(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 712 643**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04W 4/80 (2008.01)
H04W 4/50 (2008.01)
G06Q 20/04 (2012.01)
G06Q 20/22 (2012.01)
G06Q 30/06 (2012.01)
G06Q 20/32 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.02.2013 E 13000749 (5)**

(97) Fecha y número de publicación de la concesión europea: **21.11.2018 EP 2768199**

(54) Título: **Método para la transmisión a través de una red de telecomunicaciones de una información de autorización o de una autorización asociada con un terminal de telecomunicación, terminal de telecomunicación, sistema, programa informático y de programa informático**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.05.2019

(73) Titular/es:

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

(72) Inventor/es:

BOEGELSACK, MARTIN;
BARANIAK, ANDRZEJ y
MLECZKO, MARCIN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para la transmisión a través de una red de telecomunicaciones de una información de autorización o de una autorización asociada con un terminal de telecomunicación, terminal de telecomunicación, sistema, programa informático y producto de programa informático

Estado de la técnica
La invención se refiere a un método para la transmisión a través de una red de telecomunicaciones

- de una información de autorización almacenada en un área de almacenamiento de un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication)
o
- de una autorización asociada con un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC

de un primer terminal de telecomunicación a un segundo terminal de telecomunicación.

Además, la invención también se refiere a un terminal de telecomunicación y a un sistema que incluye un terminal de telecomunicación con una interfaz NFC (interfaz Near Field Communication) y una primera interfaz inalámbrica para la transmisión

- de una información de autorización almacenada en un área de almacenamiento del terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication)
o
- de una autorización asociada con el terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC

del terminal de telecomunicación a un segundo terminal de telecomunicación.

Además, la invención también se refiere a un programa informático con medios de codificación de programa y un producto de programa informático.

Los dispositivos terminales de telecomunicación, en particular los teléfonos móviles y otros dispositivos portátiles con una interfaz NFC (interfaz Near Field Communication) y, con ello, también con capacidades NFC –por ejemplo, ordenadores con pantallas sensibles al tacto (denominados Tablet Computer), PDA (Asistentes Digitales Personales) o similares– se pueden utilizar para servicios de pago, control de acceso, programas de lealtad (denominados Loyalty Programme), etc. Siempre y cuando el programa de aplicación, o bien la aplicación, y/o las claves asociadas con éste, las cuales están vinculadas con tales servicios, estén presentes en el elemento seguro (SE, secure element) del dispositivo móvil o teléfono móvil, o bien terminal de telecomunicación (por ejemplo, en la SIM/UICC-ID, junto con el conjunto de datos, el cual identifica al SP, así como a la aplicación (o bien la App) y al cliente), es posible que el autorizado, por lo general un cliente (y sólo el autorizado) del dispositivo móvil utilice estos servicios, o bien aplicaciones, en particular utilizando la interfaz NFC, esto es, para la realización de una transmisión de información local con un dispositivo opuesto, por ejemplo, un sistema de caja, o bien de entrada, para un lugar de reunión, o una máquina expendedora de billetes o un punto de venta o similares.

Ahora son concebibles muchos casos en los que, por ejemplo, el propietario original de la aplicación quiere transmitir con la clave “su” aplicación a otro cliente. Tales situaciones pueden ser, por ejemplo, la transmisión de entradas de conciertos en casos de impedimento o también como regalo, la transmisión de puntos de lealtad, la transmisión parcial o completa de tarjetas de pago, o la transmisión de derechos para la utilización de un vehículo o de una vivienda.

En el caso de las implementaciones actuales de servicios previstos para la utilización con una interfaz NFC únicamente está previsto, por motivos de seguridad, una transmisión de informaciones de autorización de una instalación de servidor (del proveedor del servicio solicitado o de la aplicación) a un terminal de telecomunicación, o bien un usuario; una transmisión de una información de autorización, o bien una autorización asociada con un terminal de telecomunicación, del primer terminal de telecomunicación al segundo terminal de telecomunicación de tal manera que los dispositivos terminales de telecomunicación están alejados el uno del otro más allá del alcance de la interfaz NFC no está prevista. El documento de patente WO 2009/060393 se refiere a un sistema para la transmisión de informaciones de autorización, las cuales se pueden utilizar por medio de una interfaz NFC, en donde tiene lugar la transmisión entre dos dispositivos de telecomunicación, y esta transmisión tiene lugar o bien a través de una instalación de servidor o bien, de manera alternativa, directamente a través de una interfaz NFC.

Publicación de la Invención
La invención se basa en la misión de indicar un método para la transmisión o bien de una información de autorización o bien de una autorización asociada con un terminal de telecomunicación de un primer terminal de telecomunicación que presenta una interfaz NFC a un segundo terminal de telecomunicación que presenta una interfaz NFC, con el cual es posible para un usuario el posibilitar la utilización de un servicio, o bien de una

aplicación, en el caso del segundo terminal de telecomunicación, el cual no estaba activado con anterioridad a la transmisión de la información de autorización, o bien de la autorización asociada con el primer terminal de telecomunicación, para la utilización de este servicio, o bien de esta aplicación, al menos no de manera similar, en donde el primer terminal de telecomunicación y el segundo terminal de telecomunicación, durante la transmisión de la información de autorización o de la autorización, están localizados separados el uno del otro relativamente mucho.

Esta tarea se resuelve de conformidad con la invención por medio de un método, según la reivindicación 1, para la transmisión a través de una red de telecomunicaciones

- de una información de autorización almacenada en un área de almacenamiento de un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication) o
- de una autorización asociada con un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC

de un primer terminal de telecomunicación a un segundo terminal de telecomunicación,
en donde en un primer momento, la información de autorización está almacenada en una primera área de almacenamiento del primer terminal de telecomunicación o la autorización está asociada con el primer terminal de telecomunicación y en donde, en un segundo momento posterior con respecto al primer momento, la información de autorización está almacenada en una segunda área de almacenamiento del segundo terminal de telecomunicación o la autorización está asociada con el segundo terminal de telecomunicación,
en donde el primer terminal de telecomunicación, además de la interfaz NFC, presenta una primera interfaz inalámbrica y el segundo terminal de telecomunicación, además de la interfaz NFC, presenta una segunda interfaz inalámbrica, en donde, para la transmisión de la información de autorización del primer terminal de telecomunicación al segundo terminal de telecomunicación, se utiliza la primera y segunda interfaz inalámbrica o, para la transmisión de la autorización, se utiliza al menos la primera interfaz inalámbrica, en donde el primer y segundo terminal de telecomunicación, durante la transmisión de la información de autorización o de la autorización, presentan una distancia el uno del otro que supera el alcance de la interfaz NFC.

A causa de esto, de conformidad con la presente invención es posible, de manera ventajosa, que la información de autorización, o bien la autorización, se transmita de tal manera que, por medio del segundo terminal de telecomunicación, se puede utilizar el servicio o la aplicación, la cual, antes de la transmisión de la información de autorización, o bien de la autorización, únicamente estaba vinculada, o bien asociada, con el primer terminal de telecomunicación.

En el caso del método de conformidad con la invención está previsto principalmente que una información de autorización se transmita del primer terminal de telecomunicación al segundo terminal de telecomunicación. Correspondientemente, el objeto de la presente invención es principalmente un método para la transmisión, a través de una red de telecomunicaciones, de una información de autorización almacenada en un área de almacenamiento de un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC de un primer terminal de telecomunicación a un segundo terminal de telecomunicación, en donde en un primer momento la información de autorización está almacenada en un primer área de almacenamiento del primer terminal de telecomunicación y en donde en un segundo momento posterior con respecto al primer momento la información de autorización está almacenada en una segunda área de almacenamiento del segundo terminal de telecomunicación, en donde el primer terminal de telecomunicación, además de la interfaz NFC, presenta una primera interfaz inalámbrica y el segundo terminal de telecomunicación, además de la interfaz NFC, presenta una segunda interfaz inalámbrica, en donde, para la transmisión de la información de autorización del primer terminal de telecomunicación al segundo terminal de telecomunicación, se utiliza la primera y segunda interfaz inalámbrica, en donde, durante la transmisión de la información de autorización, el primer y segundo terminal de telecomunicación presentan una distancia el uno del otro que supera el alcance de la interfaz NFC.

