(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 678 618**

(51) Int. CI.:

G06F 21/12 (2013.01)
H04W 4/00 (2008.01)
H04L 29/08 (2006.01)
H04M 1/725 (2006.01)
H04W 12/10 (2009.01)
G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.10.2013 E 13187650 (0)**

(97) Fecha y número de publicación de la concesión europea: **25.04.2018 EP 2735990**

(54) Título: **Procedimiento y dispositivo para el reconocimiento de aplicaciones en terminales móviles**

(30) Prioridad:

27.11.2012 DE 102012111481

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.08.2018

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

WANG, HAO y
MÜLLER-JUNG, MARCUS

(74) Agente/Representante:

SALVA FERRER, Joan

DESCRIPCIÓN

Procedimiento y dispositivo para el reconocimiento de aplicaciones en terminales móviles

[0001] La invención se refiere a un procedimiento y un dispositivo para el control de la instalación de aplicaciones en un terminal.

CAMPO DE LA INVENCIÓN

[0002] Los teléfonos móviles se preinstalan frecuentemente en la actualidad de forma específica con aplicaciones por los proveedores de las redes de telefonía móvil. A este respecto se pone una serie de aplicaciones en los equipos ya de antemano antes del envío a los clientes. Estas aplicaciones están orientadas con frecuencia de forma específica al proveedor de la red de telefonía móvil o están adaptadas para éste. Por consiguiente hay con frecuencia una pluralidad de versiones de aplicaciones diferentes para diferentes proveedores de telefonía móvil. Además, el proveedor de telefonía móvil da publicidad con frecuencia a productos y aplicaciones, que pueden cargar los usuarios luego en su terminal móvil, para ejecutarlas luego en éste. En todas estas aplicaciones ni el proveedor de telefonía móvil ni el fabricante del software saben con qué frecuencia se usan estas aplicaciones y si éstas se han instalado generalmente. Por consiguiente no hay mecanismos sólidos y flexibles entre el operador de una red de telefonía móvil y los desarrolladores de aplicaciones para comprender acuerdos en base al uso de las aplicaciones. En general también se instalan aplicaciones de un mercado global, según es el caso por ejemplo en iPhone (iStore/Appstore) o en teléfonos Android (Marketplace). A través de este área de descarga local con frecuencia no es posible reconocer por un proveedor qué equipos se proveen con qué aplicaciones. Lo mismo es válido para el fabricante o los programadores de la aplicación, cuyas aplicaciones se cargan a través del mercado central en los terminales móviles. Los desarrolladores de aplicaciones no tienen por consiguiente informaciones precisas sobre el número de instalaciones activas y los controladores instalados. De este modo no se pueden asegurar de forma correcta los modelos de participación en beneficios.

[0003] El documento WO 2004/114042 A2 da a conocer un procedimiento en el que en un terminal móvil se deposita una lista de aplicaciones activadas por el usuario que debe realizar el usuario.

[0004] El documento EP 2 337 307 A2 da a conocer el estado de aplicación de un servicio de comunicaciones y libera el servicio si se permite un acceso a través de un servidor. Por consiguiente se da una elevada importancia a la transmisión segura de las informaciones de acceso.

[0005] El documento US 2012 129503 A1 describe un sistema para la distribución del software en una red con sistemas móviles, que se basa en reglas.

[0006] El documento US 2009/061840 A1 describe la configuración de un teléfono, que comprende una pila de software, ajustes de hardware en base a las informaciones de un operador de red. La configuración se examina a este respecto por un servidor.

RESUMEN DE LA INVENCIÓN

[0007] El objetivo de la presente invención es la facilitación de un procedimiento según la reivindicación 1 y las reivindicaciones dependientes 2-8 y de un sistema según la reivindicación 9, en el que se pueda asegurar qué aplicaciones están preajustadas o preinstaladas para equipos móviles de un fabricante en un proveedor y qué aplicaciones se soportan por el proveedor.

