(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 634 320**

(51) Int. CI.:

G06F 21/74 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.09.2013 PCT/EP2013/002720**

(87) Fecha y número de publicación internacional: **20.03.2014 WO14040724**

(96) Fecha de presentación y número de la solicitud europea: **10.09.2013 E 13762067 (0)**

(97) Fecha y número de publicación de la concesión europea: **07.06.2017 EP 2895985**

(54) Título: **Gestión de contenidos para estación móvil con entorno de ejecución**

(30) Prioridad:

11.09.2012 DE 102012017915

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.09.2017

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

DIETZE, CLAUS y
GALKA, GERO

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Gestión de contenidos para estación móvil con entorno de ejecución

La invención se refiere a una estación móvil que comprende un dispositivo terminal móvil con un entorno de ejecución seguro y un elemento de seguridad reemplazable o implementado fijamente, y a un servidor de gestión así como a un sistema de gestión de contenidos (Content Management System) para el entorno de ejecución seguro.

Las estaciones móviles en los sistemas GSM y UMTS así como en sistemas de telefonía móvil similares comprenden un dispositivo terminal móvil, por ejemplo un teléfono móvil o smartphone y un elemento de seguridad reemplazable o implementado fijamente. El elemento de seguridad tiene implementados datos de conexión, por ejemplo IMSI (International Mobile Subscriber Identity), claves y algoritmos para operar una conexión a la red de telefonía móvil. En el sistema GSM, o en el UMTS, la tarjeta SIM, o la USIM, (SIM = Subscriber Identity Module, USIM = Universal SIM) se conoce como elemento de seguridad reemplazable. La tarjeta eUICC (embedded Universal Integrated Circuit Card), que es un componente soldado fijamente, se conoce como elemento de seguridad implementado fijamente. La comunicación con el elemento de seguridad está estandarizada por las normas de la organización ETSI (European Telecommunications Standards Institute).

En los dispositivos terminales móviles, se conocen entornos de ejecución seguros TEEs (TEE = trusted execution environment), en los que se genera una separación a nivel de software entre diferentes entornos de ejecución. El entorno de ejecución seguro gestiona el almacenamiento de datos críticos de seguridad y programas. El resto de datos y programas se almacenan en un entorno de ejecución normal que existe adicionalmente. El entorno de ejecución no seguro, también conocido como “Normal Zone” o “Normal World”, se controla mediante un sistema de operación normal (por ejemplo Android, Windows Phone, Symbian). El entorno de ejecución seguro o de confianza, también conocido como “Truszone” o “Trusted World” o “Secure World” o “Trusted Execution Environment TEE”, se controla mediante un sistema de operación de seguridad.

En particular, aplicaciones críticas de seguridad y algunas funciones periféricas (por ejemplo controladores de teclado) son controladas de manera segura mediante el sistema de operación segura. A las aplicaciones del sistema de operación segura se las conoce también como Trusted Applications (por ejemplo Global Platform) o, en algunos casos, Trustlets (marcas registradas), en asociación con los términos “Trust” (confianza) y “Applet”.

Así, por ejemplo el documento “Global Platform Device Technology: TEE System Architecture, Version 0.4, Public Review Draft October 2011, Document Reference: GPD_SPE_009” describe un dispositivo terminal móvil con un entorno de ejecución normal o no seguro “Rich Execution Environment (REE)” y un entorno de ejecución seguro “Trusted Execution Environment (TEE)” (ver capítulo 1).

Los operadores de telefonía móvil disponen de una desarrollada infraestructura de servidores para la gestión de los contenidos (denominados Contents; por ejemplo datos, programas) en el elemento de seguridad. Esta infraestructura les permite cargar mensajes según el ETSI-Standard en el elemento de seguridad de manera criptográficamente segura desde un servidor de contenido por medio de la red de telefonía (OTA, over-the-air).

Para gestionar los contenidos en el entorno de ejecución seguro de un dispositivo terminal móvil también se requiere una infraestructura criptográficamente asegurable. Convencionalmente, los contenidos del entorno de ejecución seguro, por ejemplo aquellos según Global Platform, son gestionados mediante lo que se denomina un Trusted Service Manager.