Además, en el caso del método de conformidad con la invención, está también previsto, sin embargo, que se transmita una autorización asociada con un terminal de telecomunicación y, precisamente, de tal manera que, antes de la transmisión, la autorización está asociada con el primer terminal de telecomunicación y, después de la transmisión, también está asociada por lo menos (o bien en partes, o bien para partes de la autorización) con el segundo terminal de telecomunicación. Correspondientemente, también es objeto de la presente invención un método para la transmisión, en particular a través de una red de telecomunicaciones, de una autorización asociada con un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC de un primer terminal de telecomunicación a un segundo terminal de telecomunicación (o bien la transmisión de la correspondiente asociación), en donde en un primer momento la autorización está asociada con el primer terminal de telecomunicación y en donde en un segundo momento posterior con respecto al primer momento la autorización está asociada con el segundo terminal de telecomunicación, en donde el primer terminal de telecomunicación, además de la terminal NFC, presenta una primera interfaz inalámbrica (y el segundo terminal de telecomunicación presenta típicamente y, en particular, también además de la interfaz NFC, una segunda interfaz inalámbrica), en donde, para la transmisión de la autorización, se utiliza al menos la primera interfaz inalámbrica, en donde, durante

la transmisión de la información de autorización o de la autorización, el primer y segundo terminal de telecomunicación presentan una distancia el uno del otro que supera el alcance de la interfaz NFC.

Según la presente invención son por lo tanto posibles distintas vías, o bien tipos, de la transmisión de la información de autorización, o bien de la autorización,

- por un lado, una denominada transmisión “Peer-2-Peer”, esto es, la transmisión más o menos directa (esto es, en particular, no transmitida a través de una instalación de servidor) de la información de autorización, o bien de la autorización (esto es, en particular, de (datos de) la aplicación, o bien de la aplicación y/o de los correspondientes datos de acceso) del primer terminal de telecomunicación al segundo terminal de telecomunicación,
- además, una denominada trasmisión “Client-Server”, esto es, se transmite la información de autorización, o bien la autorización (esto es, en particular, los (datos de) aplicación, o bien la aplicación y/o los correspondientes datos de acceso) del primer terminal de telecomunicación a la instalación de servidor y se garantiza (en particular, por medio de la utilidad, o bien la aplicación y, en particular, según las reglas de la categoría correspondiente) (en particular, a través de una orden correspondiente a la instalación de servidor) que la transmisión se ponga en acción por medio de la instalación de servidor (o bien, por medio del sistema externo del proveedor de servicios (SP-Backend)) en el segundo terminal de telecomunicación y la información de autorización, o bien la autorización (esto es, en particular, la aplicación con los datos de acceso correspondientes) se transmita al dispositivo de destino, esto es, al segundo terminal de telecomunicación; y
- por último, la transmisión de la autorización (en forma de una modificación de la asociación de la autorización del primer terminal de telecomunicación al segundo terminal de telecomunicación) se modifica a través de una modificación de la asignación en la instalación de servidor (esto es, en el sistema Backend del proveedor de servicios), en donde no tiene lugar ninguna transferencia, o bien ninguna transmisión de los datos de acceso (del primer terminal de telecomunicación al segundo terminal de telecomunicación), sino únicamente la correspondiente asignación en la instalación de servidor.

En el caso de que en el (primer, o bien segundo) terminal de telecomunicación esté almacenada la información de autorización, está preferiblemente previsto de conformidad con la invención que la información de autorización en el primer terminal de telecomunicación esté almacenada en un primer elemento seguro (SE, secure element), en el que también se encuentra la primera área de almacenamiento y que la información de autorización en el segundo terminal de telecomunicación esté almacenada en un segundo elemento seguro, en el que también se encuentra la segunda área de almacenamiento, en donde el primer y segundo elemento seguro es, en particular, un elemento SE (Secure Element) según el estándar GlobalPlatform o una UICC (Universal Integrated Circuit Card) o una tarjeta microSD (Secure Digital card) o una tarjeta ICC (integrated circuit card) o un circuito integrado.

A causa de esto, de conformidad con la invención es ventajosamente posible que el nivel de seguridad de una aplicación NFC, o bien de un servicio correspondiente, no se disminuya a través de la transmisión de la información de autorización según la presente invención, sino que, por el contrario, el nivel de seguridad sea constante –por ejemplo, con respecto a una trasmisión a través de la interfaz NFC de un terminal de telecomunicación a otro terminal de telecomunicación– o, en todo caso para casos relevantes en términos prácticos, por el contrario se reduzca únicamente de forma insignificante.

De conformidad con la invención, está previsto que tanto el primer terminal de telecomunicación como también el segundo terminal de telecomunicación presente tanto una interfaz NFC como también una interfaz inalámbrica (esto es, el primer terminal de telecomunicación presenta la primera interfaz inalámbrica y el segundo terminal de telecomunicación presenta la segunda interfaz inalámbrica). En el caso del método de conformidad con la invención y también en el caso del terminal de telecomunicación de conformidad con la invención y el sistema de conformidad con la invención, una transmisión de información tiene lugar por lo menos entre el primer terminal de telecomunicación y una instalación de servidor (por lo general del proveedor de servicios del servicio, o bien de la aplicación, la cual ha de ser utilizada por un usuario por medio del primer, o bien segundo, terminal de telecomunicación). Esta transmisión de información (con respecto a la información de autorización o con respecto a la autorización (asociada con el terminal de telecomunicación)) entre por lo menos el primer terminal de telecomunicación y la instalación de servidor se produce, de conformidad con la invención, a través de la interfaz inalámbrica (esto es, a través de la primera interfaz inalámbrica durante la comunicación entre el primer terminal de telecomunicación y la instalación de servidor (en relación con la información de autorización o en relación con la autorización), o bien a través de la primera y segunda interfaz inalámbrica durante la comunicación entre el primer terminal de telecomunicación y el segundo terminal de telecomunicación (en relación con la información de autorización). En particular, la (primera, o bien segunda) interfaz inalámbrica se trata, de conformidad con la invención, de una interfaz de radio inalámbrica relativamente de corto alcance como, por ejemplo, una interfaz de radio local –por ejemplo, una interfaz de radio WLAN (Wireless Local Area Network) o también una interfaz Bluetooth– o, en cambio, de una interfaz de radio de amplio alcance (WWAN, Wireless Wide Area Network) –por ejemplo, una interfaz de telefonía móvil convencional (del primer, o bien segundo, terminal de telecomunicación), en particular según uno de los estándares conocidos, esto es, por ejemplo, según el estándar GSM (Global System for Mobile communication) (interfaz de telefonía móvil de la segunda generación) y/o según el estándar UMTS

(Universal Mobile Telecommunication System) (interfaz de telefonía móvil de la tercera generación) y/o según el estándar EDGE (Enhanced Data Rates for GMS Evolution) y/o según el estándar LTE (Long Term Evolution) (interfaz de telefonía móvil de la cuarta generación). De conformidad con la invención, la (primera y segunda) interfaz inalámbrica también puede estar configurada alternativamente de tal manera que ésta presente tanto una interfaz de radio de corto alcance como también una interfaz de radio de amplio alcance (o bien por medio de la utilización de componentes integrados, o bien disposiciones de antenas, o, en cambio, por medio de la utilización de distintos componentes estructurales, por un lado para la interfaz de radio de corto alcance y, por otro lado, para la interfaz de radio de amplio alcance), las cuales también se pueden operar particularmente en paralelo.