[0008] En detalle se trata de un procedimiento para el control de la instalación de aplicaciones en un terminal móvil. En el caso de estos terminales se trata preferentemente de un teléfono Android o un teléfono inteligente que dispone de una interfaz de red con una red IP. Estos teléfonos inteligentes están configurados en general con un firmware cuya configuración se puede fijar por el proveedor de la red. En este firmware ya estará instalado un proveedor de tókenes al envío a los clientes finales. El proveedor de tókenes ya está configurado de modo que conoce la dirección de red de un servidor de tókenes. El servidor de tókenes se proporciona por el proveedor de red a través de una red (red IP), a fin de facilitar una pluralidad de tókenes para la descarga. Los tókenes indican qué aplicaciones se soportan por el proveedor de red. A este respecto, la facilitación de los tókenes depende de forma específica de la tarjeta SIM instalada y/o de la versión del sistema operativo. Igualmente son concebibles otros parámetros y se describen abajo. Mediante este enfoque es posible que el proveedor de la red pueda fijar que aplicaciones se soportan por él en el terminal móvil. Mediante es enfoque es posible igualmente reconocer para la

aplicación que se ejecuta en el terminal móvil si la aplicación se soporta o no por el proveedor de red. La aplicación, que está instalada en el terminal móvil o se instala por el usuario, puede acceder al proveedor de tókenes a través de una interfaz fijada de antemano. Esta interfaz puede ser una API u otra interfaz cualquiera que sea concebible para la comunicación de dos aplicaciones (XML, TCP/IP sockets etc.). Esta interfaz se tiene en cuenta de antemano en la programación de la aplicación y en general es parte del código de programa de la aplicación que está instalada en el terminal móvil. En general la aplicación presenta otra interfaz que se comunica con un servidor de aplicaciones, que en general se facilita por el desarrollador de la aplicación. Este servidor también se puede operar sin embargo por proveedores de red, de modo que igualmente el proveedor de red llega al conocimiento por ello de cuando una aplicación consulta un token en el proveedor de tókenes. No obstante, en general el token sirve para la verificación de la ejecución de aplicaciones y el soporte de las aplicaciones para el desarrollador de la aplicación. El servidor de aplicaciones obtiene en general informaciones durante el arranque de la aplicación o durante determinados procesos dentro de la aplicación. El token también se puede consultar durante la primera instalación de la aplicación.

[0009] El procedimiento comprende además las etapas:

- descarga de los tókenes específicos para el terminal móvil del servidor de tókenes a través del proveedor de tókenes y
- almacenamiento de estos tókenes en un espacio de almacenamiento de tókenes en el terminal móvil;
- arranque de la aplicación, en donde la aplicación pregunta en el proveedor de tókenes por un token para la aplicación a través de la interfaz, y
- si se proporciona el token, entonces se realiza una notificación al servidor de tókenes.

[0010] El proveedor de tókenes trabaja a este respecto junto con el servidor de tókenes, en tanto que descarga los tókenes a intervalos regulares temporalmente y los almacena localmente. Esto tiene la ventaja de que los token también están presentes localmente cuando no hay una conexión de red. Los tókenes se pueden colocar delante localmente y llamar por las aplicaciones a través del proveedor de tókenes. En una forma de realización preferida, los tókenes se depositan en un espacio de almacenamiento de tókenes en el terminal móvil, que está encriptado. La encriptación se consigue mediante procedimientos conocidos, en particular esto se puede realizar por un módulo criptográfico integrado o a través de la tarjeta SIM. Naturalmente es concebible que en aparatos que están permanentemente online se pueda evitar un almacenamiento local. El almacenamiento también puede estar configurado de modo que los tókenes sólo se ponen en caché y no se descarga toda una lista de tókenes, sino sólo los token que se necesitan por una aplicación o por una aplicación que está instalada en el terminal móvil.

[0011] El arranque de la aplicación puede contener diferentes funciones. Por un lado, durante el primer arranque se puede realizar una consulta del token o durante el desarrollo del programa siempre se puede realizar de nuevo una consulta del token. También es posible una consulta durante el arranque de una función determinada. Además, es concebible que el token sólo se consulte durante este proceso de instalación. La consulta del token está en la mano del desarrollador de la aplicación, para que éste pueda determinar el instante óptimo para él de la consulta. El desarrollador usa en general una interfaz definida que puede estar definida, por ejemplo, a través de una llamada de función o una API.