Debido a que los requisitos de seguridad del entorno de ejecución seguro son más elevados que los del entorno de ejecución normal, la infraestructura para gestionar los contenidos de un dispositivo terminal móvil convencional no es suficiente. La infraestructura de servidores para gestionar los contenidos del elemento de seguridad no es directamente apropiada para gestionar los contenidos del entorno de ejecución seguro. Esto es debido a que la comunicación entre el elemento de seguridad y un servidor se efectúa usando mensajes según ETSI-Standard. Los mensajes transmitidos al entorno de ejecución seguro deben reunir otros requisitos, por ejemplo los de la Global Platform Organisation. Un Trusted Service Manager es capaz de transmitir dichos mensajes según Global Platform de manera segura al entorno de ejecución seguro. La operación de una infraestructura de servidores segura adicional para la gestión de los contenidos del entorno de ejecución seguro conlleva un gran esfuerzo financiero y de organización para los operadores de redes de telefonía móvil.

El objetivo de la invención se basa en proporcionar una estación móvil con un entorno de ejecución seguro que posibilite una gestión eficiente y al mismo tiempo segura de los contenidos (datos, programas) del entorno de ejecución seguro. Además se ha de especificar un servidor de gestión adecuado para estaciones móviles.

A partir del documento EP 1510 012 B1 se conoce una estación móvil con un elemento de seguridad reemplazable en la forma de una tarjeta SIM. En la tarjeta SIM están almacenados, además de los datos de conexión convencionales (IMSI) para operar una conexión con la red de telefonía móvil, también datos de conexión (dirección

IP) para operar una conexión con la red IP. En la tarjeta SIM también está implementado un servidor que redirecciona una conexión establecida por medio de la red de telefonía móvil a una conexión IP.

El documento WO 2009/027743 A2 divulga una estación móvil según el preámbulo de la reivindicación 1. Más específicamente el documento WO 2009/027743 A2 divulga una estación móvil con una “less secure area”, una “trusted area” y un “virtual UICC/IF” instalado en la “less trusted area”. Un sistema de operación de seguridad “Secure OS”, que puede comunicarse con el “virtual UICC/IF” instalado en el “less trusted area”, está instalado en la “trusted area”.

Tanto el documento WO 2009/027743 A2 como el documento EP 2 291 015 A1 mencionados no enseñan un entorno de ejecución seguro ni una comunicación directa con el mismo.

El documento EP 2 291 015 A1 divulga un procedimiento para comunicar datos entre un elemento de seguridad y un servidor externo por medio de un punto de acceso a la red.

El objetivo se resuelve mediante una estación móvil según la reivindicación 1. Las reivindicaciones dependientes recogen realizaciones ventajosas de la invención.

La estación móvil de acuerdo con la invención comprende un dispositivo terminal (por ejemplo un smartphone, teléfono móvil o similar) con un entorno de ejecución seguro así como un elemento de seguridad reemplazable o implementado fijamente (por ejemplo una tarjeta SIM, UICC, eUICC, etc.). Una unidad de recepción de elemento de seguridad está instalada en el elemento de seguridad para recibir mensajes de elemento de seguridad enviados al elemento de seguridad. Los mensajes de elemento de seguridad están previstos para introducir contenidos en el elemento de seguridad, por ejemplo datos, programas o actualizaciones para datos o programas ya existentes en el elemento de seguridad, en particular también datos y programas sujetos a una suscripción, es decir a una relación contractual con objeto de operar conexiones de telefonía móvil con la estación móvil por medio de una red móvil de un operador de red móvil. Una unidad de recepción de dispositivo terminal está instalada en el entorno de ejecución seguro del dispositivo terminal para recibir mensajes de dispositivo terminal enviados al entorno de ejecución seguro del dispositivo terminal. Los mensajes de dispositivo terminal están previstos para cargar en el entorno de ejecución seguro contenidos como datos, programas y actualizaciones de datos y programas. Por ejemplo, aplicaciones como las que se utilizan para realizar transacciones de pagos están previstas como programas.

