(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 558 613**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04W 4/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.03.2013 E 13158834 (5)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 2779580**

(54) Título: **Procedimiento y dispositivo para la instalación de aplicaciones en terminales móviles**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.02.2016

(73) Titular/es:

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

(72) Inventor/es:

WANG, HAO y
BURKERT, STEFAN

(74) Agente/Representante:

MORGADES MANONELLES, Juan Antonio

DESCRIPCIÓN

Procedimiento y dispositivo para la instalación de aplicaciones en terminales móviles

La invención se refiere a un procedimiento y un dispositivo para el control de la instalación de aplicaciones en un terminal móvil. En especial, la invención se refiere a un procedimiento para la instalación de aplicaciones pre-instaladas en terminales móviles.

Sector de la invención

Los teléfonos móviles son preconfigurados en la actualidad de modo muy frecuente por el proveedor de la red de móviles con aplicaciones específicas. En esta situación, una serie de aplicaciones son introducidas en los aparatos de manera previa al suministro a los clientes. Se dan a conocer ejemplos de ello en los documentos US 2012129503 y EP 2523107.

Estas aplicaciones están frecuentemente orientadas al proveedor de la red de móviles o son adecuadas para el mismo. Se tienen, por lo tanto, frecuentemente, múltiples versiones de diferentes aplicaciones para diferentes proveedores de móviles. Además, los proveedores de móviles publicitan frecuentemente productos y aplicaciones que los usuarios pueden cargar en un terminal móvil utilizando los mismos. Para la totalidad de estas aplicaciones no conoce ni el proveedor del aparato móvil ni el fabricante del Sofware la frecuencia en que estas aplicaciones serán utilizadas y si estas llegaran a ser instaladas. Por lo tanto, no existe ningún mecanismo sólido y flexible entre el que explota una red de teléfonos móviles y los que desarrollan las aplicaciones para llevar a cabo adecuaciones sobre la base de la utilización de las aplicaciones. Habitualmente, las aplicaciones son instaladas también por alguna firma global, tal como ocurre, por ejemplo, en iPhone (App Store) o en teléfonos Android (Google Play Store). Mediante esta descarga centralizada no resulta posible, frecuentemente, para un proveedor saber qué aparatos se deben dotar de determinadas aplicaciones. Lo mismo ocurre para el fabricante o el programador de las aplicaciones, cuyas aplicaciones han sido cargadas por la entidad central a los terminales móviles. Los desarrolladores de las instalaciones carecen, por lo tanto, de informaciones precisas sobre el número de instalaciones activas y de los usuarios instalados. Por lo tanto, no se pueden determinar modelos de distribución de la producción de manera razonable. En el momento del primer suministro se debe conocer qué instalaciones deben ser pre-instaladas en un terminal móvil. Dado que el firmware necesario difícilmente cambia a lo largo de todo el ciclo de producción porque debe ser sometido a engorrosas pruebas, las aplicaciones pre-instaladas corresponden, frecuentemente a lo largo del ciclo del producto en su conjunto, a las que se han instalado en los primeros suministros. Además, se debe tener en cuenta que los programas para la determinación del firmware o bien en la constitución y configuración del terminal móvil, deben ser conocidos. Las aplicaciones que deben ser instaladas más adelante en el ciclo del producto en el terminal móvil no pueden ser, por lo tanto, tenidas en cuenta. Se impide, por lo tanto, una utilización dinámica, puesto que las aplicaciones deben ser conocidas en la configuración del terminal móvil por parte del fabricante. Por lo tanto, los cambios en el curso de ciclo del producto son posibles solamente de forma difícil y no se pueden introducir por el proveedor de la red, ya que no tiene acceso, o tiene solamente un acceso limitado, al firmware.

Resumen de la invención

Es un objetivo de la presente invención, la preparación de un procedimiento/dispositivo con el que se pueda asegurar que las aplicaciones previamente instaladas se pueden instalar de forma dinámica y, por lo tanto, el proveedor de la red tiene la posibilidad de determinar las aplicaciones previamente instaladas.