[0012] En una forma de realización preferida, la aplicación se configura en base al token obtenido. La configuración puede comprender que se usen representaciones gráficas determinadas o representaciones e indicaciones de marcas de los operadores de red o proveedores de red. Además, se pueden liberar funciones especiales en función del token. También es posible desactivar determinadas funciones.

[0013] El token comprende en general componentes que se conocen del encriptado y técnica de firma. Así por ejemplo es concebible una clave pública y privada que entra en el token. Por consiguiente puede estar contenida, por ejemplo, una información en el elemento de token que se ha encriptado por la clave pública de la aplicación o de la empresa que ha desarrollado la aplicación. La aplicación misma puede verificar entonces el token en base a la clave privada implementada. En una forma de realización alternativa, la aplicación transfiere el token al servidor del desarrollador de la aplicación o lo transfiere al servidor de aplicaciones que verifica entonces el token. De este modo se puede evitar que la clave privada esté contenida en la aplicación misma. Después de que se ha realizado la confirmación del token, entonces se efectúa un procesamiento por parte de la aplicación.

[0014] Junto a un certificado y/o una clave pública de la aplicación, el token comprende preferentemente una identificación para la aplicación, pudiendo ser la identificación de la aplicación el nombre de paquete de la aplicación.

[0015] En una forma de realización posible se descarga y almacena una cantidad de tókenes por el

proveedor de tókenes regularmente desde el servidor de tókenes. La selección de los tókenes o la asociación de los tókenes al terminal móvil se puede basar en diferentes criterios de filtrado. En general determinados tókenes sólo se pueden utilizar para determinados teléfonos de determinados fabricantes teniendo en cuenta determinados proveedores. En el caso de una consulta del proveedor de tókenes en el servidor de tókenes, los tókenes se facilitarán en base a una o varias de las siguientes informaciones: informaciones SIM, tipo de terminal, tipo de sistema operativo, versión del sistema operativo, tiempo de ejecución del token. Naturalmente también son concebibles otros criterios, como el tipo de contrato de telefonía móvil, la prestación del teléfono móvil, etc.

[0016] En la forma de realización preferida, los componentes como servidor de aplicaciones y servidor de tókenes se sitúan en una red IP (Internet), que se puede consultar a través de los servicios DNS conocidos. Por consiguiente el proveedor de tókenes puede gestionar, por ejemplo, un nombre de dominio fijo o igualmente una dirección IP fija, a fin de acceder al servidor de tókenes. Igualmente es concebible que se usen determinadas áreas reservadas de la dirección que se gestionan por el proveedor de red. Los servidores de tókenes y servidores de aplicaciones trabajan en general en sistemas informáticos conocidos, que están equipados con sistemas operativos correspondientes como Linux, Windows o Unix, a fin de proporcionar el servicio correspondiente en la red. En general se usan protocolos de red, según se conocen de una red basada en IP.

[0017] Otra parte de la invención son los componentes individuales que implementan el procedimiento. Un proveedor de tókenes, un servidor de tókenes y un servidor de aplicaciones, que están instalados y configurados para realizar el procedimiento según una o varias de las reivindicaciones 1 a 10. Según se ha expuesto ya arriba, el proveedor de tókenes es preferentemente una parte del firmware o una aplicación que está preinstalada en el firmware del terminal móvil cuando se le envía al cliente final. El servidor de tókenes es un sistema informático que proporciona una base de datos en la que están depositados la pluralidad de tókenes. A este respecto, la base de datos puede ser una base de datos relacional o una base de datos orientada al objetivo o cualquier otro tipo de base de datos. En el sistema informático se ejecuta en general un sistema operativo conocido, según se ha expuesto arriba. En otra forma de realización, el acceso al servidor de tókenes sólo es posible a través de terminales móviles que se sitúan en la red del proveedor de red. Es decir, en general se realiza un enmascaramiento mediante las direcciones de red o un enmascaramiento mediante la identificación del terminal móvil. El servidor de aplicaciones es en general un sistema que gestiona igualmente una base de datos o servicio web al que pueden acceder los terminales móviles y las aplicaciones.