La estación móvil se caracteriza por un servidor de envío de dispositivo terminal instalado en el elemento de seguridad para enviar al entorno de ejecución seguro mensajes de dispositivo terminal que pueden ser recibidos por el entorno de ejecución seguro.

De este modo los contenidos para el entorno de ejecución seguro pueden enviarse al elemento de seguridad. El servidor de envío de dispositivo terminal instalado en el elemento de seguridad retransmite los contenidos al entorno de ejecución seguro. Consecuentemente, un operador de red puede utilizar la infraestructura de servidor instalada para gestionar el elemento de seguridad también para gestionar el entorno de ejecución seguro. En particular, para gestionar los contenidos del entorno de ejecución seguro puede utilizarse un servidor de gestión que está propiamente previsto para gestionar los contenidos del elemento de seguridad y que para tal fin sólo requiere una ampliación menor. Este servidor de gestión se especifica en la reivindicación 3. La retransmisión necesaria de la comunicación en el entorno de ejecución seguro no se lleva a cabo mediante un servidor externo sino mediante el servidor interno de tarjeta (o bien eUICC-interno, etc.) implementado en el elemento de seguridad. De este modo, el operador de red queda liberado. Teniendo en cuenta que tanto la comunicación entre el servidor externo (por ejemplo el operador de red) y el elemento de seguridad como la comunicación entre el elemento de seguridad y el entorno de ejecución seguro son seguras, la solución de acuerdo con la invención tampoco presenta pérdidas de seguridad en comparación con una solución que tiene una infraestructura de servidor externa separada para el entorno de ejecución seguro.

Por tanto, según la reivindicación 1 se proporciona una estación móvil con un entorno de ejecución seguro que hace posible una gestión eficiente y al mismo tiempo segura de los contenidos del entorno de ejecución seguro.

Como servidor de envío de dispositivo terminal está previsto por ejemplo un denominado Trusted Service Manager. El Trusted Service Manager de acuerdo con la invención está implementado en el elemento de seguridad (por ejemplo una tarjeta SIM, UICC, eUICC, etc.).

Opcionalmente, el elemento de seguridad y los mensajes de elemento de seguridad están especificados según ETSI y el entorno de ejecución seguro así como los mensajes de dispositivo terminal según Global Platform.

Un servidor de gestión está configurado para gestionar los contenidos de las estaciones móviles. Cada estación móvil comprende un dispositivo terminal móvil con un entorno de ejecución seguro y un elemento de seguridad reemplazable o implementado fijamente. El servidor de gestión comprende un servidor de envío de elemento de seguridad convencional que está configurado para enviar mensajes de elemento de seguridad al elemento de seguridad que pueden ser recibidos y evaluados por el elemento de seguridad. El servidor de gestión se caracteriza

por que está configurado adicionalmente para aceptar mensajes de dispositivo terminal que pueden ser recibidos por el entorno de ejecución seguro del dispositivo terminal y para transmitir los mismos a un servidor de envío de dispositivo terminal instalado en el elemento de seguridad. La comunicación con el entorno de ejecución seguro se lleva a cabo finalmente mediante el servidor de envío de dispositivo terminal previsto en el elemento de seguridad y especificado en la reivindicación 1. Por el contrario, el servidor de gestión por sí mismo no tiene por qué estar adaptado para comunicarse directamente con el entorno de ejecución seguro. Correspondientemente, el operador del servidor de gestión, por ejemplo un operador de red de telefonía, asume un coste relativamente bajo.

Un sistema de gestión de contenidos de acuerdo con la invención comprende al menos una estación móvil así como un servidor de gestión tal como se ha descrito anteriormente.

El sistema de gestión de contenidos comprende opcionalmente además un servidor de contenidos (Content Server), mediante el que pueden proporcionarse contenidos, en particular datos y/o programas, al servidor de envío de elemento de seguridad. El servidor de contenidos para contenidos del entorno de ejecución seguro puede opcionalmente estar previsto de forma separada de un servidor de contenido para contenidos del elemento de seguridad. Alternativamente un servidor de contenido común/combinado puede estar previsto para contenidos del elemento de seguridad y el entorno de ejecución seguro. El servidor de contenido puede ser operado por los mismos operadores que el servidor de gestión o alternativamente por algún otro operador.

