(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 786 261**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04W 12/00 (2009.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04W 4/50 (2008.01)
G06Q 20/32 (2012.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.06.2015 E 15171243 (7)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2020 EP 3104635**

(54) Título: **Método para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, sistema y red de telecomunicaciones para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, programa que incluye un código de programa legible por ordenador y producto de programa informático**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2020

(73) Titular/es:

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

(72) Inventor/es:

BORGARDS, FRANK y
DUPRÉ, MICHAEL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, sistema y red de telecomunicaciones para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, programa que incluye un código de programa legible por ordenador y producto de programa informático

ANTECEDENTES

La presente invención se refiere a un método para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, estando el dispositivo de comunicación especialmente asociado a un abonado de una red de telecomunicaciones y, especialmente, siendo un equipo de usuario, en el que la aplicación de servicio relacionada con el elemento seguro, instalada en el elemento seguro, permite a una primera entidad de servidor de un proveedor de servicios, junto con una aplicación relacionada con el UE instalada en el dispositivo de comunicación, proporcionar un servicio al abonado de la red de telecomunicaciones.

La presente invención se refiere, además, a un sistema para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, estando el dispositivo de comunicación especialmente asociado a un abonado de una red de telecomunicaciones y, especialmente, siendo un equipo de usuario, en el que el sistema comprende la red de telecomunicaciones, una primera entidad de servidor de un proveedor de servicios, una segunda entidad de servidor, siendo una entidad de servidor relacionada con un emisor de un elemento seguro relacionado con el elemento seguro, y el dispositivo de comunicación, en el que la aplicación de servicio relacionada con un elemento seguro, instalada en el elemento seguro, permite a la primera entidad de servidor, junto con una aplicación relacionada con un UE instalada en el dispositivo de comunicación, proporcionar un servicio al abonado de la red de telecomunicaciones.

Adicionalmente, la presente invención se refiere, además, a una red de telecomunicaciones para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, estando el dispositivo de comunicación especialmente asociado a un abonado de una red de telecomunicaciones y, especialmente, siendo un equipo de usuario, en el que la red de telecomunicaciones está conectada a una primera entidad de servidor de un proveedor de servicios, y a una segunda entidad de servidor, que es una entidad de servidor relacionada con un emisor de elemento seguro relacionado con el elemento seguro, en el que la aplicación de servicio relacionada con el elemento seguro, instalada en el elemento seguro permite a la primera entidad de servidor, junto con una aplicación relacionada con un UE instalada en el dispositivo de comunicación, proporcionar un servicio al abonado de la red de telecomunicaciones.

Además, la presente invención se refiere a un programa y a un producto de programa informático para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, de acuerdo con el método, sistema y red de comunicación móvil de la invención.

Las utilizaciones y capacidades de los dispositivos de comunicación móvil han aumentado rápidamente en los últimos años. Por ejemplo, los usuarios de dispositivos de comunicación móvil tienen, actualmente, la capacidad de realizar pagos utilizando su teléfono móvil. Aunque los pagos a través de móvil proporcionan una herramienta conveniente para un consumidor, los pagos a través de móvil también pueden presentar problemas de seguridad. La información confidencial, tal como la información personal del consumidor, la información de la cuenta, etc., puede ser susceptible de intercepción. Adicionalmente, si el dispositivo de comunicación móvil se pierde o es robado, dicha información puede ser utilizada por un usuario no autorizado. Además, a medida que evolucionan las aplicaciones de pago a través de móvil, existe la necesidad no solo de proteger la información enviada desde el dispositivo de comunicación móvil, sino también de proteger la información enviada al dispositivo de comunicación móvil durante la transmisión.

En los entornos actuales de transacción a través de móvil, una institución financiera (tal como un banco) relacionada con un dispositivo de pago habitualmente tiene su propio gestor de servicios de confianza (TSM – Trusted Service Manager, en inglés) para comunicarse con un elemento seguro (SE – Secure element, en inglés) para aprovisionar una cuenta asociada con el dispositivo de pago en un dispositivo de comunicación móvil. El elemento seguro permite al dispositivo de comunicación móvil, por ejemplo, comunicarse con un lector de comunicación de campo cercano (NFC – Near field Communication, en inglés) que se encuentra en ubicaciones comerciales para realizar transacciones sin contacto.

De manera convencional, un consumidor o cliente que desea aprovisionar una cuenta en un dispositivo de la red de comunicación necesita que su identidad sea verificada por el emisor de la cuenta. De este modo, el consumidor o cliente contacta con el emisor para proporcionar información personal, por ejemplo, un número de cuenta principal, una fecha de vencimiento de la tarjeta, así como información de identificación personal, tal como nombre, fecha de

nacimiento, etc. Una vez que el emisor verifica que el consumidor o cliente es el usuario aprobado de la cuenta, el emisor enviará / proporcionará al usuario un código de activación de la cuenta. A continuación, el usuario proporciona el código de activación de la cuenta a una red de procesamiento de pagos para aprovisionar la cuenta en el dispositivo de comunicación móvil. La red de procesamiento de pagos contacta con el emisor para confirmar el código de activación de la cuenta y que el usuario ya está autorizado por el emisor. Este proceso es ineficiente ya que implica una comunicación innecesaria entre la red de procesamiento de pagos y el emisor durante el aprovisionamiento de la cuenta en el dispositivo de comunicación móvil. Los documentos de patente US 2012/171992, WO 2012/091351, US 2012/300932 o US 2012/300932 se refieren al aprovisionamiento seguro de servicios en un elemento seguro.

Por lo tanto, es conocido, en general, utilizar un proceso secuencial en un modelo impulsado por impulso para el aprovisionamiento de servicios en un elemento seguro tal como las UICC (Tarjeta universal de circuitos integrados - Universal Integrated Circuit Card, en inglés): el cliente realiza un pedido del servicio al proveedor de servicios. A continuación, el proveedor de servicios verifica el pedido, configura el servicio y ordena a un administrador de servicios de confianza que personalice y cifre los datos y gestione los pasos de instalación hacia el operador de la red móvil. El operador de la red móvil lo verifica y envía los datos a través de la red móvil, por ejemplo, utilizando el protocolo BIP (Protocolo independiente del portador – Bearer Independent Protocol, en inglés) / CATTP (Protocolo de transferencia de kit de herramientas de aplicación de tarjeta – Card Application Toolkit Transfer Protocol, en inglés) a la UICC.

Una limitación de este enfoque es la separación del proceso de pedido de un servicio y la instalación del mismo. El cliente, a menudo, no recibe comentarios sobre el éxito de la instalación. Solo en la aplicación de monedero el cliente puede ver si la instalación tuvo éxito. Además, el protocolo BIP / CATTP es menos estable que una conexión de internet para móviles

COMPENDIO

Un objeto de la presente invención es proporcionar una solución técnicamente simple, efectiva y especialmente rentable para integrar, por un lado, el proceso de pedido para un servicio relacionado con un elemento seguro y, por otro lado, la instalación del mismo en relación con un elemento seguro que se encuentra en un dispositivo de comunicación. Otro objeto de la presente invención es proporcionar un sistema que comprende la red de telecomunicaciones, una primera entidad de servidor de un proveedor de servicios y una segunda entidad de servidor que es una entidad de servidor relacionada con un emisor de elemento seguro relacionado con el elemento seguro, cuyo sistema permite una solución rentable y comparativamente simple para integrar el proceso de pedido de un servicio relacionado con el elemento seguro, y la instalación de la misma en relación con el elemento seguro.