BREVE DESCRIPCIÓN DE LAS FIGURAS

[0018] A continuación se describen las figuras que representan una implementación posible de la invención, no debiéndose interpretar las figuras como una limitación.

La fig. 1 muestra un diagrama de desarrollo del procedimiento;
la fig. 2 muestra un ejemplo de una estructura de dos tókenes;
la fig. 3 muestra un código de ejemplo para la implementación de la consulta de un token.

DESCRIPCIÓN DETALLADA DE LAS FIGURAS

[0019] La figura 1 muestra los diferentes componentes que se tienen en cuenta en la presente invención. En primer lugar el servidor de tókenes, que está en contacto con el proveedor de tókenes. El proveedor de tókenes consulta una lista de tókenes del servidor de tókenes. Esta consulta se puede realizar, por ejemplo, a través del protocolo HTTPS que está encriptado correspondientemente. El servidor de tókenes devuelve entonces en base a la consulta una lista de tókenes también a través del mismo tipo de encriptado HTTPS, que son específicos para el terminal móvil. En este caso se debe atender a que el proveedor de tókenes se ejecuta en el terminal móvil y el servidor de tókenes se alcanza por el terminal móvil a través de una red. Además, se ejecuta una aplicación, una así denominada socio APP, en el terminal móvil, que en el curso de su tratamiento envía una consulta (solicitud URI) de un token al proveedor de tókenes. Esta consulta se verifica por el proveedor de tókenes de si está permitida en su tipo, a fin de devolver entonces un token en el caso de la procedencia. En la consulta de la procedencia se examina si un token permitido se corresponde con las propiedades de la aplicación y su fecha de vencimiento todavía no ha expirado. En una forma de realización posible, después de la entrega del token a la aplicación se envía una notificación correspondiente al servidor de tókenes, para que esté tenga conocimiento de que el token se ha consultado por una aplicación. La aplicación verifica entonces el token de forma local; según está representado en la figura 1, pero también puede dejar que se realice una verificación a través del servidor de aplicaciones (servidor asociado), lo que no está representado. Acto seguido se activa la aplicación correspondiente y se le notifica al servidor de aplicaciones que está presente una instalación activa en el terminal móvil. Como una instalación activa

se considera una aplicación que también se usa realmente por el usuario y no sólo está instalada en este equipo. Si la consulta no fuese admisible, según se puede reconocer en la figura 1 por debajo de la línea a trazos, entonces no se transmite un token a la aplicación.

[0020] La figura 2 muestra un ejemplo de una lista de tókenes. En este caso en la representación se trata de una lista de dos tókenes, que se transmite dentro de datos XML. En primer lugar la lista de los tókenes se abre mediante <apptoken>, identificándose entonces un token a través de una ID, en el presente caso 1 y 2, además se define el nombre para tener entonces además un campo de token a partir del que se ve que para el token existe una aprobación entre el proveedor de la red y del suministrador de la aplicación. En otro campo se define el tiempo de ejecución del token. Si se realizase por ejemplo una determinada campaña publicitaria, para la que el proveedor de red pone publicidad durante un determinado intervalo de tiempo, entonces el token se debe activar durante este intervalo de tiempo a fin de poder reconocer cuánto éxito tiene una promoción semejante (puesta de publicidad) de una aplicación en el intervalo de tiempo de la promoción. El certificado mismo es en general una clave pública o una firma con una clave pública, que se puede verificar correspondientemente por la aplicación. El segundo token en la lista está construido correspondientemente en paralelo, de modo que no es necesario para ello una información detallada.

La figura 3 muestra la implementación de un código Java para una aplicación. En una primera etapa se define la dirección unívoca del proveedor de tókenes, a fin de definir el token que se busca por la aplicación. Acto seguido se transfiere el token a una función que proporciona un cursor C. Entonces se realiza una verificación del token. Si esto es admisible se realiza un informe de que se ha realizado una verificación correcta del token. En caso negativo se emite una notificación correspondiente de que la búsqueda del token no fue satisfactoria.