Un procedimiento de acuerdo con la invención para almacenar un contenido, en particular de datos y/o de un programa, en el entorno de ejecución seguro del dispositivo terminal móvil caracterizado por que

- el contenido se proporciona a un servidor de envío de elemento de seguridad previsto fuera del elemento de seguridad por un servidor de contenido previsto fuera de la estación móvil,

- el contenido se envía a un servidor de envío de dispositivo terminal instalado en el elemento de seguridad desde el servidor de envío de elemento de seguridad en un mensaje de elemento de seguridad, y

- el contenido se envía al entorno de ejecución seguro desde el servidor de envío de dispositivo terminal en un mensaje de dispositivo terminal.

En particular, datos y/o código de programa como controladores, aplicaciones y/o actualizaciones de las mismas pueden proporcionarse como contenidos para este propósito.

La invención se explica con mayor detalle a continuación con referencia a los ejemplos de realización y a los dibujos, en los cuales:

la figura 1 muestra una carga convencional en una estación móvil;

la figura 2 muestra una carga convencional de contenidos en una estación móvil;

la figura 3 muestra una carga de contenidos en una estación móvil según una realización de la invención.

Las figuras 1 y 2 muestran la carga convencional de contenidos en una estación móvil que comprende un dispositivo terminal móvil -ME- con un entorno de ejecución seguro -TEE- y un elemento de seguridad -SE-. Contenidos (datos, código de programa, controladores, aplicaciones, actualizaciones de los contenidos mencionados, etc.) -CONT- para el entorno de ejecución seguro son proporcionados a un Trusted Service Manager -TEE TSM- según Global Platform mediante un -TEE- servidor de contenidos -TEE CONT-, y cargados en el entorno de ejecución seguro -TEE- del dispositivo terminal -ME-. Contenidos (datos, código de programa, controladores, aplicaciones, actualizaciones de los contenidos mencionados, etc) -CONT- para el elemento de seguridad -SE- son proporcionados en el elemento de seguridad mediante un -SE- servidor de contenido -SE CONT- a un elemento de seguridad Trusted Service Manager -SE TSM- (servidor de envío de elemento de seguridad) según ETSI y cargados en el elemento de seguridad mediante el -SE TSM-. Como se muestra en la figura 2, los contenidos para el elemento de seguridad -SE- se transmiten en mensajes de elementos de seguridad -SN- que cumplen con ETSI. Los contenidos para el entorno de ejecución seguro -TEE- se transmiten en mensajes de dispositivo terminal -TN- que cumplen con Global Platform. El elemento de seguridad convencional Trusted Service Manager -SE TSM- puede procesar sólo mensajes que cumplen con ETSI. El Trusted Service Manager convencional para el entorno de ejecución seguro -TEE TSM- puede procesar sólo mensajes según Global Platform.

Según la figura 1 y la figura 2, los contenidos para el dispositivo terminal -ME- y el elemento de seguridad -SE- son por tanto proporcionados y cargados convencionalmente por infraestructuras de servidor separadas.

La figura 3 muestra una carga de contenidos en una estación móvil según una forma de realización de la invención. Los contenidos para el elemento de seguridad -SE- son cargados en el elemento de seguridad -SE- de manera convencional como en las figuras 1, 2. Los contenidos para el entorno de ejecución seguro -TEE- se envían para ello convencionalmente en mensajes de dispositivo terminal -TN- que cumplen con Global Platform. A diferencia del