El objeto de la presente invención se consigue mediante un método para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, estando el dispositivo de comunicación especialmente asociado a un abonado de una red de telecomunicaciones y, especialmente, siendo un equipo de usuario, en el que la aplicación de servicio relacionada con un elemento seguro, instalada en el elemento seguro, permite a una primera entidad de servidor de un proveedor de servicios, junto con una aplicación relacionada con un UE instalada en el dispositivo de comunicación, proporcionar un servicio al abonado de la red de telecomunicaciones,
en el que un emisor de elemento seguro corresponde al elemento seguro,
en el que el método comprende los siguientes pasos:

- en un primer paso, una solicitud inicial es transmitida por la aplicación de servicio relacionada con el UE del dispositivo de comunicación hacia la primera entidad de servidor, para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro, siendo transmitida la solicitud inicial por medio de un mensaje de solicitud,
- en un segundo paso, posterior al primer paso, la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro es transmitida, por la primera entidad de servidor, a la segunda entidad de servidor, del emisor de elemento seguro, generando la segunda entidad de servidor la información de token relacionada con la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro del dispositivo de comunicación, y transmitiendo la segunda entidad de servidor la información de token a la primera entidad de servidor relacionada con la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro, en el que la información de token representa una autorización combinada del emisor de elemento seguro y el proveedor del servicio al abonado para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro
- en un tercer paso, posterior al segundo paso, la información de token es transmitida, por la primera entidad de servidor, a la aplicación de servicio relacionada con un UE del dispositivo de comunicación,
- en un cuarto paso, posterior al tercer paso, una solicitud de acceso y/o instalación, relacionada con la aplicación de servicio relacionada con el elemento seguro, es transmitida, junto con la información de token, por la aplicación de servicio relacionada con el UE del dispositivo de comunicación a una aplicación de proxy del emisor de elemento seguro, pudiendo la aplicación de proxy acceder al elemento seguro y/o instalar aplicaciones relacionadas con el elemento seguro en el elemento seguro, en el que la aplicación de proxy puede interactuar con el elemento seguro del dispositivo de comunicación y es instalada en el dispositivo de

comunicación como un enlace entre, por un lado, una segunda entidad de servidor del emisor de elemento seguro, y, por otro lado, el elemento seguro del dispositivo de comunicación, siendo la segunda entidad de servidor una entidad de servidor relacionada con el emisor de elemento seguro,

– en un quinto paso, posterior al cuarto paso, se establece un enlace de comunicación entre la aplicación de proxy y la segunda entidad de servidor, de modo que la información de token, junto con una información del SEID (Información del identificador de elemento seguro – Secure Element IDentifier information, en inglés) del dispositivo de comunicación, es transmitida a la segunda entidad de servidor para ser validada por la segunda entidad de servidor,

en el que, solo durante el quinto paso, la información de token es asignada a la información del SEID.

De acuerdo con la presente invención, es ventajosamente posible proporcionar un modelo para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación de un abonado, proporcionando más control al proveedor de servicios (por ejemplo, un banco u otro los proveedores de servicios de una aplicación de servicio relacionada con un elemento seguro) y mejorando la estabilidad mediante la utilización de una conexión IP (Protocolo de Internet) móvil de datos. Adicionalmente, al proveedor de servicios se le ofrece una opción para controlar la instalación desde la aplicación que está instalada en el dispositivo de comunicación del abonado, es decir, desde la aplicación de servicio relacionada con el UE (que habitualmente proporciona el proveedor de servicios). En lugar de una instalación secuencial a través de enlaces seguros (es decir, VPN), de acuerdo con la presente invención, se utiliza una secuencia de aprovisionamiento cíclico basada en una aplicación, en la que la autorización es gestionada mediante un token o una información de token. De acuerdo con la presente invención a través de una función proxy (o una aplicación de proxy), la instalación en el elemento seguro está controlada.

De acuerdo con la presente invención, se establece un enlace de comunicación en forma de conectividad de protocolo de Internet entre el dispositivo de comunicación, por un lado, y la primera entidad de servidor del proveedor de servicios, por otro lado. El enlace de comunicación puede utilizar una red de comunicación móvil u otra red de comunicación, por ejemplo, una red de telecomunicaciones de línea fija con el dispositivo de comunicación conectado a través de WLAN, Bluetooth u otra tecnología de radio a un punto de acceso.

De acuerdo con la presente invención, la instalación de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro puede ser facilitada utilizando el token o la información de token. El token (o la información de token) representa la autorización combinada del emisor de elemento seguro y un proveedor de servicios a un cliente (o abonado) para solicitar la instalación del servicio, es decir, la instalación de la aplicación de servicio relacionada con el elemento seguro. Por ello, es ventajosamente posible, de acuerdo con la presente invención, que se abran nuevas posibilidades para los procesos de instalación, es decir, un soporte para procesos de instalación que presentan un enfoque más centrado en el usuario en la forma de utilizar aplicaciones (apps) en dispositivos de comunicación (especialmente móviles). Es de especial importancia (tanto con respecto al nivel de seguridad relacionado con el enfoque de la invención como con la aceptación de este enfoque) que la solución de acuerdo con la presente invención sea compatible con interfaces estándar, tales como, por ejemplo, la interfaz Plataforma Global con respecto a la comunicación de elementos seguros.

De acuerdo con la presente invención, se debe instalar una aplicación de servicio relacionada con un elemento seguro en un elemento seguro en un dispositivo de comunicación. El dispositivo de comunicación está especialmente asociado a un abonado de una red de telecomunicaciones y especialmente es un equipo de usuario. El elemento seguro. habitualmente, se encuentra en el dispositivo de comunicación, habitualmente,

– en una tarjeta de hardware, extraíble, tal como una tarjeta SIM (tarjeta de módulo de identidad del abonado), o

– en un componente de hardware dedicado, no extraíble, del dispositivo de comunicación que realiza el elemento seguro y que comprende un módulo de software apropiado, o

– en un componente de hardware de propósito general, no extraíble, del dispositivo de comunicación y un módulo de software que realiza el elemento seguro.

La aplicación de servicio relacionada con el elemento seguro está instalada, normalmente, en el elemento seguro, permitiendo a una primera entidad de servidor de un proveedor de servicios, junto con una aplicación relacionada con el UE instalada en el dispositivo de comunicación, proporcionar un servicio al abonado de la red de telecomunicaciones. Además, el elemento seguro es emitido por un emisor de elementos seguros, es decir, el emisor de elemento seguro corresponde al elemento seguro.

De acuerdo con la presente invención, en el primer paso del método de la invención, la aplicación de servicio relacionada con el UE del dispositivo de comunicación transmite una solicitud inicial hacia la primera entidad de servidor para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro, la solicitud inicial es transmitida mediante un mensaje de solicitud. Especialmente, esto significa que un cliente (del operador de la red móvil, es decir, un abonado que, normalmente, posee el dispositivo de comunicación) solicita un servicio (es decir, por ejemplo, una tarjeta de pago) que se inicia en una aplicación (app) (es decir, una

app bancaria). En el contexto de la presente invención, el servicio solicitado también se conoce por el término "aplicación de servicio relacionada con un elemento seguro", y la aplicación (app) también se conoce por el término "aplicación relacionada con el UE". El cliente (del operador de la red móvil, es decir, el abonado) envía el pedido del servicio (de la aplicación de servicio relacionada con el elemento seguro) al lado del servidor del proveedor de servicios (es decir, la primera entidad de servidor), posiblemente después de haber llevado a cabo un proceso de autenticación que implica, habitualmente, introducir y/o generar credenciales de usuario y/o información biométrica tal como datos relacionados con huellas dactilares.