De conformidad con la presente invención, está previsto que tanto el primer terminal de telecomunicación como también el segundo terminal de telecomunicación disponga de una interfaz NFC y sea capaz de intercambiar, a través de la interfaz NFC, informaciones para la utilización de servicios, o bien aplicaciones (con estaciones secundarias correspondientes en forma de terminales NFC o similares). De conformidad con la invención, la interfaz NFC (tanto del primer terminal de telecomunicación como también del segundo terminal de telecomunicación) está concebida de tal manera que ésta funciona para aplicaciones basadas en NFC generales, para aplicaciones MiFare, para aplicaciones Calypso o cualquier otro sistema de gestión de identificación o autorización sobre la base de NFC (esto es, típicamente con datos de acceso/claves seguros en el dispositivo, el SE (elemento seguro) o en un sistema de copias de seguridad (externo) (o bien, una instalación de servidor).

De conformidad con la presente invención, se elimina la desventaja del estado de la técnica por la cual no está prevista una transmisión de la información de autorización (o bien una transmisión de una autorización asociada con un primer terminal de telecomunicación) del primer terminal de telecomunicación al segundo terminal de telecomunicación a través de una distancia que va más allá del alcance de la interfaz NFC. Para ello está previsto que en los dispositivos terminales de telecomunicación, esto es, en los dispositivos móviles (y aquí en particular dentro del elemento seguro SE del primer, o bien segundo, terminal de telecomunicación), y también en la instalación de servidor (externa en relación con los dispositivos terminales de telecomunicación) (o bien, en el sistema Backend) existan medios, los cuales permiten transmitir una información de autorización, o bien una autorización (en particular, en forma de una aplicación correspondiente a los servicios, o bien aplicaciones, solicitados en relación con la transmisión con las claves/datos de acceso correspondientes) del primer terminal de telecomunicación al segundo terminal de telecomunicación (o bien transmitir por lo menos la asociación del primer terminal de telecomunicación al segundo terminal de telecomunicación), en donde, de conformidad con la invención, esta transmisión se efectúa de manera segura particularmente de tal manera que, o bien se consigue un nivel de seguridad igual de alto con respecto a una transmisión utilizando la interfaz NFC (esto es, en particular, del primer terminal de telecomunicación directamente al segundo terminal de telecomunicación) o bien, en cambio, por lo menos un nivel de seguridad, el cual no se sitúa significativamente por debajo.

De conformidad con la invención, es por ejemplo posible transmitir la información de autorización del primer terminal de telecomunicación al segundo terminal de telecomunicación, aunque el primer y segundo terminal de telecomunicación están situados separados el uno del otro varios metros (por ejemplo, dentro de una casa o un edificio).

De conformidad con la invención, es preferido que, durante la transmisión de la información de autorización o de la autorización, el primer y segundo terminal de telecomunicación presenten una distancia el uno del otro que supere el alcance de una red inalámbrica local (WLAN, Wireless Local Area Network).

A causa de esto, de conformidad con la invención es, por ejemplo, posible transmitir la información de autorización del primer terminal de telecomunicación al segundo terminal de telecomunicación, aunque el primer y segundo terminal de telecomunicación están situados separados el uno del otro varios centenares de metros o también varios kilómetros (hasta varios centenares o varios miles de kilómetros), por ejemplo, dentro de una ciudad o dentro de un país o en continentes distintos.

De conformidad con la invención, es además preferido que la transmisión de la información de autorización o de la asociación de la autorización del primer terminal de telecomunicación al segundo terminal de telecomunicación autorice al usuario del segundo terminal de telecomunicación o bien:

- en lugar del usuario del primer terminal de telecomunicación, o bien
- además del usuario del primer terminal de telecomunicación, para la utilización de un servicio o de una cosa.

A causa de esto, de conformidad con la invención es ventajosamente posible, en particular, dependiendo de la categoría de la(s) aplicación(es) (vinculada(s) con la información de autorización, o bien la autorización), operar la transmisión de conformidad con la invención del primer terminal de telecomunicación al segundo terminal de telecomunicación en distintos modos de operación como, por ejemplo, “copy and paste” (esto es, además del usuario del primer terminal de telecomunicación, el usuario en el segundo terminal de telecomunicación está autorizado para la utilización de un servicio o de una cosa) –por ejemplo, para aplicaciones del control de acceso, una función de pago o similares– o también “cut and paste” (esto es, en lugar del usuario del primer terminal de telecomunicación, el usuario del segundo terminal de telecomunicación está autorizado para la utilización de un

servicio o una cosa) –por ejemplo, para aplicaciones de puntos de lealtad (puntos loyalty), de entradas para eventos, de determinados billetes del transporte público (de personas) (transporte de cercanías y/o de larga distancia).

Además, de conformidad con la invención, es preferido que la transmisión de la información de autorización o de la asociación de la autorización del primer terminal de telecomunicación al segundo terminal de telecomunicación autorice al usuario del segundo terminal de telecomunicación

- durante la duración de un intervalo de tiempo predeterminado o
- dentro de un área geográfica predeterminada o
- para una combinación de una condición temporal y una geográfica, para la utilización de un servicio o de una cosa.

Por lo tanto, de conformidad con la invención, es ventajosamente posible que se puedan establecer otras condiciones como, por ejemplo, la transmisibilidad de la aplicación y de los datos de acceso y eventuales restricciones de uso (en particular, temporales, o bien locales) tras la transmisión. De conformidad con la invención, estas condiciones se pueden establecer, por ejemplo, por parte del proveedor de servicios (Service Provider), quien es el editor de la prestación (o bien del servicio) o de la utilidad (o bien de la aplicación) –a modo de ejemplo, un billete de transporte de corta distancia únicamente se podría transmitir hasta una determinada cantidad de procesos de transmisión (por ejemplo, 10 veces)–. Alternativa o acumulativamente a esto, estas condiciones (que limitan la utilización de la información de autorización, o bien de la autorización, por parte del usuario del segundo terminal de telecomunicación) también se pueden limitar, de conformidad con la invención, por parte del usuario del primer terminal de telecomunicación (esto es, por lo general del cliente del proveedor de servicios, el cual ha adquirido, o bien pagado, originalmente la prestación, o bien la utilidad (servicio/aplicación) –a modo de ejemplo, una persona amiga (como usuaria del segundo terminal de telecomunicación) únicamente podría utilizar un automóvil a motor en un determinado fin de semana o también recibir un determinado importe en una tarjeta monedero.

De conformidad con la invención es además preferido que el primer elemento seguro para la transmisión de la información de autorización presente una primera interfaz de transmisión y el segundo elemento seguro para la transmisión de la información de autorización presente una segunda interfaz de transmisión, en donde la información de autorización se transmite de forma transparente a través de la primera y segunda interfaz de transmisión utilizando un canal de transmisión, en particular, de forma protegida, en particular cifrada.

A causa de esto, de conformidad con la invención es ventajosamente posible que, por un lado, se alcance un alto grado de seguridad durante la transmisión de la información de autorización, o bien de la autorización, y, por otro lado, también un gran grado de modularidad en el sentido de que se puede transmitir la aplicación que se desee –en particular dentro del (primer, o bien segundo) elemento seguro según el método de conformidad con la invención, o bien se puede transmitir la información de autorización, o bien autorización, relacionada con ésta.