estado de la técnica, estos mensajes de dispositivo terminal -TE- son enviados al elemento de seguridad -SE- mediante el Trusted Service Manager -SE TSM- que está previsto para el elemento de seguridad -SE- (servidor de envío de elemento de seguridad). El -TEE- Trusted Service Manager -TEE TSM- implementado en el elemento de seguridad -SE- y que está previsto para el entorno de ejecución seguro -TEE- (servidor de envío de dispositivo terminal) reconoce el mensaje de dispositivo terminal -TN- como tal y lo reenvía al entorno de ejecución seguro -TEE- del dispositivo terminal -ME-. Por tanto, en el sistema esquematizado en la figura 3, la gestión del entorno de ejecución seguro -TEE- se desplaza desde un servidor -TEE TSM- convencional externo al elemento de seguridad -SE- ampliado. En el elemento de seguridad -SE- la gestión del -TEE- se lleva a cabo de forma más precisa mediante el servidor -TEE TSM- integrado en tarjeta.

REIVINDICACIONES

1. Estación móvil que comprende un dispositivo terminal móvil (ME) con un entorno de ejecución seguro (TEE) y un elemento de seguridad (SE) reemplazable o implementado fijamente,

estando instalada una unidad de recepción de elemento de seguridad para recibir mensajes de elemento de seguridad (SN) enviados al elemento de seguridad en el elemento de seguridad (SE),

y estando instalada una unidad de recepción de dispositivo terminal para recibir mensajes de dispositivo terminal (TN) enviados al entorno de ejecución seguro (TEE) del dispositivo terminal (ME) en el entorno de ejecución seguro (TEE) del dispositivo terminal (ME),

comprendiendo adicionalmente un servidor de envío de dispositivo terminal (TEE-TSM) instalado en el elemento de seguridad (SE) para enviar al entorno de ejecución seguro (TEE) mensajes de dispositivo terminal (TN) que pueden ser recibidos por el entorno de ejecución (TEE) seguro;

en la que

los mensajes de elemento de seguridad (SN) enviados al elemento de seguridad son mensajes enviados por un servidor externo.

2. Estación móvil, según la reivindicación 1, en la que el elemento de seguridad (SE) y los mensajes de elemento de seguridad (SN) están especificados según ETSI y el entorno de ejecución seguro (TEE) así como los mensajes de dispositivo terminal (TN) están especificados según Global Platform.

3. Sistema de gestión de contenidos que comprende al menos una estación móvil según la reivindicación 1 ó 2 y un servidor de gestión (SERV) para estaciones móviles, comprendiendo la respectiva estación móvil un dispositivo terminal móvil (ME) con un entorno de ejecución seguro (TEE) y un elemento de seguridad (SE) reemplazable o implementado fijamente,

comprendiendo el servidor de gestión (SERV) un servidor de envío de elemento de seguridad (SE-TSM) que está configurado para enviar al elemento de seguridad (SE) mensajes de elemento de seguridad (SN) que pueden ser recibidos por el elemento de seguridad (SE),

estando configurado el servidor de gestión (SERV) adicionalmente para aceptar mensajes de dispositivo terminal (TE) que pueden ser recibidos por el entorno de ejecución seguro (TEE) del dispositivo terminal (ME) y para transmitir los mismos a un servidor de envío de dispositivo terminal (TEE-TSM) instalado en el elemento de seguridad (SE).

4. Sistema de gestión de contenidos según la reivindicación 3, que comprende adicionalmente un servidor de contenidos (CONT), por medio del que pueden suministrarse al servidor de envío de elemento de seguridad (SE-TSM) contenidos, en particular datos y/o programas, para ser almacenados en el entorno de ejecución seguro (TEE) de un dispositivo terminal móvil (ME).

5. Procedimiento para una estación móvil que comprende un dispositivo terminal móvil (ME) con un entorno de ejecución seguro (TEE) y un elemento de seguridad (SE) reemplazable o implementado fijamente, para almacenar un contenido, en particular datos y/o programas, en el entorno de ejecución seguro (TEE) del dispositivo terminal móvil (ME),

- en el que el contenido se envía al entorno de ejecución seguro (TEE) en un mensaje de dispositivo terminal (TN) desde un servidor de envío de dispositivo terminal (ME-TSM) instalado en el elemento de seguridad (SE),

- el contenido se suministra a un servidor de envío de elemento de seguridad (SE-TSM) previsto fuera de la estación móvil desde un servidor de contenido (CONT) previsto fuera de la estación móvil,

- el contenido se envía al servidor de envío de dispositivo terminal (ME-TSM) desde el servidor de envío de elemento de seguridad (SE-TSM) en un mensaje de elemento de seguridad (SN).