Este procedimiento se define por las características de las reivindicaciones. En particular, se trata de un procedimiento para el control de la instalación de aplicaciones en un terminal móvil con un dispositivo instalador que está instalado en el terminal móvil, o bien, que está integrado en el sistema operativo del terminal móvil, de manera que la instalación tiene lugar básicamente de modo “silencioso” sin actuación del usuario y que conoce la dirección de red de un servidor, de manera que el servidor del proveedor de red puede ser preparado con intermedio de una red para preparar una lista de aplicaciones permisibles, de manera que la lista comprende certificados para cada aplicación y sus nombres, en base a los cuales se puede determinar, de manera inequívoca, si la aplicación está autorizada para la instalación de otras aplicaciones en el terminal móvil. Es decir, la lista se refiere a las aplicaciones que debe requerir el dispositivo instalador (en la forma de realización descrita, solamente el “asistente”) comprendiendo además un asistente, que funciona como aplicación en el terminal móvil, y que conoce la dirección del servidor, para conseguir de éste una lista con las aplicaciones a instalar, comprendiendo el procedimiento las siguientes etapas:

- Descarga por el dispositivo instalador de una lista de aplicaciones autorizadas y almacenamiento de esta lista en el terminal móvil, de manera que la lista contiene los nombres y certificados de las aplicaciones autorizadas;
- Descarga a través del asistente del servidor de una lista de las aplicaciones a instalar, preferentemente, en el inicio de funcionamiento del terminal móvil por el cliente final, de manera que la lista comprende el lugar de almacenamiento de las aplicaciones;

- Descarga a través del asistente de las aplicaciones de la red como paquete de instalación, para introducir éstas como paquete de instalación en el terminal móvil;
- Transferencia del lugar de almacenamiento del paquete de instalación a través del asistente al dispositivo instalador;
- Comprobación del dispositivo instalador con ayuda de los certificados y de los nombres de las aplicaciones permisibles de la lista, determinando si el asistente está autorizado para determinar qué aplicaciones se deben instalar y en caso de que la comprobación es satisfactoria, instalar la aplicación sin actuación por parte del usuario.

De manera específica, se trata de un procedimiento para el control de la instalación de aplicaciones en un terminal móvil. En estos terminales se trata, preferentemente, de un teléfono Android u otro ”teléfono inteligente”, que dispone un IP de red a través de un interfaz de red. Estos “teléfonos inteligentes” están dotados habitualmente de un firmware, cuyas configuraciones pueden ser determinadas por el proveedor de la red. En éstos firmware se habrá instalado, ya en el suministro al cliente final, un dispositivo instalador o “instalador”. El instalador tiene la misión de instalar aplicaciones, cuando éstas han sido preparadas y son fiables. El dispositivo instalador está constituido en una forma de realización preferente, de manera que instala aplicaciones en el aparato básicamente sin interacción con el usuario. Adicionalmente, comprueba el dispositivo instalador si el asistente presenta un nombre permitido y/o certificado permitido. Mediante una comprobación de seguridad de este tipo se garantiza que solamente se instalarán aplicaciones a un asistente autorizado, o bien el asistente autorizado llama al dispositivo instalador para la instalación de aplicaciones. Mediante dicha comprobación se asegurará que el dispositivo instalador no solicita ninguna aplicación no permisible (Malware) y, por lo tanto, que no puede instalar eventuales aplicaciones sin conocimiento y autorización del usuario. La lista con los nombres y los certificados, que muestran de manera correspondiente los programas autorizados, pueden ser descargados a través del dispositivo instalador desde un servidor. La descarga tiene lugar en una forma de realización preferente, a través de un protocolo de internet estándar (IP) a través de mecanismos de transferencia seguros tales como HTTP PS o GLS. El dispositivo instalador es, preferentemente, una aplicación que es un componente integral del sistema operativo y que el instalador estándar amplia el que se utilizada en este caso, por ejemplo, por el terminal (Mercado) o bien Play Store. El dispositivo instalador presenta una funcionalidad propia y permite la instalación de aplicaciones en el sistema operativo de manera autónoma. Por lo tanto, antes de que se instale una aplicación o bien una App binaria, que ha sido cargada en el aparato, tiene lugar una comprobación del asistente que quiere instalar esta aplicación. La comprobación tiene lugar sobre la base de firmas o valores Hash y, preferentemente, el nombre del paquete de la aplicación o bien la propia aplicación. Adicionalmente, es necesaria otra aplicación adicional, que se denominará Asistente que, o bien está pre-instalada o se instalará mediante un almacenamiento de aplicaciones (“App Store”). En este caso se trata de una aplicación que será instalada por encima del sistema operativo. Esto significa que no es ninguna parte componente integral del sistema operativo, para ampliar las características funcionales de dicho sistema operativo. Esta aplicación reconoce el inicio por primera vez, o bien los procesos iniciales de utilización de un terminal móvil y descarga los programas/Apps binarios, que deben ser pre-instalados en el terminal móvil. Después de la descarga de las aplicaciones de un almacenamiento de apps u otra memoria de internet (ftp, tftp, etc.), se enviará una consulta al dispositivo instalador del asistente para instalar las aplicaciones descargadas o bien paquetes de aplicaciones/paquetes de instalación. El dispositivo instalador comprueba al asistente en base al nombre y certificado en la lista que está a disposición del dispositivo instalador e instala las aplicaciones. El asistente, o bien la aplicación de asistente, tiene la ventaja de que puede ser distinto para cada país de aplicación y tipo de aparato y/o tipo de contrato. La aplicación puede tener en cuenta, por lo tanto, una configuración específica para diferentes tipos de aparatos y países, o bien también para diferentes contratos. Las aplicaciones posibilitan, por lo tanto, que se puedan instalar a posteriori aplicaciones sin exigir al usuario un proceso de instalación manual para cada aplicación. Además, se asegura que mediante la comprobación de los certificados y nombres de la aplicación, solamente tendrán derecho de instalar otras aplicaciones adicionales aquellas aplicaciones para las que existe un acuerdo correspondiente con asociados. La utilización del asistente posibilita preparar diferentes asistentes para diferentes tipos de aparatos, países y contratos, que solamente cargan las aplicaciones que son apropiadas para el correspondiente aparato. Según otra posibilidad adicional de realización, el asistente se encuentra en posición de mostrar publicidad u ofertas específicas. De ello resulta que las aplicaciones pueden ser instaladas a posteriori por aparato y país, y se asegurará con la mínima interacción con el usuario que solamente se instalarán las aplicaciones autorizadas. En base a la comprobación, se produce además, una separación entre un programa de instalador que está integrado en el sistema operativo o en el firmware y una aplicación normal tal como el asistente, que son fáciles de gestionar y flexibles de introducir. El dispositivo instalador tiene usualmente una funcionalidad o bien autorización, para una instalación sin preguntas al usuario, de modo silencioso. Esta autorización llega al dispositivo instalador a través de correspondientes autorizaciones en el sistema operativo, es decir, funciona como proceso con derechos de usuario muy elevado, en especial derechos Raíz, o bien es una parte de la funcionalidad del sistema operativo. El dispositivo instalador consigue de un servidor determinado una lista de aplicaciones a través de HTTP PS.