Además, de conformidad con la invención también es preferido que, como información de autorización, se transmitan:

- tanto informaciones en relación con una aplicación utilizada o que se desea utilizar dentro del primer y/o del segundo elemento seguro e implicada en la transmisión
- como también informaciones confidenciales y protegidas conectadas con la aplicación implicada en la transmisión (credential informations).

A causa de esto, de conformidad con la invención es ventajosamente posible que sea posible una transmisión especialmente fácil de la información de autorización, o bien de la autorización, porque las informaciones necesarias para la utilización del servicio solicitado o de la aplicación desde el segundo terminal de telecomunicación no sólo se transmiten informaciones confidenciales y protegidas conectadas con la aplicación implicada en la transmisión (credential informations), sino también informaciones en relación con la aplicación implicada en la transmisión y utilizada o que se desea utilizar dentro del primer y/o del segundo elemento seguro. A causa de esto, de conformidad con la invención está automáticamente garantizado que, debido a distintos estados de versiones de la aplicación utilizada e implicada en la transmisión, no se den limitaciones de la usabilidad del servicio o de la aplicación en el caso del segundo terminal de telecomunicación, o bien por parte del usuario del segundo terminal de telecomunicación.

Otro objeto de la presente invención se refiere a un terminal de telecomunicación, según la reivindicación 7, con una interfaz NFC (interfaz Near Field Communication) y una primera interfaz inalámbrica para la transmisión

- de una información de autorización almacenada en un área de almacenamiento del terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication) o
- de una autorización asociada con el terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC del terminal de telecomunicación en un segundo terminal de telecomunicación,

en donde el terminal de telecomunicación está configurado de tal manera para almacenar la información de autorización en una primera área de almacenamiento del terminal de telecomunicación, en donde el terminal de telecomunicación está configurado para la transmisión de la información de autorización del terminal de telecomunicación al segundo terminal de telecomunicación utilizando la primera interfaz inalámbrica, en donde, durante la transmisión de la información de autorización, el terminal de telecomunicación y el segundo terminal de telecomunicación presentan una distancia el uno del otro que supera el alcance de la interfaz NFC.

Por medio de un terminal de telecomunicación tal, de conformidad con la invención es posible de manera ventajosa que la información de autorización, o bien la autorización, se transmita de tal manera que, por medio del segundo terminal de telecomunicación, se puede utilizar el servicio o la aplicación, la cual, antes de la transmisión de la información de autorización, o bien la autorización, únicamente estaba vinculada, o bien asociada, con el primer terminal de telecomunicación, en donde los dispositivos terminales de telecomunicación están separados el uno del otro al menos varios metros, esto es, presentan una distancia el uno del otro que supera el alcance de la interfaz NFC.

De conformidad con la invención, es asimismo particularmente preferido, en relación con el terminal de telecomunicación, que la información de autorización en el primer terminal de telecomunicación esté almacenada en un primer elemento seguro, en el que también se encuentra la primera área de almacenamiento, en donde el primer elemento seguro es en particular un elemento SE (Secure Element) según el estándar GlobalPlatform o una UICC (Universal Integrated Circuit Card) o una tarjeta microSD (Secure Digital card) o una tarjeta ICC (integrated circuit card) o un circuito integrado.

Mediante la utilización de elementos seguros (SE) tanto en el primer terminal de telecomunicación como también en el segundo terminal de telecomunicación, de conformidad con la invención se puede realizar, a pesar de la transmisión de la información de autorización, o bien de la autorización, un nivel de seguridad suficientemente alto, en particular con respecto al robo de datos, o bien acciones fraudulentas, para la obtención ilegal de servicios, o bien medios de pago, con costes razonables.

Además, de conformidad con la invención, en relación con el terminal de telecomunicación es particularmente preferido que el primer elemento seguro para la transmisión de la información de autorización presente una primera interfaz de transmisión, en donde la información de autorización se transmite de forma transparente a través de la primera interfaz de transmisión utilizando un canal de transmisión, en particular, de forma protegida, en particular, cifrada, en donde el terminal de telecomunicación está particularmente configurado de tal manera que, como información de autorización, se transmiten

- tanto informaciones en relación con una aplicación utilizada o que se desea utilizar dentro del primer y/o del segundo elemento seguro e implicada en la transmisión
- como también informaciones confidenciales y protegidas conectadas con la aplicación implicada en la transmisión (credentials informations).

Otro objeto de la presente invención se refiere a un sistema según la reivindicación 10 que incluye un primer terminal de telecomunicación y un segundo terminal de telecomunicación para la transmisión, a través de una red de telecomunicaciones,

- de una información de autorización almacenada en un área de almacenamiento de un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication) o
- de una autorización asociada con un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC

del primer terminal de telecomunicación al segundo terminal de telecomunicación,

en donde el sistema está configurado de tal manera para almacenar la información de autorización en una primera área de almacenamiento del primer terminal de telecomunicación o para asociar la autorización con el primer terminal de telecomunicación y/o en donde el sistema está configurado de tal manera para almacenar la información de autorización en una segunda área de almacenamiento del segundo terminal de telecomunicación o para asociar la autorización con el segundo terminal de telecomunicación,
en donde el primer terminal de telecomunicación, además de la interfaz NFC, presenta una primera interfaz inalámbrica y el segundo terminal de telecomunicación, además de la interfaz NFC, presenta una segunda interfaz inalámbrica, en donde el sistema está configurado para la transmisión de la información de autorización del primer terminal de telecomunicación al segundo terminal de telecomunicación utilizando la primera y segunda interfaz inalámbrica o está configurado para la transmisión de la autorización utilizando al menos la primera interfaz inalámbrica, en donde el sistema está configurado de tal manera que el primer y segundo terminal de telecomunicación, durante la transmisión de la información de autorización, o bien de la autorización, presentan una distancia el uno del otro que supera el alcance de la interfaz NFC.

Por medio de un sistema tal, de conformidad con la invención es posible de manera ventajosa que la información de autorización, o bien la autorización, para la utilización del servicio o de la aplicación se pueda transmitir por medio del segundo terminal de telecomunicación desde el primer terminal de telecomunicación, en donde los dispositivos terminales de telecomunicación están separados el uno del otro al menos varios metros, esto es, presentan una distancia el uno del otro que supera el alcance de la interfaz NFC.

De conformidad con la invención, en relación con el sistema es particularmente preferido que la información de autorización en el primer terminal de telecomunicación esté almacenada en un primer elemento seguro (SE, secure element), en el que también se encuentra el primer área de almacenamiento, y que la información de autorización en el segundo terminal de telecomunicación esté almacenada en un segundo elemento seguro, en el que también se encuentra la segunda área de almacenamiento, en donde el primer y segundo elemento seguro es, en particular, un elemento SE (Secure Element) según el estándar GlobalPlatform o una UICC (Universal Integrated Circuit Card) o una tarjeta microSD (Secure Digital card) o una tarjeta ICC (integrated circuit card).

La utilización de elementos seguros (SE) tanto en el primer terminal de telecomunicación como también en el segundo terminal de telecomunicación posibilita, a pesar de la transmisión de la información de autorización, o bien de la autorización, el alcanzar un nivel de seguridad suficientemente alto, en particular, con respecto al robo de datos, o bien acciones fraudulentas, para la obtención ilegal de servicios, o bien de medios de pago, con costes razonables.

Además, la presente invención se refiere a un programa informático, según la reivindicación 12, con medios de codificación de programa, con cuya ayuda se pueden realizar todos los pasos del método de conformidad con la invención, cuando el programa informático se ejecuta en una instalación que se puede programar.

Además, es objeto de la presente invención un producto de programa informático, según la reivindicación 13, con un medio legible por ordenador y un programa informático almacenado en el medio legible por ordenador con medios de codificación de programa, los cuales son apropiados para que se puedan realizar todos los pasos del método de conformidad con la invención, cuando el programa informático se ejecuta en una instalación que se puede programar, en particular, como parte del sistema, o en el primer o segundo terminal de telecomunicación.