En el segundo paso de acuerdo con la presente invención, la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro es transmitida, por la primera entidad de servidor, a la segunda entidad de servidor, generando la segunda entidad de servidor la información de token relacionada con la solicitud de instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro del dispositivo de comunicación, y transmitiendo la segunda entidad de servidor la información de token a la primera entidad de servidor relacionada con la solicitud de instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro. Especialmente, esto significa que el proveedor de servicios envía la solicitud (del servicio solicitado de, por ejemplo, una tarjeta de pago) al emisor de elemento seguro (SEI – Secure Element Issuer, en inglés), siendo el emisor de elemento seguro el operador de la red móvil (MNO – Mobile Network Operator, en inglés), que posiblemente implique a un gestor de servicios de confianza (TSM). Una posible interfaz para la comunicación entre la primera entidad de servidor (es decir, el proveedor del servicio) y la segunda entidad de servidor (es decir, el emisor de elemento seguro, SEI) es Plataforma Global. Esta parte de la comunicación a menudo está garantizada y permite al emisor de elemento seguro (SEI) validar y aprobar la solicitud (transmitida por el proveedor de servicios, es decir, la primera entidad de servidor). El emisor de elemento seguro genera un token (o información de token), lo guarda y lo devuelve al proveedor de servicios (es decir, al primer servidor).

En el tercer paso, la información de token es transmitida, por la primera entidad de servidor, a la aplicación de servicio relacionada con el UE del dispositivo de comunicación. Esto significa que el proveedor de servicios (o la primera entidad de servidor) después de recibir el token o la información de token de la segunda entidad de servidor envía el token (o la información de token) a la aplicación (es decir, a la aplicación relacionada con el UE, en el dispositivo de comunicación) del cliente.

En el cuarto paso, una solicitud de acceso y/o instalación, relacionada con la aplicación de servicio relacionada con el elemento seguro, es transmitida, junto con la información de token, por la aplicación de servicio relacionada con el UE del dispositivo de comunicación a una aplicación de proxy del emisor de elemento seguro, pudiendo acceder la aplicación de proxy al elemento seguro y/o instalar aplicaciones relacionadas con el elemento seguro en el elemento seguro, en la que la aplicación de proxy puede interactuar con el elemento seguro del dispositivo de comunicación y está instalada en el dispositivo de comunicación como un enlace entre, por un lado, una segunda entidad de servidor del emisor de elemento seguro y, por otro lado, el elemento seguro del dispositivo de comunicación, siendo la segunda entidad de servidor una entidad de servidor relacionada con el emisor de elemento seguro. Esto significa que la aplicación del proveedor de servicios (es decir, la aplicación de servicio relacionada con el UE) envía una solicitud de instalación para el servicio (es decir, la aplicación de servicio relacionada con el elemento seguro) a la app de proxy (o aplicación de proxy) del emisor de elemento seguro (SEI), es decir, especialmente integrado en la app de monedero del MNO, proporcionando de este modo el token (o la información de token) como parámetro. La app de proxy proporciona el enlace entre el SEI del lado del servidor (o segunda entidad de servidor) y el elemento seguro, lee la ID del elemento seguro (es decir, el SEID (Información del identificador del elemento seguro) o el ICCID (identificador de la tarjeta de circuito integrado) del elemento seguro.

En el quinto paso, posterior al cuarto paso, se establece un enlace de comunicación entre la aplicación de proxy y la segunda entidad de servidor de tal manera que la información de token, junto con una información de SEID (información de Identificador de Elemento Seguro) del dispositivo de comunicación (o del elemento seguro dentro del dispositivo de comunicación) se transmite a la segunda entidad de servidor para ser validado por la segunda entidad de servidor. Esto significa que se abre una conexión (desde la aplicación de proxy) al lado del servidor del SEI (es decir, la segunda entidad de servidor) y la aplicación de proxy solicita la instalación del servicio proporcionando el ICCID / SEID y el token (información).

De acuerdo con la presente invención, la información de token se asigna (desde la perspectiva del emisor de elemento seguro, es decir, la segunda entidad de servidor) a la información ICCID / SEID solo durante el quinto paso, es decir, antes del quinto paso (dentro del método de la invención) o antes del establecimiento del enlace de comunicación entre la aplicación de proxy y la segunda entidad de servidor (de acuerdo con el sistema inventivo o la red de telecomunicaciones), la segunda entidad de servidor no tiene conocimiento de la asignación de una información de token dada (generada previamente) a un abonado específico del operador de red móvil.

De acuerdo con la presente invención, se prefiere que durante el quinto paso, se reciban comandos de instalación (en caso de que un proceso de validación (que involucra la información de token), realizado dentro de la segunda entidad de servidor, finalice con éxito) segunda entidad de servidor, por la aplicación de proxy para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro, en el que, preferiblemente, los comandos de instalación, recibidos por la aplicación de proxy, se transmiten en forma cifrada.

Esto significa que, después de abrir la conexión desde la aplicación de proxy al lado del servidor del SEI (es decir, la segunda entidad de servidor) o durante el quinto paso, el SEI (es decir, la segunda entidad de servidor) verifica la validez del token (información). Si es válido, el SEI (o la segunda entidad de servidor) genera los comandos de instalación (habitualmente utilizando una APDU, Unidad de datos de protocolo de aplicación (Application Protocol Data Unit, en inglés), un formato de comunicación ampliamente utilizado entre el elemento seguro y las aplicaciones exteriores a la tarjeta) y los asegura especialmente con las claves ISD que pueden ser obtenidas a partir de la ID del elemento seguro (es decir, ICCID / SEID). Estos comandos son enviados al elemento seguro, es decir, a través de la app de proxy, y se ejecutan allí.

Por lo tanto, es ventajosamente posible, de acuerdo con la presente invención, que un alto nivel de seguridad se pueda combinar con un mayor nivel de conveniencia y facilidad de utilización para un usuario del dispositivo de comunicación.

De acuerdo con la presente invención, es más preferible que el lado del servidor del SEI (es decir, la segunda entidad de servidor) indique al proveedor de servicios o al lado del servidor del TSM (es decir, la primera entidad de servidor) la ejecución con éxito de los comandos (en el dispositivo de comunicación). El proveedor de servicios o TSM (es decir, la primera entidad de servidor) habitualmente consulta la ID del elemento seguro (es decir, la ICCID) del emisor de elemento seguro (SEI) para obtener una clave secreta. El proveedor de servicios (es decir, la primera entidad de servidor) genera un texto de personalización y, habitualmente, lo hace seguro con la clave secreta. De acuerdo con una variante de la presente invención, este texto de personalización es enviado al lado del servidor del SEI (es decir, a la segunda entidad de servidor) y, a través de la aplicación de proxy, al elemento seguro del dispositivo de comunicación. De acuerdo con una variante alternativa de la presente invención, el texto es enviado a través de la app del proveedor de servicios (es decir, a la aplicación de servicio relacionada con el UE) a este elemento seguro.

Además, de acuerdo con la presente invención, se prefiere que la segunda entidad de servidor forme parte de la red de telecomunicaciones.