Otros protocolos que, preferentemente, están codificados, son igualmente posibles. La dirección del servidor está dispuesta previamente. Habitualmente, tiene lugar una petición a través de una determinada dirección IP. Se facilitará en retorno desde el servidor una lista con informaciones firmadas sobre aplicaciones que pueden instalar otras aplicaciones. El instalador administra esta lista en una zona de almacenamiento segura. Habitualmente, esta lista es solicitada regularmente para comprobar variaciones. La lista comprende habitualmente solo los nombres de las aplicaciones y las correspondientes firmas. Entonces, el asistente carga, después del inicio por primera vez del

teléfono móvil, que se puede reconocer por los correspondientes indicadores, una lista específica de aplicaciones de un servidor, que se pueden instalar en un aparato específico con una configuración específica. El inicio por primera vez del teléfono puede ser reconocido por la disposición de indicadores determinados en una memoria no volátil. Si, por ejemplo, un teléfono móvil es colocado en su situación original nuevamente, estos indicadores se apagan. En una operación de inicio, el asistente conoce que se deben instalar nuevamente todos los programas que han sido definidos en las listas. El servidor puede administrar las listas o bien, las puede componer según reglas dinámicas, que son específicas para tipos de aparatos, tipos de contratos y países. Mediante el envío de las listas al asistente, éste tendrá conocimiento de cuáles aplicaciones se deben cargar en la etapa siguiente. El asistente consigue entonces las características del teléfono y la tarjeta SIM, así como sus informaciones, y las transmite al servidor. El dispositivo instalador y el asistente están ya configurados, de manera que la dirección de red del servidor es conocida. El servidor será preparado por el proveedor de red a través de una red (red IP) para facilitar múltiples firmas y nombres de aplicaciones en listas específicas, que después serán preparadas para descarga. Las firmas muestran cuáles de las aplicaciones están soportadas por el proveedor de red. La preparación de la firma es, por lo tanto, específica de la tarjeta SIM instalada y/o de la versión de sistema operativo correspondiente. Se puede pensar igualmente en otros parámetros y se describirán más adelante. Mediante esta añadidura es posible que el proveedor de la red pueda determinar cuáles aplicaciones son soportadas en el aparato móvil. Mediante este añadido es igualmente posible, que la aplicación que está funcionando en el aparato móvil, determinar si la aplicación será soportada por el proveedor de red o no. La aplicación que está instalada en el aparato móvil o que será instalada por el usuario, puede llegar al servidor por medio de un interfaz determinado en el campo previo. No obstante, de manera habitual la firma sirve para comprobación de la realización de aplicaciones y del soporte de las aplicaciones para el Desarrollador de la aplicación. El asistente consigue, por ejemplo, informaciones al inicio de la aplicación o en periodos determinados dentro de la aplicación y puede realizar de esta forma una estadística que será enviada al proveedor. Asimismo, la firma puede ser solicitada para una instalación de primera vez de la aplicación.