Otros detalles, características y ventajas de la invención se deducen de los dibujos, así como de la siguiente descripción de formas de realización preferidas mediante los dibujos. Los dibujos únicamente ilustran en este caso formas de realización ejemplares de la invención, las cuales no limitan las ideas fundamentales de la invención. La invención se define por las reivindicaciones independientes adjuntas y sus reivindicaciones dependientes.

Descripción breve de los dibujos

La Figura 1 muestra, de forma esquemática, una primera variante del método de conformidad con la invención.

la Figura 2 muestra, de forma esquemática, una segunda variante del método de conformidad con la invención.

la Figura 3 muestra, de forma esquemática, un sistema de conformidad con la invención con un primer y un segundo terminal de telecomunicación.

Formas de realización de la Invención

La presente invención se describe haciendo referencia a realizaciones especiales y haciendo referencia a los dibujos adjuntos, en donde la invención no está limitada, sin embargo, a estas realizaciones y a estos dibujos, sino que está definida por las reivindicaciones de patente. Los dibujos no son limitantes. A efectos de representación, en los dibujos determinados elementos pueden estar representados ampliados, o bien exagerados, así como no a escala.

En caso de que no se indique específicamente lo contrario, la utilización de un artículo indeterminado o determinado en relación con una palabra en el número singular, por ejemplo, “un”, “una”, “de uno”, “de una”, “el”, “la”, también incluye el plural de una palabra tal. Las denominaciones “primero”, “primera”, “segundo”, “segunda”, etc. en la descripción y en las reivindicaciones se utilizan para diferenciar entre elementos similares o iguales que se desea diferenciar y no obligatoriamente para la descripción de una sucesión temporal u otra. Los términos utilizados de tal manera se deben ver, en principio, como intercambiables bajo condiciones correspondientes.

En la figura 1 está representada de forma esquemática una primera variante de un método de conformidad con la invención. El método de conformidad con la invención sirve, según la primera variante del método de conformidad con la invención, para la transmisión, a través de una red de telecomunicaciones 100, de una información de autorización almacenada en un área de almacenamiento de un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication) de un primer terminal de telecomunicación 10 a un segundo terminal de telecomunicación 20.

Para esto, el primer terminal de telecomunicación 10 presenta de conformidad con la invención, en particular, un primer elemento seguro 12 y el segundo terminal de telecomunicación 20 presenta para esto de conformidad con la invención, en particular, un segundo elemento seguro 22. Dentro del primer terminal de telecomunicación 10 está

prevista una primera área de almacenamiento 11 para el almacenamiento de la información de autorización, en donde la primera área de almacenamiento 11 está prevista, en particular, dentro del primer elemento seguro 12. Igualmente, dentro del segundo terminal de telecomunicación 20 está prevista una segunda área de almacenamiento 21 para el almacenamiento de la información de autorización, en donde la segunda área de almacenamiento 21 está prevista, en particular, dentro del segundo elemento seguro 22.

El primer terminal de telecomunicación 10 presenta, de conformidad con la invención, además de la, o bien "su", interfaz NFC una primera interfaz inalámbrica y el segundo terminal de telecomunicación 20, igualmente además de la, o bien "su", interfaz NFC una segunda interfaz inalámbrica. Para la transmisión de la información de autorización del primer terminal de telecomunicación 10 al segundo terminal de telecomunicación 20 se utiliza, según la primera variante del método de conformidad con la invención, la primera y segunda interfaz inalámbrica, en donde el primer y segundo terminal de telecomunicación 10, 20, durante la transmisión de la información de autorización, presentan una distancia el uno del otro que supera el alcance de la interfaz NFC, esto es, queda excluida una transmisión directa de la información de autorización utilizando la interfaz NFC. En este caso, tiene lugar o bien una comunicación, o bien transmisión, directa de la información de autorización del primer terminal de telecomunicación 10 al segundo terminal de telecomunicación 20, o bien, en cambio, tiene lugar una transmisión de la información de autorización del primer terminal de telecomunicación 10 a la instalación de servidor y, a continuación, una transmisión de la información de autorización de la instalación de servidor al segundo terminal de telecomunicación 20. Ambos subcasos tienen que estar representados de forma indicada como por medio de las dos representaciones de flechas en la figura 1.

De conformidad con la invención, con esto, como resultado en un primer momento la información de autorización está almacenada en la primera área de almacenamiento 11 del primer terminal de telecomunicación 10 y, en un segundo momento posterior con respecto al primer momento, la información de autorización está almacenada en la segunda área de almacenamiento 21 del segundo terminal de telecomunicación 20, por lo cual un servicio, o bien una aplicación, también se puede acceder, o bien utilizar, en el segundo terminal de telecomunicación 20, o bien para su usuario.

En la figura 2 está representada de forma esquemática una segunda variante del método de conformidad con la invención.

El método de conformidad con la invención según la segunda variante sirve para la transmisión, en particular a través de una red de telecomunicaciones 100, de una autorización asociada con un dispositivo de telecomunicación y que se puede utilizar por medio de una interfaz NFC, del primer terminal de telecomunicación 10 al segundo terminal de telecomunicación 20.

El primer terminal de telecomunicación 10 presenta para ello, conforme a la primera variante, en particular, un primer elemento seguro 12 y el segundo terminal de telecomunicación 20 presenta para ello, conforme a la primera variante, igualmente, en particular, un segundo elemento seguro 22. Típicamente, también según la segunda variante, dentro del primer terminal de telecomunicación 10 está prevista una primera área de almacenamiento 11 para el almacenamiento de una información de autorización, en donde la primera área de almacenamiento 11 está prevista, en particular, dentro del primer elemento seguro 12. Asimismo, en el caso de la segunda variante, dentro del segundo terminal de telecomunicación 20 también está prevista típicamente una segunda área de almacenamiento 21 para el almacenamiento de la información de autorización, en donde la segunda área de almacenamiento 21 está prevista, en particular, dentro del segundo elemento seguro 22.

También en el caso de la segunda variante, el primer terminal de telecomunicación 10 presenta, de conformidad con la invención, además de la, o bien "su", interfaz NFC una primera interfaz inalámbrica y, el segundo terminal de telecomunicación 20, presenta asimismo, además de la, o bien "su", interfaz NFC una segunda interfaz inalámbrica. En el caso de la segunda variante, para la transmisión de la autorización se utiliza al menos la primera interfaz inalámbrica, en donde, durante la transmisión de la autorización, el primer y segundo terminal de telecomunicación 10, 20 presentan una distancia el uno del otro que supera el alcance de la interfaz NFC, esto es, queda excluida una transmisión directa de la información de autorización utilizando la interfaz NFC.

De conformidad con la invención, en un primer momento la autorización está asociada con el primer terminal de telecomunicación 10 y, en un segundo momento posterior con respecto al primer momento, la autorización está asociada con el segundo terminal de telecomunicación 20, por lo cual un servicio, o bien una aplicación, también se puede acceder, o bien utilizar, en el segundo terminal de telecomunicación 20, o bien para su usuario. En este caso no tiene lugar obligatoriamente una comunicación, o bien transmisión, directa de una información del primer terminal de telecomunicación 10 al segundo terminal de telecomunicación 20, sino que una asociación, correspondiente, por ejemplo, a un indicador o una referencia, se modifica en una instalación de servidor 101 de tal manera que –en relación con la utilización de un servicio o de una aplicación– un primer indicador o una primera referencia 110, o bien una asociación, la cual existía en el primer momento con el primer terminal de telecomunicación 10, presenta en el segundo momento un segundo indicador o una segunda referencia 120, o bien una asociación, con el segundo terminal de telecomunicación 20. Obligatoriamente necesario para ello es únicamente una transmisión de información del primer terminal de telecomunicación 10 a la instalación de servidor 101, lo cual está indicado en la

figura 2 por medio de una flecha. Una instalación de servidor correspondiente a la instalación de servidor 101 representada en la figura 2 está también típicamente presente en el caso de la primera variante del método, en particular, como parte de la red de telecomunicaciones 100, o bien unida con ésta.