Además, la presente invención se refiere a un sistema para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, estando el dispositivo de comunicación especialmente asociado a un abonado de una red de telecomunicaciones y siendo, especialmente, un equipo de usuario, en el que el sistema comprende la red de telecomunicaciones, una primera entidad de servidor de un proveedor de servicios, una segunda entidad de servidor, estando una entidad de servidor relacionada con un emisor de elemento seguro relacionado con el elemento seguro, y el dispositivo de comunicación, en el que la aplicación de servicio relacionada con un elemento seguro, instalada en el elemento seguro, permite a la primera entidad de servidor, junto con una aplicación relacionada con el UE instalada en el dispositivo de comunicación, proporcionar un servicio al abonado de la red de telecomunicaciones, en el que el sistema está configurado de tal manera que:

- una solicitud inicial es transmitida por la aplicación de servicio relacionada con el UE del dispositivo de comunicación hacia la primera entidad de servidor, para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro, siendo transmitida la solicitud inicial por medio de un mensaje de solicitud,
- la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro es transmitida, por la primera entidad de servidor, a la segunda entidad de servidor, del emisor de elemento seguro, generando la segunda entidad de servidor la información de token relacionada con la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro del dispositivo de comunicación, y transmitiendo la segunda entidad de servidor la información de token a la primera entidad de servidor relacionada con la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro,
- la información de token es transmitida, por la primera entidad de servidor, a la aplicación de servicio relacionada con un UE del dispositivo de comunicación,
- una solicitud de acceso y/o instalación, relacionada con la aplicación de servicio relacionada con el elemento seguro, es transmitida, junto con la información de token, por la aplicación de servicio relacionada con el dispositivo de comunicación a una aplicación de proxy del emisor de elemento seguro, pudiendo la aplicación de proxy acceder al elemento seguro y/o instalar aplicaciones relacionadas con el elemento seguro en el elemento seguro, en el que la aplicación de proxy puede interactuar con el elemento seguro del dispositivo de comunicación y es instalada en el dispositivo de comunicación como un enlace entre, por un lado, una segunda entidad de servidor del emisor de elemento seguro, y, por otro lado, el elemento seguro del dispositivo de comunicación,
- se establece un enlace de comunicación entre la aplicación de proxy y la segunda entidad de servidor, de modo que la información de token, junto con una información del SEID (Información del identificador de elemento seguro) del dispositivo de comunicación, es transmitida a la segunda entidad de servidor para ser validada por la segunda entidad de servidor,

en el que la información de token es asignada a la información del SEID tras el establecimiento del enlace de comunicación entre la aplicación de proxy y la segunda entidad de servidor.

Por lo tanto, es ventajosamente posible, de acuerdo con la presente invención, especialmente con respecto al sistema de la invención, proporcionar una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación de un abonado.

De acuerdo con la presente invención, se prefiere especialmente con respecto al sistema de la invención que el sistema esté configurado de tal manera que la aplicación de proxy reciba los comandos de instalación, desde la segunda entidad de servidor, para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro, en el que, preferiblemente, los comandos de instalación, recibidos por la aplicación de proxy, son transmitidos en forma cifrada.

Todas las realizaciones preferidas mencionadas anteriormente con respecto al método de la invención deben ser aplicadas también - mutatis mutandis - al sistema.

Adicionalmente, la presente invención se refiere a una red de telecomunicaciones para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, estando el dispositivo de comunicación especialmente asociado a un abonado de una red de telecomunicaciones y, especialmente, a un equipo de usuario, en el que la red de telecomunicaciones está conectada a una primera entidad de servidor de un proveedor de servicios, y a una segunda entidad de servidor, siendo una entidad de servidor relacionada con un emisor de elemento seguro relacionado con el elemento seguro, en el que la aplicación de servicio relacionada con el elemento seguro, instalada en el elemento seguro, permite a la primera entidad de servidor, junto con una aplicación relacionada con el UE instalada en el dispositivo de comunicación, proporcionar un servicio al abonado de la red de telecomunicaciones, en el que el sistema está configurado de tal manera que:

- una solicitud inicial es transmitida por la aplicación de servicio relacionada con el UE del dispositivo de comunicación hacia la primera entidad de servidor, para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro, siendo transmitida la solicitud inicial por medio de un mensaje de solicitud,
- la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro es transmitida, por la primera entidad de servidor, a la segunda entidad de servidor, del emisor de elemento seguro, generando la segunda entidad de servidor la información de token relacionada con la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro del dispositivo de comunicación, y transmitiendo la segunda entidad de servidor la información de token a la primera entidad de servidor relacionada con la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro,
- la información de token es transmitida, por la primera entidad de servidor, a la aplicación de servicio relacionada con un UE del dispositivo de comunicación,
- una solicitud de acceso y/o instalación, relacionada con la aplicación de servicio relacionada con el elemento seguro, es transmitida, junto con la información de token, por la aplicación de servicio relacionada con el UE del dispositivo de comunicación a una aplicación de proxy del emisor de elemento seguro, pudiendo la aplicación de proxy acceder al elemento seguro y/o instalar aplicaciones relacionadas con el elemento seguro en el elemento seguro, en el que la aplicación de proxy puede interactuar con el elemento seguro del dispositivo de comunicación y es instalada en el dispositivo de comunicación como un enlace entre, por un lado, una segunda entidad de servidor del emisor de elemento seguro y, por otro lado, el elemento seguro del dispositivo de comunicación,
- se establece un enlace de comunicación entre la aplicación de proxy y la segunda entidad de servidor, de modo que la información de token, junto con una información del SEID (información del identificador de elemento seguro) del dispositivo de comunicación, es transmitida a la segunda entidad de servidor para ser validada por la segunda entidad de servidor,

en el que la información de token se asignada a la información del SEID una vez establecido el enlace de comunicación entre la aplicación de proxy y la segunda entidad de servidor.

Por lo tanto, es ventajosamente posible de acuerdo con la presente invención, especialmente con respecto al sistema de la invención, proporcionar una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación de un abonado.

De acuerdo con la presente invención, se prefiere, especialmente con respecto a la red de telecomunicaciones de la invención, que la red de telecomunicaciones esté configurada de tal manera que los comandos de instalación sean recibidos por la aplicación de proxy, desde la segunda entidad de servidor, para instalar la aplicación de servicio

relacionada con el elemento seguro en el elemento seguro, en el que, preferiblemente, los comandos de instalación, recibidos por la aplicación de proxy, son transmitidos en forma cifrada.

Todas las realizaciones preferidas mencionadas anteriormente con respecto al método de la invención deben ser aplicadas, también, mutatis mutandis, a la red de telecomunicaciones de la invención.

Adicionalmente, la presente invención se refiere a un programa que comprende un código de programa legible por ordenador que, cuando es ejecutado en un ordenador o en una aplicación o componente de un dispositivo de comunicación, especialmente el elemento seguro, o en un componente de red de una red de telecomunicaciones o en una primera entidad de servidor o en una segunda entidad de servidor o, en parte, en una aplicación o componente de un dispositivo de comunicación y, en parte, en un componente de red de una red de telecomunicaciones o, en parte, en una primera entidad de servidor o, en parte, en una segunda entidad de servidor, hace que el ordenador o la aplicación o el componente del dispositivo de comunicación, especialmente, el elemento seguro, o el componente de red de la red de telecomunicaciones, o la primera entidad de servidor, o la segunda entidad de servidor, lleven a cabo el método de la invención.