El procedimiento comprende además las siguientes etapas:

- Descarga de las firmas específicas para el aparato móvil desde el servidor a través del dispositivo instalador y
- Almacenamiento de estas firmas en un lugar de memoria del aparato móvil;

En una forma de realización preferente, las firmas son colocadas en un lugar de almacenamiento del terminal móvil que está codificado. La codificación se realiza mediante procedimientos conocidos, en especial, puede ser llevada a cabo mediante un módulo de codificación integrado o a través de la tarjeta SIM. Se puede pensar naturalmente que en aparatos que se encuentran permanentemente online puede no estar permitido un almacenamiento local. El almacenamiento puede estar constituido también de manera tal que, las firmas están solamente en memoria caché y no se descargará ninguna lista conjunta de firmas, si no solamente las firmas que son necesarias o bien que deben ser instaladas por una aplicación sobre el terminal móvil.

La puesta en marcha de la aplicación puede comprender varias funciones distintas. Por una parte, en la puesta en marcha por primera vez puede tener lugar una consulta de la firma, o durante el desarrollo del programa puede tener lugar siempre una consulta de la firma por parte del dispositivo instalador. También puede ser necesaria una consulta en la puesta en marcha sobre una determinada función. En una forma de realización preferente, la aplicación se configura en base a la firma conseguida. La configuración puede comprender que se utilicen determinadas representaciones gráficas o bien representaciones e indicaciones de marca del explotador de la red o bien del proveedor de la red. Además, se pueden liberar determinadas funciones con dependencia de la firma. También es posible desactivar determinadas funciones. De ello resulta que la firma actúa de forma dinámica sobre la aplicación, dado que determinadas funciones y aspectos son liberados o bloqueados. De este modo, es posible diferenciar entre aplicaciones que han sido instaladas originalmente en la primera instalación y, por lo tanto, han sido soportadas por el proveedor, y aplicaciones que han sido instaladas a posteriori manualmente por el usuario. Si el proveedor soporta, por ejemplo, determinadas aplicaciones tales como sistemas de navegación, esas aplicaciones pueden solicitar o comprobar las firmas en el instalador y entonces liberar funciones adicionales. Las aplicaciones que han sido instaladas a posteriori pueden tener acceso de modo correspondiente a esta interfaz, no obstante cuando la aplicación no ha sido dispuesta en una lista correspondiente de las aplicaciones autorizadas, no tiene lugar la liberación de funciones.

La firma comprende habitualmente componentes que son conocidos de la codificación y técnica de firma. Así, por ejemplo, se puede prever una clave pública y privada que se introduce en la firma. De este modo, se puede contener una información en el elemento de la firma que ha sido desarrollada por la clave pública de la aplicación o bien de la empresa que ha desarrollado la aplicación. La aplicación por si misma puede comprobar entonces, en base a la clave privada implementada, la firma. En una forma de realización alternativa, la aplicación dirige la firma al servidor, que comprueba la firma. De este modo, se puede evitar que la clave privada esté contenida en la misma aplicación. Después de haber tenido lugar la confirmación de la firma, se emprenderá un trabajo mediante la aplicación.

Además de un certificado y/o una clave pública, la aplicación comprende la firma, preferentemente, una identificación para la aplicación, de manera que la identificación de la aplicación puede ser el nombre de paquete (PacketName) de la aplicación.

En una forma de realización posible se descargan y se almacenan en el servidor una serie de firmas de modo regular. La selección de la firma o bien la asignación de la firma al terminal móvil se puede basar sobre diferentes criterios de filtrado. Habitualmente, determinadas firmas son utilizables solamente para determinados teléfonos de determinados fabricantes, teniendo en cuenta determinados proveedores. En caso de una consulta de la firma por parte del servidor, se preparan las firmas 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 vida de la firma. Naturalmente, se pueden prever otros criterios adicionales tal como el tipo de contrato del teléfono móvil, potencia del teléfono móvil, etc.