En la figura 3 está representado de forma esquemática un sistema de conformidad con la invención con un primer terminal de telecomunicación 10, un segundo terminal de telecomunicación 20 y una instalación de servidor 101. El primer terminal de telecomunicación 10 presenta un primer elemento seguro 12 y el segundo terminal de telecomunicación 20 presenta un segundo elemento seguro 22.

El primer, o bien segundo, terminal de telecomunicación 10, 20 se puede tratar, de conformidad con la invención, de cualquier “dispositivo personal”, en particular, teléfonos móviles y otros dispositivos portátiles, los cuales están equipados con una interfaz NFC (interfaz Near Field Communication) y, con ello, también con capacidades NFC – por ejemplo, ordenadores con pantallas sensibles al tacto (denominados Tablet Computer), PDA (Asistentes Digitales Personales)–. Dentro del primer y segundo terminal de telecomunicación 10, 20 (o bien, unido con éste) se encuentra un elemento seguro, así como aplicaciones, las cuales se pueden utilizar en relación con el elemento seguro. Los elementos seguros están típicamente alojados en elementos de hardware certificados y a prueba de manipulaciones (del primer, o bien segundo, terminal de telecomunicación), los cuales están protegidos contra el acceso no autorizado. De conformidad con la invención, estos “Secure Elements” pueden ser elementos instalados o insertados, en particular, en forma de UICC-ID, microSD, ICC instaladas de manera fija o similar, los cuales utilizan, en particular, estándares industriales habituales, como GP (GlobalPlatform), ISO o similares, o son compatibles con estos. Los datos de aplicación, así como las informaciones confidenciales y protegidas conectadas con la aplicación implicada en la transmisión (credential informations) también se denominan a continuación como datos sensibles.

Los datos sensibles, los cuales están almacenados en los elementos seguros (o bien “Secure Elements”), se pueden hacer accesibles para dispositivos, o bien unidades, externos a través de una o un grupo de aplicaciones, las cuales están instaladas en el “Secure Element” junto con estos. Este acceso se produce a través de distintos tipos de interfaces, como contacted I/O, SWP, CAT o similares. Correspondientemente, el primer elemento seguro 12 presenta, según la representación ejemplar en la figura 3, una primera aplicación 13 con primeros datos 14 confidenciales y que se desea proteger correspondientes, una segunda aplicación 13’ con segundos datos 14’ confidenciales y que se desea proteger correspondientes y una tercera aplicación 13’’ con terceros datos 14’’ confidenciales y que se desea proteger correspondientes. En este caso, la primera, segunda y tercera aplicación 13, 13’, 13’’ representan una cantidad cualquiera de aplicaciones de este tipo del primer elemento seguro 12 y los primeros, segundos y terceros datos 14, 14’, 14’’ corresponden a una cantidad cualquiera de datos confidenciales y que se desea proteger correspondientes. El segundo elemento seguro 22 presenta, según la representación ejemplar en la figura 3, una cuarta aplicación 23 con cuartos datos 24 confidenciales y que se desea proteger correspondientes, una quinta aplicación 23’ con quintos datos 24’ confidenciales y que se desea proteger correspondientes y una sexta aplicación 23’’ con sextos datos 24’’ confidenciales y que se desea proteger correspondientes. En este caso, la cuarta, quinta y sexta aplicación 23, 23’, 23’’ representan una cantidad cualquiera de aplicaciones de este tipo del segundo elemento seguro 22 y los cuartos, quintos y sextos datos 24, 24’, 24’’ corresponden a una cantidad cualquiera de datos confidenciales y que se desea proteger correspondientes.

De conformidad con la invención, está previsto transmitir tales datos confidenciales y que se desea proteger entre el primer elemento seguro 12 y el segundo elemento seguro 22 (o también entre el primer elemento seguro 12 y un sistema externo como la instalación de servidor 101, en donde el primer y segundo terminal de telecomunicación 10, 20, durante la transmisión de los datos confidenciales y que se desea proteger, esto es, durante la transmisión de la información de autorización, presentan una distancia (de, correspondientemente, pocos varios metros) el uno del otro que supera el alcance de la interfaz NFC, o bien presentan una distancia mayor que va aún más allá de varios kilómetros hasta varios cientos o miles de kilómetros.

Para ello, el sistema de conformidad con la invención reproducido en la figura 3 presenta, en particular, dentro del elemento seguro 12, 22 respectivo, una aplicación de transmisión que, en lo sucesivo, también se denomina como “aplicación de transferencia”, o bien como “xfer-App”. Una primera aplicación de transmisión 15 está prevista en el primer elemento seguro 12 y una segunda aplicación de transmisión 25 está prevista en el segundo elemento seguro 22. La primera aplicación de transmisión 15 incluye o está unida con una primera interfaz 16 con las aplicaciones 13, 13’, 13’’ (es decir, a modo de ejemplo, la primera, segunda, o bien tercera) disponibles en el primer elemento seguro 12. La primera aplicación de transmisión 15 incluye además, o bien está unida con, una segunda interfaz 17 para la comunicación con el segundo terminal de telecomunicación 20 (en particular, el segundo elemento seguro 22) y/o la instalación de servidor 101 y/o una primera aplicación de dispositivo 19 (en lo sucesivo también denominada como “Device App”) disponible en el primer terminal de telecomunicación 10, aunque fuera del primer elemento seguro 12. La primera aplicación de transmisión 15, la primera interfaz 16 y la segunda interfaz 17 forman en conjunto una primera interfaz de transmisión 18, la cual, para la transmisión de la información de autorización, está disponible de conformidad con la invención preferiblemente en el primer terminal de telecomunicación 10. Correspondientemente a la primera aplicación de transmisión 15, la segunda aplicación de transmisión 25 incluye una tercera interfaz 26 para las aplicaciones 23, 23’, 23’’ (es decir, a modo de ejemplo, la cuarta, quinta y sexta) disponibles en el segundo elemento seguro 22, o bien está unida con esta tercera interfaz 26. La segunda aplicación de transmisión 25 incluye además, o bien

está unida con una cuarta interfaz 27 para la comunicación con el primer terminal de telecomunicación 10 (en particular, el primer elemento seguro 12) y/o la instalación de servidor 101 y/o una segunda aplicación de dispositivo 29 (en lo sucesivo también denominada como “Device App”) disponible en el segundo terminal de telecomunicación 20, aunque fuera del segundo elemento seguro 22. La segunda aplicación de transmisión 25, la tercera interfaz 26 y la cuarta interfaz 27 forman en conjunto una segunda interfaz de transmisión 28, la cual, para la transmisión de la información de autorización, está disponible de conformidad con la invención preferiblemente en el segundo terminal de telecomunicación 20.