REIVINDICACIONES

1. Procedimiento para el control de la configuración de aplicaciones en un terminal móvil, con un proveedor de tókenes, que está instalado en el terminal móvil y que conoce la dirección de red de un servidor de tókenes, en donde el servidor de tókenes se proporciona por el proveedor de red a través de una red a fin de proporcionar una pluralidad de tókenes para la descarga, en donde los tókenes muestran qué aplicaciones se soportan por el proveedor de red, y en donde un token semejante comprende un certificado y/o una clave pública de la aplicación y una identificación para la aplicación, con una aplicación que está instalada en el terminal móvil, en donde las aplicaciones acceden al proveedor de tókenes a través de una interfaz, además que comprende un servidor de aplicaciones que contiene informaciones de la aplicación, que comprende las etapas:

- descarga de los tókenes específicos para el terminal móvil del servidor de tókenes a través del proveedor de tókenes y
- almacenamiento de estos tókenes en un espacio de almacenamiento de tókenes en el terminal móvil;
- arranque de la aplicación, en donde la aplicación pregunta en el proveedor de tókenes por un token para la aplicación a través de la interfaz, y
- si se proporciona el token, se realiza una verificación del token por parte de la aplicación misma o el token se envía a través de la aplicación al servidor de aplicaciones, que verifica de forma alternativa el token, después del examen se realiza una activación correspondiente de la aplicación, en donde la verificación se realiza a través del examen del certificado y/o de la clave pública y se le notifica al servidor de aplicaciones que está presente una instalación activa en el terminal móvil.

2. El procedimiento según la reivindicación anterior, en donde la aplicación se configura en base al token obtenido.

3. El procedimiento según la reivindicación anterior, en donde la aplicación libera funciones en base al token obtenido.

4. El procedimiento según la reivindicación anterior, en donde la identificación de la aplicación es un nombre de paquete de la aplicación.

5. El procedimiento según una de las aplicaciones anteriores, en donde los tókenes, que se han descargado por el proveedor de tókenes, se depositan en una zona de almacenamiento segura.

6. El procedimiento según una de las aplicaciones anteriores, en donde una cantidad de los tókenes se descargan y almacenan regularmente por el proveedor de tókenes del servidor de tókenes.

7. El procedimiento según una de las aplicaciones anteriores, en donde en el caso de una consulta del proveedor de tókenes en el servidor de tókenes, los tókenes se facilitan en base a una o varias de las informaciones siguientes: informaciones SIM, tipo de terminal, tipo de sistema operativo, versión de sistema operativo, tiempo de ejecución del token.

8. El procedimiento según una de las aplicaciones anteriores, en donde el servidor de tókenes y/o el servidor de aplicaciones son accesibles a través de una red IP.

9. Sistema para el control de la instalaciones de aplicaciones en un terminal móvil, **caracterizado por** un proveedor de tókenes, un servidor de tókenes y un servidor de aplicaciones, que están instalados y configurados para realizar el procedimiento según una o varias de las reivindicaciones 1 a 8.