En una forma de realización preferente, los componentes tales como el servidor, se encuentran en un lugar de la red IP (Internet), a la que se pueden solicitar servicios a través de los DNS conocidos. De este modo, el servidor puede administrar, por ejemplo, un nombre de dominio fijo o de manera correspondiente una dirección IP fija. Se puede prever también que se utilicen determinadas zonas reservadas de la dirección que pueden ser administradas por el proveedor de red. Los servidores funcionan habitualmente a base de determinados sistemas de ordenador que están dotados de correspondientes sistemas operativos, tales como Linux, Windows o Unix, para preparar el correspondiente servicio en la red. Habitualmente, se utilizan protocolos de red, tal como son conocidos en una red basada en IP. El terminal móvil es habitualmente un teléfono inteligente en base a Adroid, Apple iOS, Windows Móvil, Symbian u otros similares. Estos teléfonos presentan procesadores, procesadores de banda base, memorias y correspondientes capas de un sistema operativo. El sistema operativo se designa también, frecuentemente, como firmware y se coloca en una zona de la memoria que se puede variar. Habitualmente se trata, en este caso, de una memoria flash.

Otra parte de la invención, son los componentes individuales que implementan el procedimiento. Un servidor, un dispositivo de instalación o instalador y un asistente. Tal como se ha explicado anteriormente, el instalador es preferentemente una parte del firmware, o bien una aplicación que ha sido preinstalada en el firmware de terminal móvil cuando se suministra al cliente final. El servidor es un sistema de ordenador que prepara un banco de datos, en el que se colocan múltiples firmas. El banco de datos puede ser un banco de datos relacional o un banco de datos orientado al objeto o cualquier otro tipo de banco de datos. En el sistema del ordenador funciona, habitualmente, un sistema operativo conocido tal como se ha explicado anteriormente. En otra forma de realización, el acceso al servidor es posible solamente a través de terminales móviles que se encuentran en la red del proveedor de red. Es decir, tiene lugar habitualmente un enmascaramiento en base de las direcciones de red o un enmascaramiento en base a la identificación del terminal móvil. El servidor es habitualmente un sistema que administra de modo correspondiente una base de datos o servicios de web a los que pueden acceder los terminales móviles y las aplicaciones.

Breve descripción de las figuras:

A continuación, se describirán las figuras que muestran una implementación posible de la invención, de manera que las figuras no se deben interpretar como limitación.

La figura 1 muestra un diagrama de recorrido del procedimiento.

La figura 2 muestra un ejemplo de la constitución de una lista con firmas.

La figura 3 muestra la constitución de la lista.

Descripción detallada de las figuras:

La figura 2 muestra un resumen de abreviaturas que se utilizan con respecto a las figuras 1 y 3.

La figura 1 muestra los diferentes componentes que se tienen en cuenta en la presente invención. En primer lugar el servidor, que se encuentra en contacto con el dispositivo instalador y, en segundo lugar el asistente, que también se encuentra en contacto con el servidor. En cuanto al servidor, se puede tratar de dos servidores distintos que pueden presentar estructuras igualmente distintas. En una forma de realización preferente se trata, no obstante, solamente de un servidor. El instalador consulta una lista de aplicaciones con firmas del servidor. Esta solicitud puede tener lugar, por ejemplo, a través del protocolo HTTPS, que está codificado de modo correspondiente. El servidor facilita entonces, basándose en la petición o consulta, una lista de aplicaciones con firmas que habitualmente están también codificadas con el mismo tipo de codificación HTTPS, que son específicas para el terminal. Se debe tener en cuenta, en este caso, que el instalador discurre sobre el terminal móvil y que el servidor será accedido por el terminal móvil a través de una red. La lista a transferir define aquellas aplicaciones que deben comunicar con el instalador para instalar la aplicación de modo silencioso, preferentemente, sin actuación del usuario. El instalador adquiere la función de la instalación y dispone una interfaz a disposición del sistema para instalar aplicaciones. Además

funciona una aplicación, una llamada aplicación de asistente, en el terminal móvil, que en el transcurso de su preparación, en especial, en la puesta en marcha inicial del aparato, carga una lista de aplicaciones del servidor. Esta consulta será comprobada por el servidor para comprobar si es permisible en su forma, para que, en caso de que sea autorizable, devolver una lista de aplicaciones que se deben instalar en una primera puesta en marcha. Después de que la lista de aplicaciones del asistente ha sido descargada, tiene lugar la descarga del paquete de aplicaciones que se han previsto para instalación en el terminal móvil. Este paquete de aplicaciones son transferidas al instalador o bien se transfieren una consulta URI con el lugar de colocación. El instalador comprueba si el que hace la consulta, es decir, el asistente, se trata de una aplicación permisible que presenta de modo correspondiente una firma autorizada y que no ha sido modificada, con ayuda de la firma en su lista. De este modo tiene lugar una instalación de modo silenciosa en la que el usuario no se debe involucrar. Por lo tanto, tendrá lugar una instalación silente de la que el usuario no tiene conocimiento alguno. De este modo, se puede prever el aparato en la primera utilización o bien en la primera conexión con el software adecuado sin que este esté integrado en el firmware. Después de una instalación satisfactoria, se enviará la correspondiente comunicación al asistente de que la instalación ha sido satisfactoria. En caso de que la consulta no ha sido autorizada o bien la aplicación no corresponde a las especificaciones de la firma, presentando el correspondiente nombre, se comunicará un correspondiente Fallo.