La función de la primera y segunda interfaces de transmisión 18, 28 es establecer una comunicación segura entre las aplicaciones 13, 13’, 13’’, 23, 23’, 23’’ (primera, segunda, tercera, cuarta, quinta, o bien sexta) que se encuentran en los elementos seguros 12, 22 y los datos 14, 14’, 14’’, 24, 24’, 24’’ (primeros, segundos, terceros, cuartos, quintos, o bien sextos) sensibles correspondientes. Esta comunicación se puede establecer por medio de distintos soportes de transmisión, como redes IP (redes de Protocolo de Internet), SMS (Short Message Service de una red de telefonía móvil), NFC, u otro tipo de sistema de transmisión. En este caso, un sistema de transmisión, o bien medio de transmisión, tal es preferiblemente transparente para la aplicación 13, 13’, 13’’, 23, 23’, 23’’ (primera, segunda, tercera, cuarta, quinta, o bien sexta) respectivas y los datos 14, 14’, 14’’, 24, 24’, 24’’ (primeros, segundos, terceros, cuartos, quintos, o bien sextos) sensibles correspondientes, con el fin de posibilitar a la aplicación la transmisión de los datos sensibles (esto es, “sus” datos sensibles). La primera, o bien segunda, aplicación de transmisión 15, 25 (o bien la primera, o bien segunda, interfaz de transmisión 18, 28) también se encarga, de conformidad con la invención, de otros aspectos de la transmisión de la información de autorización, los cuales están unidos con esta transmisión, como, por ejemplo, el reconocimiento del tipo de objeto (como, por ejemplo, el reconocimiento del modo de transmisión (transfer mode) de los datos sensibles, los escenarios de aplicación y las condiciones), la elección de los soportes, la aplicación y el cumplimiento de protocolos de seguridad, la eventual notificación de sistemas externos, el tratamiento de errores y similares.

Las interfaces de transmisión 18, 28 proporcionan respectivamente una interfaz (o bien una Interface) para las aplicaciones, o bien utilidades, en el primer, o bien segundo, elemento seguro 12, 22 (o bien “secure element”), las cuales están asignadas a los datos sensibles de las aplicaciones, por lo demás denominada como xfer App Interface, o bien como primera, o bien segunda, interfaz 16, 26. La comunicación entre la primera y segunda aplicación de transmisión 15, 25 y las primeras a sextas aplicaciones 13, 13’, 13’’, 23, 23’, 23’’ se realiza y contiene y transmite a través de esta primera, o bien tercera, interfaz 16, 26, además de otros datos y actividades, el registro y desregistro de las primeras a sextas aplicaciones 13, 13’, 13’’, 23, 23’, 23’’ y sus datos sensibles, el establecimiento de la comunicación segura con estas aplicaciones, el almacenamiento temporal de los datos seguros que se desea transmitir, la transferencia de los objetos que contienen los datos seguros, en el modo push (push mode), o bien en el modo pull (pull mode), así como el control y la verificación del estado de la transferencia. La aplicación de transmisión, o bien aplicación xfer, 15, 25 también proporciona, a través de la segunda y cuarta interfaz 17, 27, una interfaz para la infraestructura, la cual se encuentra fuera de los elementos seguros 12, 22 (lo cual también se denomina en lo sucesivo como Messaging Interfaces 17, 27). A través de estas segunda y cuarta aplicaciones 17, 27, se conduce la comunicación con las instalaciones externas, como, por ejemplo, todo tipo de aplicaciones sobre y en respectivamente otros elementos seguros o sobre (otros) dispositivos personales o sistemas externos como instalaciones de servidor 101 o similares.

La función de la aplicación del dispositivo 19, 29, o bien aplicación de dispositivo, únicamente opcional es proporcionar una interfaz gráfica de usuario (GUI, graphical user interface) para la funcionalidad de transmisión, o bien funcionalidad de transferencia, por ejemplo, para la visualización y/o modificación de la lista de las aplicaciones que soportan el servicio de transmisión y/o las autorizaciones que se pueden transmitir, las cuales están unidas con los objetos de datos sensibles, para la visualización y/o modificación de características, para la visualización y/o modificación de las condiciones de uso y transferencia, para la provisión de los canales de comunicación, los cuales no se soportan directamente por el respectivo elemento seguro 12, 22, así como para el tratamiento, la provisión y el mantenimiento de los ajustes del usuario. Otros sistemas opcionales dentro o fuera del elemento seguro respectivo pueden estar previstos para la notificación eventualmente necesaria del Service Provider, esto es, de la instalación de servidor 101, a través de la transferencia realizada, la protección de datos opcional de los datos sensibles y la provisión de datos sensibles en nombre del Service Provider, la observancia de directrices de seguridad.

Un ejemplo para la transmisión de la información de autorización según la presente invención incluye, a modo de ejemplo, los siguientes pasos:

Un usuario del primer terminal de telecomunicación 10 utiliza la primera aplicación de dispositivo, o bien App de dispositivo 19, la cual se comunica con la interfaz de transmisión 18 en el (o bien dentro del) primer elemento seguro 12 (o bien con la primera aplicación de transmisión 15 a través de la segunda interfaz 17, “messaging interface”), con el fin de listar todas las informaciones de autorización (o bien objetos de datos sensibles, o bien “objetos de datos sensibles”) que se pueden transmitir. La primera interfaz de transmisión 18, o bien la primera aplicación de transmisión 15, lee todos los objetos de datos sensibles que se pueden transmitir de cada primera, segunda, o bien tercera aplicación 13, 13’, 13’’ registrada (a través de la primera interfaz 16, o bien la “interfaz xfer App”). A continuación, el resultado se transmite por medio de la primera aplicación de dispositivo 19 App al usuario del primer

terminal de telecomunicación 10. Tan pronto como se haya seleccionado (por parte del usuario) un objeto para la transmisión, la aplicación de transmisión 15 recibe la notificación de la primera, segunda o tercera aplicación 13, 13', 13'' afectada con el "objeto de datos sensibles" correspondiente, esto es, los primeros, segundos o terceros datos 14, 14', 14'', de que la información de autorización está pendiente para la transmisión. A continuación, la información de autorización, o bien el objeto de la primera, segunda o tercera aplicación 13, 13', 13'' afectada se asegura de tal manera que, para la información de autorización, o bien la aplicación afectada, se aplican correspondientemente todas las reglas (por ejemplo, una marca se realizó como eliminada, cuando la información de autorización que se puede transmitir se trata de una información del tipo "cut & paste" (esto es, el usuario del segundo terminal de telecomunicación 20 se ha de autorizar para la utilización de un servicio o de una cosa en lugar del usuario del primer terminal de telecomunicación 10)). La información de autorización se envía a través de la primera interfaz 16 ("xfer App Interface") a la primera aplicación de transmisión 15. La primera aplicación de transmisión 15 aplica como consecuencia todas las normas a la información de autorización (o bien el objeto) (por ejemplo, estas se vinculan, las normas de seguridad afectadas se aplican) y envía la información de autorización, o bien el objeto, a través de la segunda interfaz 17 ("messaging interface") a la instalación externa, en particular, la instalación de servidor 101, o bien al segundo terminal de telecomunicación 20 y, allí, en particular, la segunda aplicación de transmisión 25. En el lado del receptor, si la segunda aplicación de transmisión 25 es receptora, el proceso transcurre a la inversa. El "Secure Data Object" terminado, o bien cuartos, quintos o sextos datos 24, 24', 24'' se unen con la aplicación respectiva (esto es, la cuarta, quinta o sexta aplicación 23, 23', 23''), la cual es entonces capaz de tratar y utilizar la información de autorización como "secure Data Objects". De conformidad con la invención está además preferiblemente previsto que después de la transmisión satisfactoria de la información de autorización se envíe una confirmación de la transmisión a la "xfer App" que envía, esto es, la primera aplicación de transmisión 15, la cual informa a la aplicación que envía (esto es, la primera, segunda o tercera aplicación 13, 13', 13'') sobre la transmisión de datos segura. Según una forma de realización preferida, la instalación de servidor 101 se informa asimismo sobre la transmisión realizada de la información de autorización.