Aún más, la presente invención se refiere a un producto de programa informático para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro que se encuentra en un dispositivo de comunicación, comprendiendo el producto de programa informático un programa informático almacenado en un medio de almacenamiento, comprendiendo el programa informático código de programa que, cuando es ejecutado en un ordenador o en una aplicación o componente de un dispositivo de comunicación, especialmente, el elemento seguro, o en un componente de red de una red de telecomunicaciones o en una primera entidad de servidor o en una segunda entidad de servidor o, en parte, en una aplicación o componente de un dispositivo de comunicación y, en parte, en un componente de red de una red de telecomunicaciones o, en parte, en una primera entidad de servidor o, en parte, en una segunda entidad de servidor, hace que el ordenador o la aplicación o componente del dispositivo de comunicación, especialmente, el elemento seguro, o el componente de red de la red de telecomunicaciones o la primera entidad de servidor o la segunda entidad de servidor lleven a cabo el método de la invención.

Estas y otras características, funcionalidades y ventajas de la presente invención serán evidentes a partir de la siguiente descripción detallada, tomada junto con los dibujos adjuntos, que ilustrarán, a modo de ejemplo, los principios de la invención, proporcionada solo a modo de ejemplo, sin limitar el alcance de la invención. Las figuras de referencia citadas a continuación se refieren a los dibujos adjuntos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 ilustra esquemáticamente un dispositivo de comunicación provisto de un elemento seguro, así como una red de telecomunicaciones que comprende o está conectada a una primera y a una segunda entidad de servidor.

La figura 2 ilustra esquemáticamente un diagrama de comunicación entre un elemento seguro, una aplicación de servicio relacionada con el UE, una aplicación de proxy, la primera entidad de servidor (proveedor de servicios) y la segunda entidad de servidor (emisor de elemento seguro, SEI).

DESCRIPCIÓN DETALLADA

La presente invención se describirá con respecto a realizaciones particulares y con referencia a ciertos dibujos, pero la invención no está limitada a los mismos, sino solo por las reivindicaciones. Los dibujos descritos son solo esquemáticos y no limitativos. En los dibujos, el tamaño de algunos de los elementos puede estar exagerado, y no dibujado a escala, con fines ilustrativos.

Cuando se utiliza un artículo indefinido o definido cuando se hace referencia a un sustantivo singular, por ejemplo, “un”, “una”, “el”, “la”, esto incluye un plural de ese sustantivo, a menos que se indique específicamente otra cosa.

Además, los términos primero, segundo, tercero y similares en la descripción y en las reivindicaciones se utilizan para distinguir entre elementos similares, y no necesariamente para describir un orden secuencial o cronológico. Se debe entender que los términos utilizados de este modo son intercambiables en circunstancias apropiadas y que las realizaciones de la invención descritas en el presente documento son capaces de funcionar en otras secuencias distintas de las descritas en este documento.

En la figura 1, se muestra esquemáticamente un dispositivo de comunicación 20 que tiene un elemento seguro 21, así como una red de telecomunicaciones 100 que comprende o está conectada a una primera entidad 160 de servidor y a una segunda entidad 130 de servidor. El dispositivo de comunicación 20 puede ser utilizado, por ejemplo, en (o en conexión con) la red de telecomunicaciones 100, que es una red de comunicación móvil. Además, la red de telecomunicaciones 100 también puede estar realizada mediante una red de telecomunicaciones de línea fija y el dispositivo de comunicación 20 está conectado a un nodo de red de dicha red de telecomunicaciones 100 utilizando una conexión por cable o utilizando una conexión inalámbrica, por ejemplo, WLAN, Bluetooth u otra tecnología de acceso inalámbrico. Especialmente, la red de telecomunicaciones 100 puede ser considerada como

una red de comunicación móvil, especialmente como una red móvil terrestre pública (red de telecomunicaciones celular), que comprende, habitualmente, una red de acceso y una red central. Sin embargo, por sencillez, dichos detalles no están representados en la figura 1.

En la realización a modo de ejemplo representada en la figura 1, el dispositivo de comunicación 20 está conectado a través de la red de telecomunicaciones 100 a una primera entidad 160 de servidor. La primera entidad 160 de servidor corresponde, habitualmente, a un proveedor de servicios, y una segunda entidad 130 de servidor es una entidad de servidor relacionada con un emisor de elemento seguro, relacionada con el elemento seguro 21 en el dispositivo de comunicación 20. La primera entidad 160 de servidor es contactada por el dispositivo de comunicación 20 (o por el usuario del dispositivo de comunicación 20, siendo este usuario, habitualmente, un abonado de la red de telecomunicaciones 100, especialmente en el caso de que la red de telecomunicaciones 100 corresponda a una red de comunicaciones móvil) para obtener un servicio, que es, de acuerdo con la presente invención, un servicio relacionado con un elemento seguro, que implica una aplicación de servicio relacionada con un elemento seguro.

El dispositivo de comunicación 20 es, habitualmente, cualquier equipo de usuario que pueda comunicar con la red de telecomunicaciones 100 / red de comunicación móvil 100 a la primera entidad 160 de servidor. Por ejemplo, el dispositivo de comunicación 20 también puede ser realizado como un dispositivo de comunicación de máquina a máquina (dispositivo de comunicación de tipo máquina).

El elemento seguro 21, habitualmente, corresponde a una tarjeta SIM / UICC (Tarjeta de circuito integrado universal) (ya sea un hardware o una SIM (tarjeta) blanda) que se encuentra en el dispositivo de comunicación 20, o está integrado en la misma.

De acuerdo con la presente invención, el dispositivo de comunicación 20 comprende, además del elemento seguro 21, una aplicación de servicio 23 relacionada con el UE y una aplicación de proxy 22.

En la figura 2, un diagrama de comunicación entre el elemento seguro 21, la aplicación de servicio 23 relacionada con el UE, la aplicación de proxy 22, la primera entidad 160 de servidor (proveedor de servicios) y la segunda entidad 130 de servidor (emisor de elemento seguro, SEI) se muestra esquemáticamente.

En un primer paso de procesamiento 201, la aplicación de servicio 23 relacionada con el UE (en el dispositivo de comunicación 20) envía un mensaje de solicitud también llamado solicitud inicial a la primera entidad 160 de servidor, solicitando de este modo a la primera entidad 160 de servidor que inicie la instalación de la aplicación de servicio relacionada con el elemento seguro en el dispositivo de comunicación 20. Esto corresponde al primer paso del método de la invención, en el que la aplicación de servicio 23 relacionada con el UE del dispositivo de comunicación 20 transmite la solicitud inicial hacia la primera entidad 160 de servidor para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro 21.

En un segundo paso de procesamiento 202, la primera entidad 160 de servidor envía un mensaje a la segunda entidad 130 de servidor, solicitando de este modo a la segunda entidad 130 de servidor que cree o genere un nuevo token (o información de token). En un tercer paso de procesamiento 203, la segunda entidad 130 de servidor crea un token o información de token, y almacena el token o la información de token en una base de datos o en otro dispositivo de memoria. En un cuarto paso de procesamiento 204, la segunda entidad 130 de servidor envía un mensaje a la primera entidad 160 de servidor, transmitiendo de este modo la información de token a la primera entidad 160 de servidor. Los segundo, tercer y cuarto pasos de procesamiento 202, 203, 204 corresponden al segundo paso del método de la invención (siendo transmitida la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro a la segunda entidad 130 de servidor; generando la segunda entidad 130 de servidor la información de token; y transmitiendo la segunda entidad 130 de servidor 130 la información de token a la primera entidad 160 de servidor).