La figura 3 muestra un ejemplo de una lista de aplicaciones que, en este caso, comprende solamente una aplicación. En este caso, se trata de una lista para el asistente de aplicaciones App cuyos datos son comunicados. En primer lugar, se abre la lista mediante <id>. El ID significa una identificación de la lista de manera que la lista, puede ser debidamente identificada en un momento posterior. A continuación, se define un nombre de paquete en el que se puede apreciar de qué aplicación se trata y de qué proveedor. Se transfieren en primer lugar, firmas que posibilitan conocer si la aplicación está utilizada con ayuda del instalador para instalar otras aplicaciones. Para ello, se utiliza la firma que ha sido generada a través de PrK_Launcher. En base a esta firma se puede determinar que se trata de una aplicación autorizada que ha sido generada por el correspondiente servidor con la clave privada. A este respecto se hará referencia nuevamente a las tablas de la las figuras 2 y 1. Además, existen claves públicas del desarrollador que ha desarrollado esta aplicación para la correspondiente comprobación de las firmas.

Elementos individuales:

<published-date>: fecha de publicación de la lista, puede ser conseguida para comprobación de actualidad.

<category>, <category-id>, <title>: es el encabezamiento para una categoría, en este caso, esta categoría contiene las Apps seguras. Pueden estar contenidas en este archivo categorías para otros objetivos.

<recommendation>: cada App segura (“TrustedApp”) es una <recommendation>. Este concepto tiene solamente justificación histórica.

<id>: es un indicador significativo dentro del sistema de gestión de contenido.

<package-name>: el nombre del paquete de la App segura.

<name>, <icon>, <type>, <catalogue-date>, <catalogue-add-date>, <promotion> : Atributos de la App segura.

<platform-attributes>: estos contienen otros atributos, en este caso, concretamente la firma y la clave pública del certificado de la App segura.

<signature>: esta está codificada con la firma generada por SHA-2 a partir del nombre del paquete y de la clave pública del certificado de la App segura con una clave privada (la clave se llama “PrK_TrustedApp” en los otros documentos.

<certificate>: la clave pública del certificado de la App segura.

REIVINDICACIONES

1. Procedimiento para el control de la instalación de aplicaciones en un dispositivo móvil, con un instalador que está instalado en el dispositivo móvil y que está integrado en el sistema operativo del dispositivo móvil, de manera tal que tiene lugar una instalación silenciosa sin acción alguna por parte del usuario y que conoce la dirección de red de un servidor, de manera que el servidor del proveedor de red es habilitado a través de una red para proporcionar una lista de aplicaciones aceptables que tienen capacidad de instalar aplicaciones a través del instalador, de manera que la lista incluye certificados para cada aplicación y sus nombres, a base de la cual se determina claramente si la aplicación está autorizada para acceder al instalador,
comprendiendo además, un asistente que funciona como aplicación en el dispositivo móvil y que conoce la dirección del servidor para recibir una lista de aplicaciones a instalar desde el mismo,
comprendiendo las siguientes etapas:

- descarga a través del instalador de una lista de aplicaciones permitidas, y almacenando esta lista en el dispositivo móvil, de manera que la lista comprende los nombres y certificados de las aplicaciones permitidas;
- descarga a través del asistente desde el servidor, de una lista de aplicaciones a instalar, preferentemente, en la primera puesta en marcha del dispositivo móvil con el cliente final, de manera que la lista incluye la localización en memoria de las aplicaciones;
- descarga a través del asistente de las aplicaciones de la red como paquetes de instalación para almacenar estos como paquetes de instalación en el dispositivo móvil;
- transferencia del lugar de almacenamiento de los paquetes de instalación a través del asistente al instalador;
- comprobar el asistente por el instalador con ayuda de los certificados y nombres de la lista de aplicaciones permitidas, permitiendo si la verificación es satisfactoria, la instalación por el asistente conjuntamente con el instalador sin acción por parte del usuario.