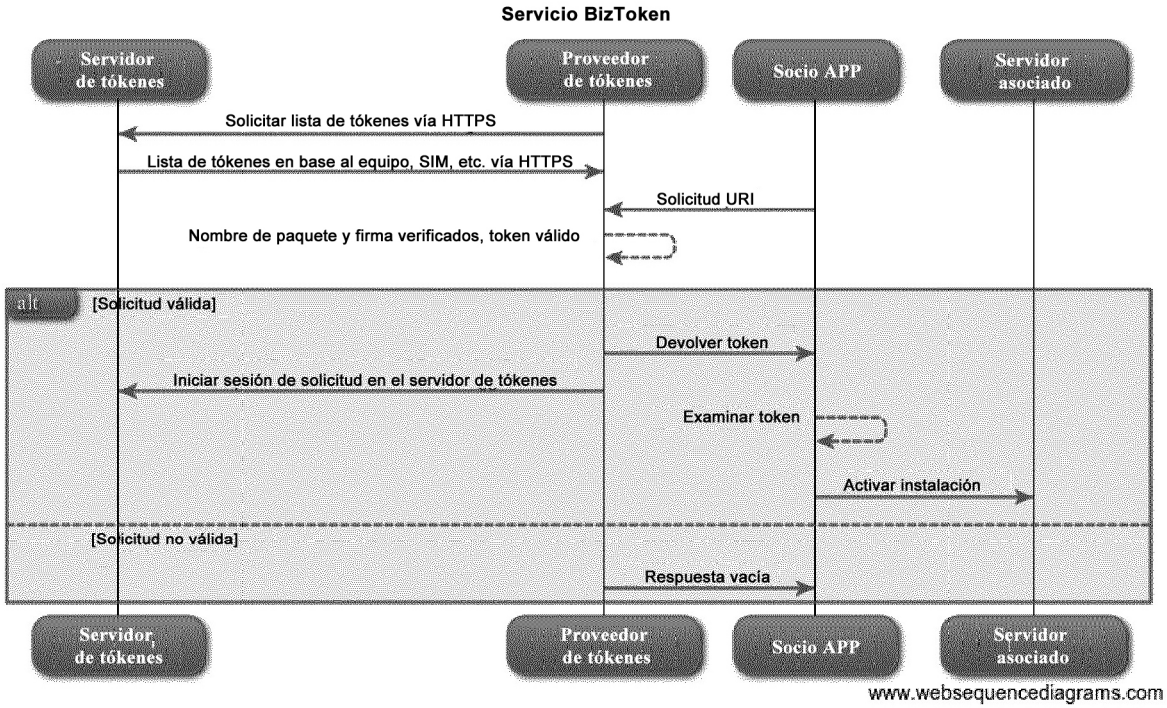
Servicio BizToken
Servidor de tókenes
Proveedor de tókenes
Socio APP
Servidor asociado
Solicitar lista de tókenes vía HTTPS
Lista de tókenes en base al equipo, SIM, etc. vía HTTPS
Solicitud URI
Nombre de paquete y firma verificados, token válido
alt
[Solicitud válida]
Devolver token
Iniciar sesión de solicitud en el servidor de tókenes
Examinar token
Activar instalación
[Solicitud no válida]
Respuesta vacía
Servidor de tókenes
Proveedor de tókenes
Socio APP
Servidor asociado
www.websequencediagrams.com

Fig. 1

- <?xml version="1.0" encoding="utf-8"?>
- <apptoken>
  - <app id="1" name="com.android.hao.BizToken" token="jkuiy9"
  - expireDate="20/01/2012 15:00:00"
    cert="831481b1ed42e2a201349fa6e6c0e4264ccccc264c1cad7ed27d923c708a269d9d717700aa3
    879ef37929ff8f6e0f58d028404bce3d44c4441a20800dd549ca4a4b2c4a2f67bd0430ca44ff3cf4ca5
    a8a22e7679bb9417983088f532f93cc1d202abc09545752d8a9da03b40e2f9925c05ca470c1f3909f4
    f6cb7693dd8e590f"/>
  - <app id="2" name="com.android.hao.BizTokenReader" token="ui87ko"
    expireDate="20/06/2012 15:00:00"
    cert="831481b1ed42e2a201349fa6e6c0e4264ccccc264c1cad7ed27d923c708a269d9d717700aa3
    879ef37929ff8f6e0f58d028404bce3d44c4441a20800dd549ca4a4b2c4a2f67bd0430ca44ff3cf4ca5
    a8a22e7679bb9417983088f532f93cc1d202abc09545752d8a9da03b40e2f9925c05ca470c1f3909f4
    f6cb7693dd8e590f"/>
- </apptoken>

Fig. 2

```
private static Uri tokens =
Uri.parse("content://com.android.hao.biztoken.tokencontentprovider");
boolean isTokenValid = false;
try {
    Cursor c = managedQuery(tokens, null, null, null, null);
    if(c.moveToFirst())
    {
        isTokenValid = compareToken(c.getString(c.getColumnIndex("token")));
    }
}catch (Exception e) {
    // TODO Auto-generated catch block
    Log.d("TokenReader", "query failed!");
}

if(isTokenValid)
{
    //Report a successful installation or transaction
}
```

Fig. 3