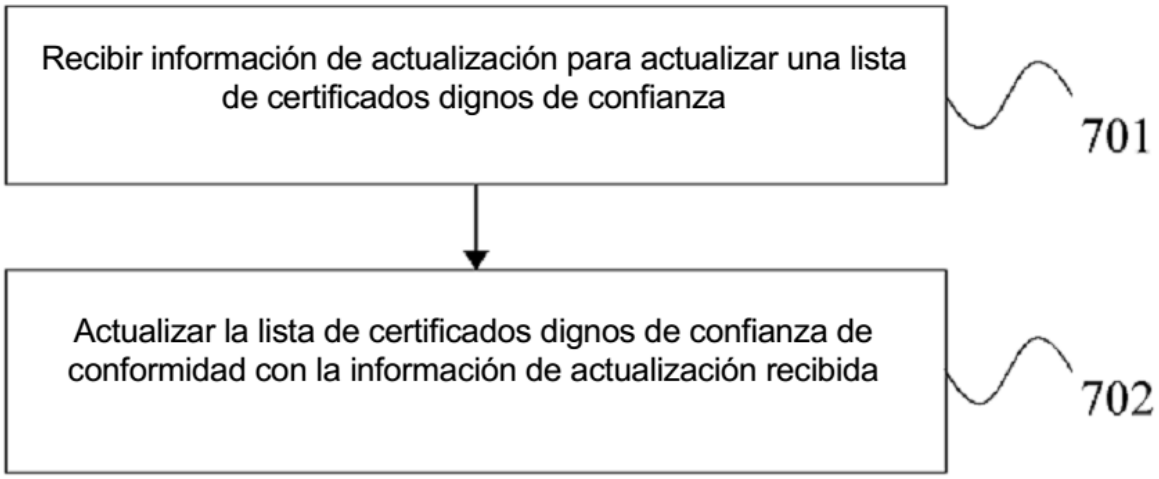
Recibir información de actualización para actualizar una lista de certificados dignos de confianza
701
Actualizar la lista de certificados dignos de confianza de conformidad con la información de actualización recibida
702

FIG. 7

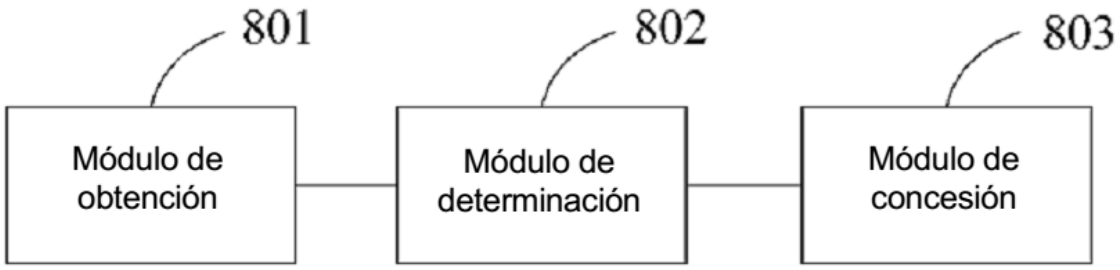
801
802
803
Módulo de obtención
Módulo de determinación
Módulo de concesión

FIG. 8

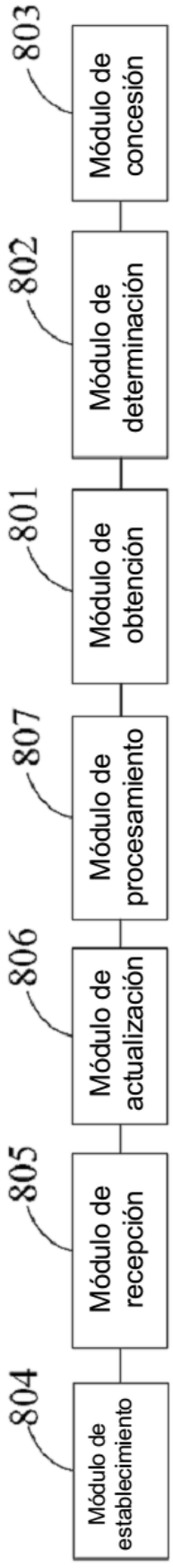
803
Módulo de concesión
802
Módulo de determinación
801
Módulo de obtención
807
Módulo de procesamiento
806
Módulo de actualización
805
Módulo de recepción
804
Módulo de establecimiento

FIG. 9

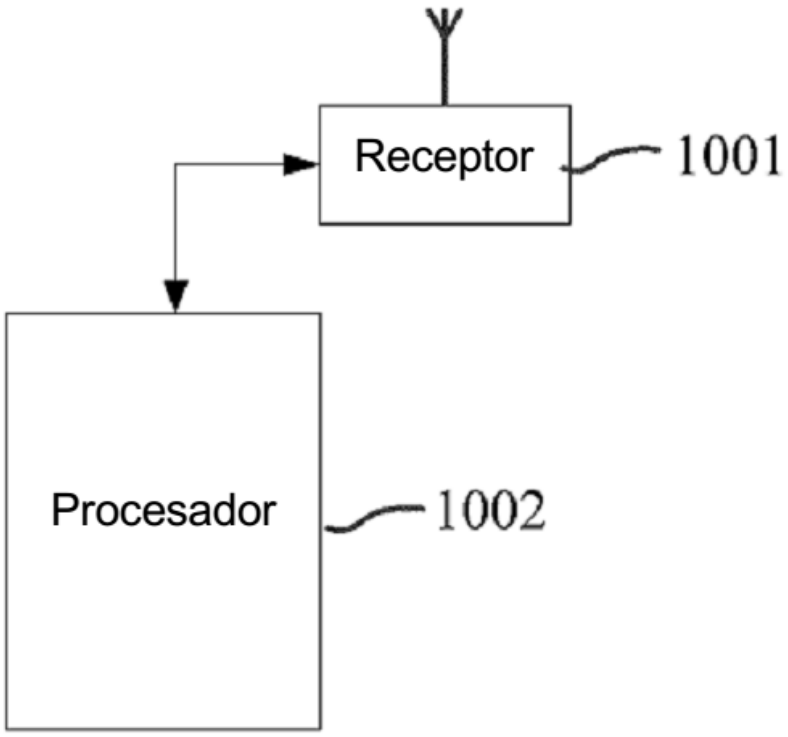

FIG. 10