2. Procedimiento, según la reivindicación anterior, en el que la aplicación es configurada en base al certificado.

3. Procedimiento, según la reivindicación anterior, en el que la aplicación activa funciones en base al certificado.

4. Procedimiento, según la reivindicación anterior, en el que la identificación de la aplicación es un paquete de instalación del nombre de la aplicación.

5. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que los certificados que han sido descargados por el instalador son almacenados en un área de memoria segura.

6. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que a petición del instalador y/o del asistente al servidor, se facilitan los certificados o lista de las aplicaciones instaladas en base a una o varias de las informaciones siguientes: información SIM, tipo de terminal, tipo de sistema operativo, versión de sistema operativo, duración del certificado.

7. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que el instalador forma parte del sistema operativo, y se lleva a cabo con una autorización que permite la instalación de aplicaciones sin acción por parte del usuario.

8. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que la localización de las aplicaciones es un MarketPlace/ Playstore o un servidor de archivo, en particular FTP.

9. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que el asistente funciona como aplicación a nivel de aplicación del sistema operativo.

10. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que el asistente reconoce en base a cambios y/o indicadores, si el terminal móvil procede de un estado original.

11. Sistema para el control de la instalación de aplicaciones en un dispositivo móvil, **caracterizado** por un instalador, un servidor y un asistente, que son designados y formados para llevar a cabo el procedimiento según una o varias de las reivindicaciones 1 a 10.

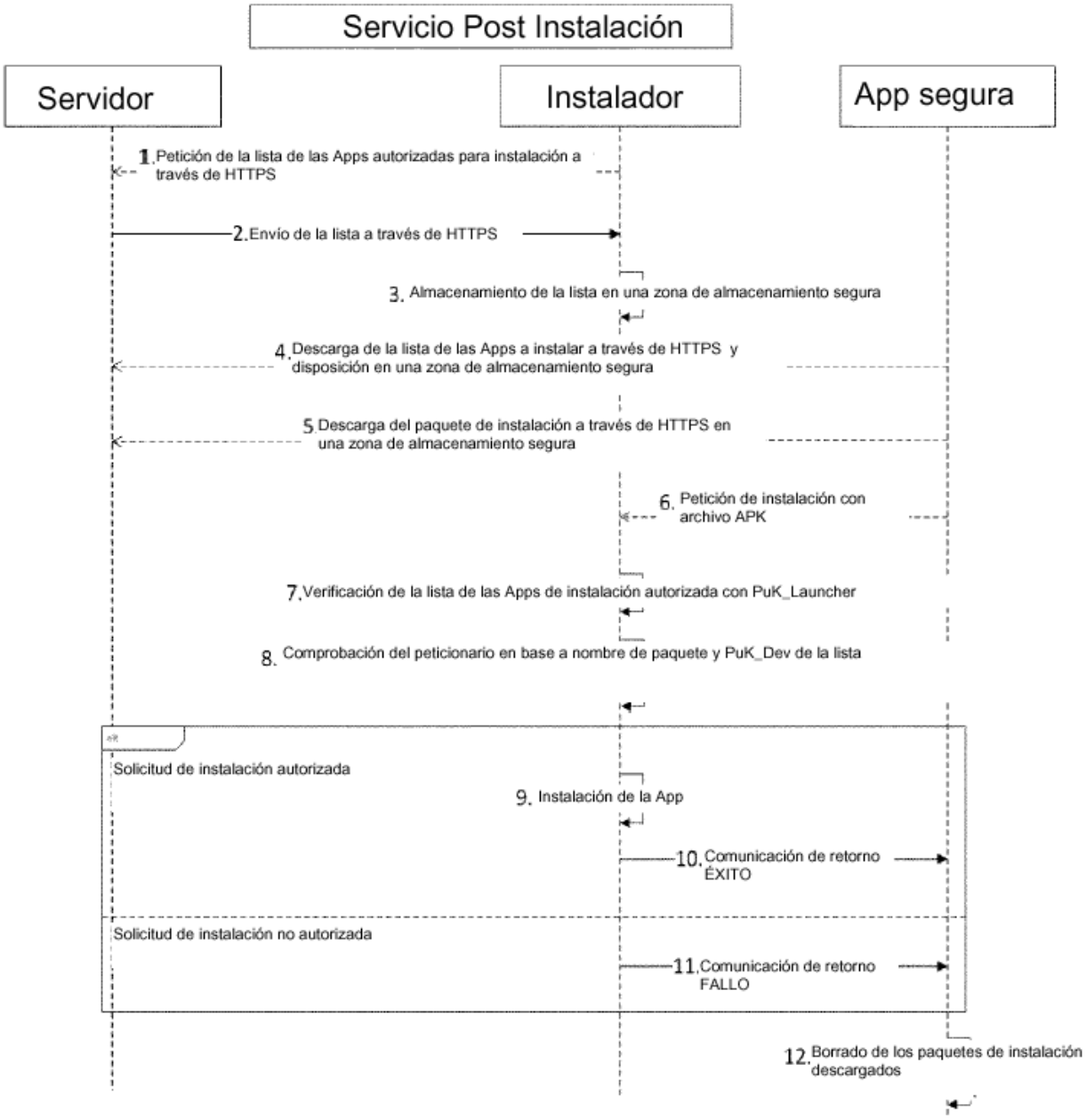
Servicio Post Instalación
Servidor
Instalador
App segura
1. Petición de la lista de las Apps autorizadas para instalación a través de HTTPS
2. Envío de la lista a través de HTTPS
3. Almacenamiento de la lista en una zona de almacenamiento segura
4. Descarga de la lista de las Apps a instalar a través de HTTPS y disposición en una zona de almacenamiento segura
5. Descarga del paquete de instalación a través de HTTPS en una zona de almacenamiento segura
6. Petición de instalación con archivo APK
7. Verificación de la lista de las Apps de instalación autorizada con PuK_Launcher
8. Comprobación del peticionario en base a nombre de paquete y PuK_Dev de la lista
alt
Solicitud de instalación autorizada
9. Instalación de la App
10. Comunicación de retorno ÉXITO
Solicitud de instalación no autorizada
11. Comunicación de retorno FALLO
12. Borrado de los paquetes de instalación descargados