En un quinto paso de procesamiento 205, la primera entidad 160 de servidor envía un mensaje a la aplicación de servicio 23 relacionada con el UE. Esto corresponde al tercer paso del método de la invención, en la que la información de token es transmitida, por la primera entidad 160 de servidor a la aplicación de servicio 23 relacionada con el UE del dispositivo de comunicación 20.

De acuerdo con una variante de la presente invención, en un sexto paso de procesamiento 206, la aplicación de servicio 23 relacionada con el UE envía un mensaje a la primera entidad 160 de servidor, confirmando de este modo la recepción de la información de token. Opcionalmente, se omite el sexto paso de procesamiento 206.

En un séptimo paso de procesamiento 207, la aplicación de servicio 23 relacionada con el UE envía un mensaje a la aplicación de proxy 22. En un octavo paso de procesamiento 208, la aplicación de proxy 22 intercambia información con el elemento seguro 21 para leer el SEID (identificador de elemento seguro) y/o el ICCID (identificador de tarjeta de circuito integrado) del elemento seguro 21. Los séptimo y octavo pasos de procesamiento 207, 208 corresponden al cuarto paso del método de la invención (una solicitud de acceso y/o instalación, relacionada con la aplicación de servicio relacionada con el elemento seguro, que es transmitida, junto con la información de token, por la aplicación

de servicio 23 relacionada con el UE del dispositivo de comunicación 20 a la aplicación de proxy 22 del emisor de elemento seguro).

En un noveno paso de procesamiento 209, la aplicación de proxy 22 envía un mensaje a la segunda entidad 130 de servidor. En un décimo paso de procesamiento 210, la segunda entidad 130 de servidor almacena el ICCID / SEID en la información de token. Los noveno y décimo pasos de procesamiento 209, 210 corresponden al quinto paso del método de la invención (estableciéndose un enlace de comunicación entre la aplicación de proxy 22 y la segunda entidad 130 de servidor, de tal manera que la información de token, junto con una información del SEID (Información del identificador de elemento seguro)) del dispositivo de comunicación 20 son transmitida a la segunda entidad 130 de servidor para ser validada por la segunda entidad 130 del servidor).

De acuerdo con la presente invención, la información de token es asignada a la información del SEID / información del ICCID solo durante el quinto paso, es decir, no antes del quinto paso / no antes del noveno paso de procesamiento 209.

De acuerdo con una variante de la presente invención, en un undécimo paso de procesamiento 211, la primera entidad 160 de servidor envía un mensaje a la segunda entidad 130 de servidor. Opcionalmente, se omite el undécimo paso de procesamiento 211.

En un duodécimo paso de procesamiento 212, la segunda entidad 130 de servidor espera una solicitud por parte de la primera entidad 160 de servidor y/o espera la información de ICCID / información del SEID.

En un decimotercer paso de procesamiento 213, la segunda entidad 130 de servidor envía un mensaje de APDU (APDU habitualmente se refiere a “Unidad de Datos de Protocolo de Aplicación” y es el formato de comunicación entre el elemento seguro 21 y las aplicaciones fuera de la tarjeta) a la aplicación de proxy 22 En un decimocuarto paso de procesamiento 214, la aplicación de proxy 22 intercambia información con el elemento seguro 21, y en un decimoquinto paso de procesamiento 215, la aplicación de proxy 22 envía un mensaje de respuesta a la segunda entidad 130 de servidor. Los decimotercero, decimocuarto y decimoquinto pasos de procesamiento 213, 214, 215, juntos, se indican mediante el signo de referencia 240, y corresponden a un bucle en el flujo de procesamiento a modo de ejemplo de una implementación de acuerdo con la presente invención.

En un decimosexto paso de procesamiento 216, la segunda entidad 130 de servidor envía un mensaje a la primera entidad 160 de servidor. En un decimoséptimo paso de procesamiento 217, la segunda entidad 130 de servidor envía un mensaje adicional a la aplicación de proxy 22, y en un decimoctavo paso de procesamiento 218, la aplicación de proxy 22 envía un mensaje a la aplicación de servicio 23 relacionada con el UE.

De acuerdo con la presente invención, la creación y la utilización de una información de token es sugerida en el proceso de instalación de una aplicación de servicio relacionada con un elemento seguro 21 en un elemento seguro de un dispositivo de comunicación 20. De este modo, es ventajosamente posible obtener una autorización combinada para la instalación del servicio por parte del proveedor del servicio (es decir, la primera entidad 160 de servidor) y la segunda entidad 130 de servidor, es decir, el emisor de elemento seguro: el proveedor del servicio (es decir, la primera entidad 160 de servidor) verifica la solicitud del cliente y traduce la autorización en una solicitud de token a la segunda entidad 130 de servidor (emisor de elemento seguro). El emisor de elemento seguro (segunda entidad 130 de servidor) verifica si esa solicitud es enviada desde un proveedor de servicios autorizado y, opcionalmente, verifica que el cliente (es decir, el usuario del dispositivo de comunicación 20) sea elegible para el servicio relacionado con el elemento seguro solicitado (es decir, para utilizar la aplicación de servicio relacionada con un elemento seguro solicitada). La información de token representa la autorización adicional de la segunda entidad 130 de servidor / el emisor de elemento seguro). De acuerdo con la presente invención, diferentes aplicaciones (apps) se comunican entre sí utilizando la información de token para identificar la aplicación de servicio autorizada para un usuario (abonado) particular. De acuerdo con la presente invención, la información de token se utiliza como un identificador del cliente para el proveedor de servicios. Especialmente de acuerdo con la presente invención, se realiza una recuperación dinámica de la identidad (información) del elemento seguro 21 (es decir, el ICCID o el SEID) por parte de la app de proxy 22 como una “dirección de suministro” para la instalación. De acuerdo con la presente invención, es ventajosamente posible instalar una aplicación en el elemento seguro 21 / la tarjeta de circuito integrado universal (UICC) sin utilizar la MSISDN en absoluto.

REIVINDICACIONES

1. Método para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro (21) que se encuentra en un dispositivo de comunicación (20), estando asociado el dispositivo de comunicación (20), especialmente, a un abonado de una red de telecomunicaciones (100) y siendo, especialmente, un equipo de usuario (20), en el que la aplicación de servicio relacionada con un elemento seguro, instalada en el elemento seguro (21), permite a una primera entidad (160) de servidor de un proveedor de servicios, junto con una aplicación de servicio (23) relacionada con un UE instalada en el dispositivo de comunicación (20), proporcionar un servicio al abonado de la red de telecomunicaciones (100),
en el que un emisor de elemento seguro está relacionado con el elemento seguro (21), en el que el método comprende los pasos siguientes:

– en un primer paso, una solicitud inicial es transmitida por la aplicación de servicio (23) relacionada con un UE del dispositivo de comunicación (20) hacia la primera entidad (160) de servidor para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21), siendo transmitida la solicitud inicial por medio de un mensaje de solicitud,
– en un segundo paso, posterior al primer paso, la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro es transmitida, por la primera entidad (160) de servidor, a la segunda entidad (130) de servidor del emisor de elemento seguro; generando la segunda entidad (130) de servidor la información de token relacionada con la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21) del dispositivo de comunicación (20), y transmitiendo la segunda entidad (130) de servidor la información de token a la primera entidad (160) de servidor relacionada con la solicitud de instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21), en el que la información de token representa una autorización combinada del emisor de elemento seguro y el proveedor del servicio al abonado para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro,
– en un tercer paso, posterior al segundo paso, la información de token es transmitida, por la primera entidad (160) de servidor a la aplicación de servicio (23) relacionada con el UE del dispositivo de comunicación (20),
– en un cuarto paso, posterior al tercer paso, una solicitud de acceso y/o instalación, relacionada con la aplicación de servicio relacionada con el elemento seguro, es transmitida, junto con la información de token, por la aplicación de servicio (23) relacionada con el UE del dispositivo de comunicación (20) a una aplicación de proxy (22) del emisor de elemento seguro, pudiendo la aplicación de proxy (22) acceder al elemento seguro (21) y/o instalar aplicaciones relacionadas con elementos seguros en el elemento seguro (21), en el que la aplicación de proxy puede interactuar con el elemento seguro (21) del dispositivo de comunicación (20) y es instalada en el dispositivo de comunicación (20) como un enlace entre, por un lado, la segunda entidad (130) de servidor del emisor de elemento seguro y, por otro lado, el elemento seguro (21) del dispositivo de comunicación (20),
– en un quinto paso, posterior al cuarto paso, se establece un enlace de comunicación entre la aplicación de proxy (22) y la segunda entidad (130) de servidor, de modo que la información de token, junto con una información del SEID (Información del identificador de elemento seguro) del dispositivo de comunicación (20), es transmitida a la segunda entidad (130) de servidor para ser validada por la segunda entidad (130) de servidor,

en el que, solo durante el quinto paso, la información de token es asignada a la información del SEID.

2. Método, de acuerdo con la reivindicación 1, en el que, durante el quinto paso, los comandos de instalación, son recibidos, desde la segunda entidad (130) de servidor, por la aplicación de proxy (22), para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21), en el que, preferiblemente, los comandos de instalación, recibidos por la aplicación de proxy (22), son transmitidos en forma cifrada.

3. Método, de acuerdo con una de las reivindicaciones anteriores, en el que la segunda entidad (130) de servidor forma parte de la red de telecomunicaciones (100).

4. Sistema para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro (21) que se encuentra en un dispositivo de comunicación (20), estando el dispositivo de comunicación (20) especialmente asociado a un abonado de una red de telecomunicaciones (100) y, especialmente, siendo un equipo de usuario (20), en el que el sistema comprende la red de telecomunicaciones (100), una primera entidad (160) de servidor de un proveedor de servicios, siendo una segunda entidad (130) de servidor una entidad de servidor relacionada con un emisor de elemento seguro relacionado con el elemento seguro (21) y el dispositivo de comunicación (20), en el que la aplicación de servicio relacionada con el elemento seguro, instalada en el elemento seguro (21), permite a la primera entidad (160) de servidor, junto con una aplicación de servicio (23) relacionada con el UE instalada en el dispositivo de comunicación (20), proporcionar un servicio al abonado de la red de telecomunicaciones (100), en el que el sistema está configurado de tal manera que:

– una solicitud inicial es transmitida por la aplicación de servicio (23) relacionada con el UE del dispositivo de comunicación (20) hacia la primera entidad (160) de servidor para solicitar la instalación de la aplicación de servicio relacionada en el elemento seguro (21), siendo transmitida la solicitud inicial por medio de un mensaje de solicitud,

– la solicitud para instalar la aplicación de servicio relacionada con el elemento seguro es transmitida, por la primera entidad (160) de servidor, a la segunda entidad (130) de servidor, del emisor de elemento seguro; generando la segunda entidad (130) de servidor la información de token relacionada con la solicitud de instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21) del dispositivo de comunicación (20), y transmitiendo la segunda entidad (130) de servidor la información de token a la primera entidad (160) de servidor relacionada con la solicitud de instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21), en el que la información de token representa una autorización combinada del emisor de elemento seguro y el proveedor de servicios al abonado para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro,

– la información de token, por la primera entidad (160) de servicio a la aplicación de servicio (23) relacionada con el UE del dispositivo de comunicación (20),

– una solicitud de acceso y/o instalación, relacionada con la aplicación de servicio relacionada con el elemento seguro, es transmitida, junto con la información de token, por la aplicación de servicio (23) relacionada con el UE del dispositivo de comunicación (20) a una aplicación de proxy (22) del emisor de elemento seguro, pudiendo la aplicación de proxy (22) acceder al elemento seguro (21) y/o instalar aplicaciones relacionadas con el elemento seguro en el elemento seguro (21), en el que la aplicación de proxy puede interactuar con el elemento seguro (21) del dispositivo de comunicación (20) y es instalada en el dispositivo de comunicación (20) como un enlace entre, por un lado, una segunda entidad (130) de servidor del emisor de elemento seguro y, por otro lado, el elemento seguro (21) del dispositivo de comunicación (20),

– se establece un enlace de comunicación entre la aplicación de proxy (22) y la segunda entidad (130) de servidor, de modo que la información de token, junto con una información del SEID (Información de identificador de elemento seguro) del dispositivo de comunicación (20), es transmitida a la segunda entidad (130) de servidor para ser validada por la segunda entidad (130) de servidor,

en el que la información de token es asignada a la información del SEID tras el establecimiento del enlace de comunicación entre la aplicación de proxy (22) y la segunda entidad (130) de servidor.

5. Sistema, de acuerdo con la reivindicación 4, en el que el sistema está configurado de tal manera que se reciben comandos de instalación, desde la segunda entidad (130) de servidor, por parte de la aplicación de proxy (22), para instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21), en el que, preferiblemente, los comandos de instalación, recibidos por la aplicación de proxy (22), son transmitidos en forma encriptada.

6. Red de telecomunicaciones (100) para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro (21) que se encuentra en un dispositivo de comunicación (20), estando el dispositivo de comunicación (20) especialmente asociado a un abonado de una red de telecomunicaciones (100) y, especialmente, siendo un equipo de usuario (20), en el que la red de telecomunicaciones (100) está conectada a una primera entidad (160) de servidor de un proveedor de servicios, y a una segunda entidad (130) de servidor, siendo una entidad de servidor relacionada con un emisor de elemento seguro relacionado con el elemento seguro (21), en el que la aplicación de servicio relacionada con el elemento seguro, instalada en el elemento seguro (21), permite a la primera entidad (160) de servidor, junto con una aplicación de servicio (23) relacionada con el UE instalada en el dispositivo de comunicación (20), proporcionar un servicio al abonado de la red de telecomunicaciones (100), en el que la red de telecomunicaciones (100) está configurada de modo que:

– una solicitud inicial es transmitida por la aplicación de servicio (23) relacionada con un UE del dispositivo de comunicación (20) hacia la primera entidad (160) de servidor para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21), siendo transmitida la solicitud inicial mediante un mensaje de solicitud,

– la solicitud de instalar la aplicación de servicio relacionada con el elemento seguro es transmitida, por la primera entidad (160) de servidor, a la segunda entidad (130) de servidor del emisor de elemento seguro; generando la segunda entidad (130) de servidor la información de token relacionada con la solicitud de instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21) del dispositivo de comunicación (20), y transmitiendo la segunda entidad (130) de servidor la información de token a la primera entidad (160) de servidor relacionada con la solicitud de instalar la aplicación de servicio relacionada con el elemento seguro en el elemento seguro (21), en el que la información de token representa una autorización combinada del emisor de elemento seguro y el proveedor del servicio al abonado para solicitar la instalación de la aplicación de servicio relacionada con el elemento seguro,