6. Procedimiento según la reivindicación 5, en el que el elemento de seguridad (SE) y los mensajes de elemento de seguridad (SN) se especifican según ETSI y el entorno de ejecución seguro (TEE) y los mensajes de dispositivo terminal (TN) se especifican según Global Platform.

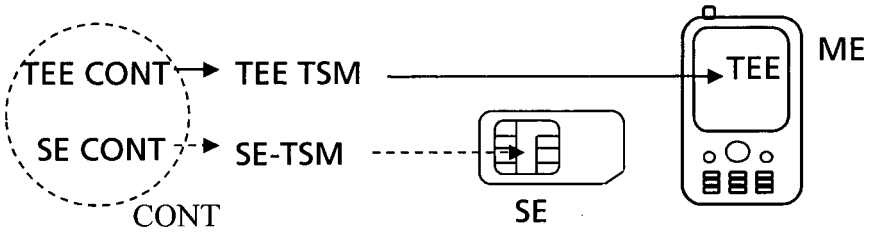
TEE CONT
TEE TSM
SE CONT
SE-TSM
CONT
SE
TEE
ME

Fig. 1

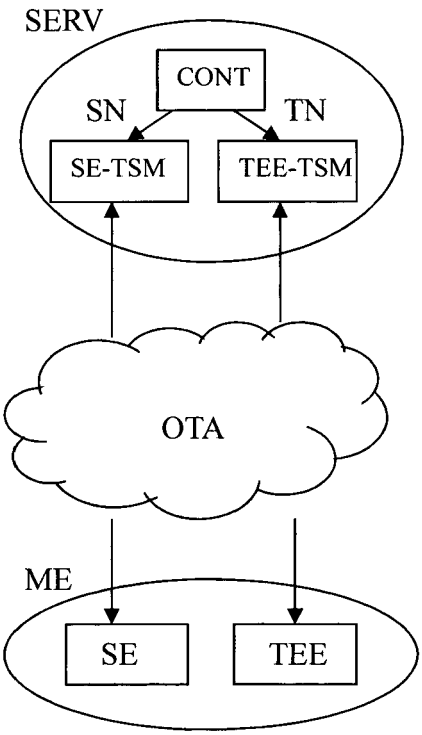
SERV
CONT
SN
TN
SE-TSM
TEE-TSM
OTA
ME
SE
TEE

Fig. 2

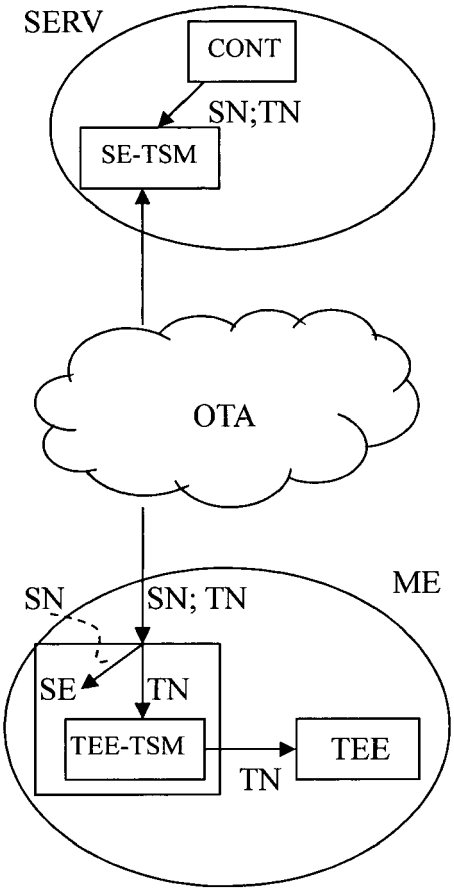

Fig. 3