Fig. 1

Abreviatura	Explicación
Instalador	Servicio de sistema, que recibe peticiones de las Apps seguras para instalar Apps sin interacción con el usuario.
App segura	App que está autorizada a enviar peticiones de instalación al instalador.
Lista de App seguras	Lista de Apps, que están autorizadas a enviar peticiones de instalación al instalador.
Asistente	Una App segura, que descarga Apps y las instala a través del instalador; puede presentar también una interfaz de usuario.
Lista de colecciones de App	Lista de colecciones de App, que pueden ser instaladas automáticamente o a través del instalador, descargadas del sistema ("Backend")
PrK_App segura	Clave privada con la que está firmado cada elemento de la App segura-Liste. La clave es colocada en sistema.
PuK_App segura	Clave pública para la verificación de cada uno de los elementos de la App segura-Liste, almacenada en cliente.
PuK_SSL	Clave pública del certificado SSL para HTTPS almacenada en cliente
PuK_Dev	Clave pública del certificado de desarrollador de una App segura.

Fig. 2

```
<?xml version="1.0" encoding="UTF-8"?>
<catalogue>
   <published-date>2012-10-30T10:40:53</published-date>
   <category type="default">
      <category-id>installer</category-id>
      <title>installer</title>
      <recommendation>
         <id>56283</id>
         <package-name>de.telekom.appslauncher</package-name>
         <name>App Assistant</name>
         <icon>http://i.t-mobile-
favourites.net/icons/catalogue/de/apptokens/images/1/1/2/4/4/9.png
</icon>
         <type>application</type>
         <catalogue-date>2012-10-30T08:50:33</catalogue-date>
         <catalogue-add-date>2012-10-12T11:39:50</catalogue-add-
date>
         <promotion>false</promotion>
         <platform-attributes>
            <attribute>
               <name>signature</name>
               <type>string</type>

<value>RxKJiFwUgds+7ThJ11Tiaag+unurx0Zw5TF3qREeck2AQWKtNRfyerCr+Ep
/Ntd4MN+IPwPtCcd9LYaT9asD7fnQfdhXHgnVskRMJ9DPmlqlfwd7dT3a/kI+qshLd
PE+vbMxsqWpNzBaj+4WmCUuMyCZt6lblUxcYwyHjAvS7vA=</value>
            </attribute>
            <attribute>
               <name>certificate</name>
               <type>string</type>

<value>884ddff1a21a17ae149056dc8f07917887b0b4fe095f36c669b916e4780
079ca7ca9071e777ac7f20fffc7df838d2a61889f903cc6bf2e616bc89d7b1188c
d943ef2250dd712f2d5507e8476c000071034053e52f7504fd7821177ff523ed2b
eb5c707565a5718d976ba7f0ec51e11874c96f2da15f426bf83d78cb96853886d<
/value>
```

```
            </attribute>
          </platform-attributes>
        </recommendation>
    </category>
</catalogue>
```

Fig. 3