– la primera entidad (160) de servidor transmite la información de token a la aplicación de servicio (23) relacionada con el UE del dispositivo de comunicación (20),

– una solicitud de acceso y/o instalación, relacionada con la aplicación de servicio relacionada con el elemento seguro, es transmitida, junto con la información de token, por la aplicación de servicio (23)

relacionada con el UE del dispositivo de comunicación (20) a una aplicación de proxy (22) del emisor de elemento seguro, pudiendo la aplicación de proxy (22) acceder al elemento seguro (21) y/o instalar aplicaciones relacionadas con el elemento seguro en el elemento seguro (21), en el que la aplicación de proxy es capaz de interactuar con el elemento seguro (21) del dispositivo de comunicación (20) y es instalada en el dispositivo de comunicación (20) como un enlace entre, por un lado, una segunda entidad (130) de servidor del emisor de elemento seguro, y, por otro lado, el elemento seguro (21) del dispositivo de comunicación (20),

– se establece un enlace de comunicación entre la aplicación de proxy (22) y la segunda entidad (130) de servidor, de modo que la información de token, junto con una información del SEID (Información del identificador del elemento seguro) del dispositivo de comunicación (20) es transmitida a la segunda entidad (130) de servidor para ser validada por la segunda entidad (130) de servidor,

en el que la información de token es asignada a la información del SEID una vez establecido el enlace de comunicación entre la aplicación de proxy (22) y la segunda entidad (130) de servidor.

7. Red de telecomunicaciones (100), de acuerdo con la reivindicación 6, en la que la red de telecomunicaciones (100) está configurada de tal manera que se reciben comandos de instalación, desde la segunda entidad (130) de servidor, por parte de la aplicación de proxy (22) para instalar la aplicación de servicio relacionada con un elemento seguro en el elemento seguro (21), en el que, preferiblemente, los comandos de instalación, recibidos por la aplicación de proxy (22), son transmitidos en forma encriptada.

8. Programa, que comprende un código de programa legible por ordenador que, cuando es ejecutado en un ordenador o en una aplicación o componente de un dispositivo de comunicación (20), especialmente el elemento seguro (21), o en un componente de red de una red de telecomunicaciones (100) o en una primera entidad (160) de servidor o en una segunda entidad (130) de segundo o, en parte, en una aplicación o componente de un dispositivo de comunicación (20) y, en parte, en un componente de red de una red de telecomunicaciones (100) o, en parte, en una primera entidad (160) de servidor o, en parte, en una segunda entidad (130) de servidor, hace que el ordenador o la aplicación o el componente del dispositivo de comunicación (20), especialmente el elemento seguro (21), o el componente de red de la red de telecomunicaciones (100), o la primera entidad (160) de servidor, o la segunda entidad (130) de servidor lleven a cabo un método de acuerdo con una de las reivindicaciones 1 a 3.

9. Producto de programa informático para una instalación mejorada de una aplicación de servicio relacionada con un elemento seguro en un elemento seguro (21) que se encuentra en un dispositivo de comunicación (20), comprendiendo el producto de programa informático un programa informático almacenado en un medio de almacenamiento, comprendiendo el programa informático un código de programa que, cuando es ejecutado en un ordenador o en una aplicación o componente de un dispositivo de comunicación (20), especialmente el elemento seguro (21), o en un componente de red de una red de telecomunicaciones (100) o en una primera entidad (160) de servidor o en una segunda entidad (130) de servidor o, en parte, en una aplicación o componente de un dispositivo de comunicación (20) y, en parte, en un componente de red de una red de telecomunicaciones (100) o, en parte, en una primera entidad (160) de servidor o, en parte, en una segunda entidad (130) de servidor, hace que el ordenador o la aplicación o componente del dispositivo de comunicación (20), especialmente el elemento seguro (21), o el componente de red de la red de telecomunicaciones (100) o la primera entidad (160) de servidor o la segunda entidad (130) de servidor lleven a cabo un método de acuerdo con una de las reivindicaciones 1 a 3.

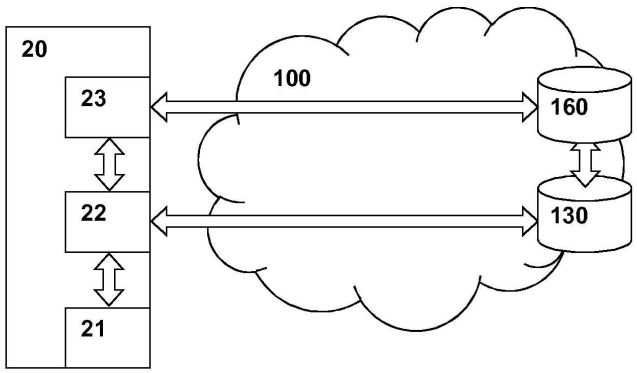
20
23
22
21
100
160
130

Fig. 1

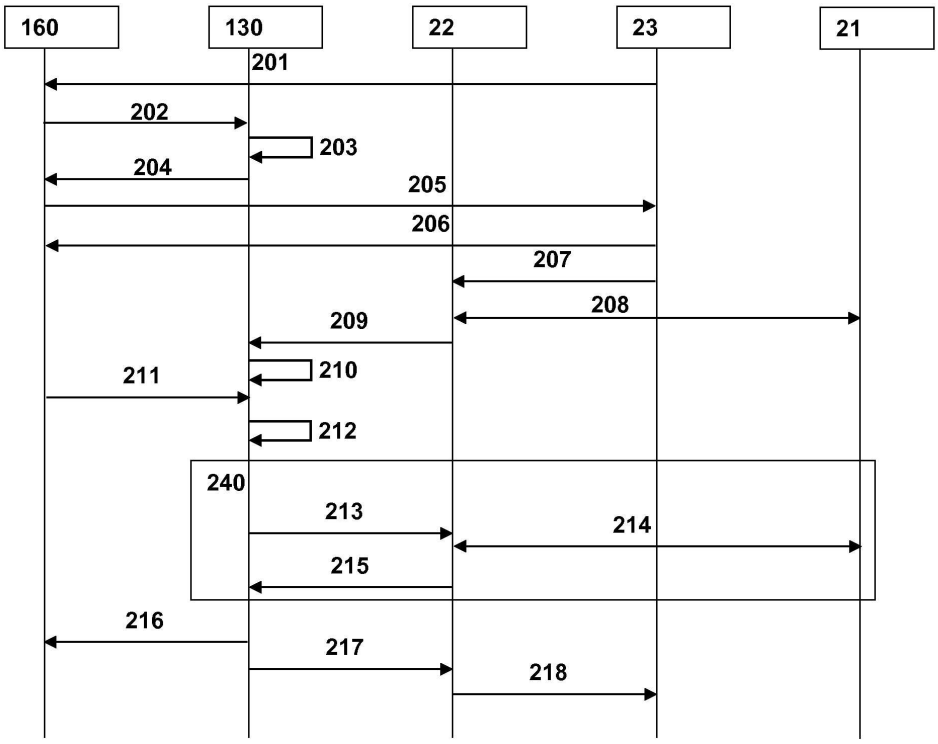
160
130
22
23
21
201
202
203
204
205
206
207
208
209
210
211
212
240
213
214
215
216
217
218

Fig. 2