Según la segunda variante del método de transmisión de conformidad con la invención se alcanza el mismo resultado cuando se utilizan la primera aplicación de transmisión 15 y un sistema externo, en particular, en forma de la instalación de servidor 101. Después de la selección de la autorización que se desea transmitir, la primera aplicación de transmisión 15 se comunica con la instalación de servidor 101, en donde, en este caso, la primera aplicación de transmisión 15 (xfer App) no transmite ningún objeto de datos sensibles a través de la segunda interfaz 17 ("Messaging Interface"), sino sólo una información sobre la modificación de la asociación de la autorización con el segundo terminal de telecomunicación 20. La instalación de servidor 101, o bien el Service Provider Backend System, pone en acción la instalación, o bien transmisión de los (terceros, cuartos o quintos datos) en el elemento seguro del segundo terminal de telecomunicación 20, por ejemplo, por medio de una instalación OTA (Over The Air Installation). A continuación, la instalación de servidor 101 informa al primer terminal de telecomunicación 10 (o bien la primera aplicación de transmisión 15, o bien la primera aplicación de dispositivo 19) sobre el estado de la transmisión, para que la aplicación que envía (primera, segunda o tercera aplicación 13, 13', 13'') se informe sobre la transmisión segura.

REIVINDICACIONES

1. Método para la transmisión a través de una red de telecomunicaciones (100)

- de una información de autorización almacenada en un área de almacenamiento de un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication) o
- de una autorización asociada con un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC

de un primer terminal de telecomunicación (10) a un segundo terminal de comunicación (20),
en donde, en un primer momento, la información de autorización está almacenada en una primera área de almacenamiento (11) del primer terminal de telecomunicación (10) o la autorización está asociada con el primer terminal de telecomunicación (10) y en donde, en un segundo momento posterior con respecto al primer momento, la información de autorización está almacenada en una segunda área de almacenamiento (21) del segundo terminal de telecomunicación (20) o la autorización está asociada con el segundo terminal de telecomunicación (20),
en donde el primer terminal de telecomunicación (10), además de la interfaz NFC, presenta una primera interfaz inalámbrica y el segundo terminal de telecomunicación (20), además de la interfaz NFC, presenta una segunda interfaz inalámbrica, en donde, para la transmisión de la información de autorización del primer terminal de telecomunicación (10) al segundo terminal de telecomunicación (20), se utiliza la primera y segunda interfaz inalámbrica o, para la transmisión de la autorización, se utiliza al menos la primera interfaz inalámbrica, en donde, durante la transmisión de la información de autorización o de la autorización, el primer y segundo terminal de telecomunicación (10, 20) presentan una distancia el uno del otro que supera el alcance de la interfaz NFC, en donde la información de autorización en el primer terminal de telecomunicación (10) está almacenada en un primer elemento seguro (12) (SE, secure element), en el que también se encuentra la primera área de almacenamiento (11) y en donde la información de autorización en el segundo terminal de telecomunicación (20) está almacenada en un segundo elemento seguro (22), en el que también se encuentra la segunda área de almacenamiento (21), en donde el primer elemento seguro (12) para la transmisión de la información de autorización presenta una primera interfaz de transmisión (18) y el segundo elemento seguro (22) para la transmisión de la información de autorización presenta una segunda interfaz de transmisión (28), en donde la información de autorización se transmite de forma transparente a través de la primera y segunda interfaz de transmisión (18, 28) utilizando un canal de transmisión, en donde se produce una transmisión no transmitida a través de una instalación de servidor **caracterizado por que** la transmisión de la información de autorización o de la asociación de la autorización del primer terminal de telecomunicación (10) al segundo terminal de telecomunicación (20) autoriza al usuario del segundo terminal de telecomunicación (20)

- durante la duración de un intervalo de tiempo predeterminado o
- dentro de un área geográfica predeterminada o
- para una combinación de una condición temporal y una geográfica, para la utilización de un servicio o de una cosa,

en donde esta utilización limitante se establece por un usuario del primer terminal de telecomunicación (10).

2. Método según la reivindicación 1 **caracterizado por que** el primer y segundo terminal de telecomunicación (10), durante la transmisión de la información de autorización o de la autorización, presentan una distancia el uno del otro que supera el alcance de una red inalámbrica local (WLAN, Wireless Local Area Network).

3. Método según una de las reivindicaciones anteriores **caracterizado por que** el primer y segundo elemento seguro (12, 22) es un elemento SE (Secure Element) según el estándar GlobalPlatform o una UICC (Universal Integrated Circuit Card) o una tarjeta microSD (Secure Digital card) o una tarjeta ICC (integrated circuit card) o un circuito integrado.

4. Método según una de las reivindicaciones anteriores **caracterizado por que** la transmisión de la información de autorización o de la asociación de la autorización del primer terminal de telecomunicación (10) al segundo terminal de telecomunicación (20) autoriza al usuario del segundo terminal de telecomunicación (20) o bien:

- en lugar del usuario del primer terminal de telecomunicación (10) o
- además del usuario del primer terminal de telecomunicación (10), para la utilización de un servicio o de una cosa.

5. Método según una de las reivindicaciones anteriores **caracterizado por que** la información de autorización se transmite de forma transparente por medio de la primera y segunda interfaz de transmisión (18, 28) utilizando un canal de transmisión, de forma protegida, en particular, cifrada.

6. Método según una de las reivindicaciones anteriores **caracterizado por que** como información de autorización se transmiten

- tanto informaciones en relación con una aplicación utilizada o que se desea utilizar dentro del primer y/o del segundo elemento seguro (12, 22) e implicada en la transmisión
- como también informaciones confidenciales y protegidas conectadas con la aplicación implicada en la transmisión (credential informations).

7. Terminal de telecomunicación (10) con una interfaz NFC (interfaz Near Field Communication) y una primera interfaz inalámbrica para la transmisión

- de una información de autorización almacenada en un área de almacenamiento del terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication) o
- de una autorización asociada con el terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC

del terminal de telecomunicación (10) a un segundo terminal de telecomunicación (20),
en donde el terminal de telecomunicación (10) está configurado de tal manera para almacenar la información de autorización en una primera área de almacenamiento (11) del terminal de telecomunicación (10), en donde el terminal de telecomunicación (10) está configurado para la transmisión de la información de autorización del terminal de telecomunicación (10) al segundo terminal de telecomunicación (20) utilizando la primera interfaz inalámbrica, en donde el terminal de telecomunicación (10) y el segundo terminal de telecomunicación (20), durante la transmisión de la información de autorización, presentan una distancia el uno del otro que supera el alcance de la interfaz NFC, en donde la información de autorización en el primer terminal de telecomunicación (10) está almacenada en un primer elemento seguro (12) (SE, secure element), en el que también se encuentra la primera área de almacenamiento (11), en donde el primer elemento seguro (12) para la transmisión de la información de autorización presenta una primera interfaz de transmisión (18), en donde la información de autorización se transmite de forma transparente a través de la primera interfaz de transmisión (18) utilizando un canal de transmisión, en donde se produce una transmisión no transmitida a través de una instalación de servidor **caracterizado por que** la transmisión de la información de autorización o de la asociación de la autorización del primer terminal de telecomunicación (10) al segundo terminal de telecomunicación (20) autoriza al usuario del segundo terminal de telecomunicación (20)

- durante la duración de un intervalo de tiempo predeterminado o
- dentro de un área geográfica predeterminada o
- para una combinación de una condición temporal y una geográfica, para la utilización de un servicio o de una cosa,

en donde el terminal de telecomunicación (10) está configurado de tal manera que esta utilización limitante se establece por un usuario del terminal de telecomunicación (10).

8. Terminal de telecomunicación (10) según la reivindicación 7 **caracterizado por que** el primer elemento seguro (12) es un elemento SE (Secure Element) según el estándar GlobalPlatform o una UICC (Universal Integrated Circuit Card) o una tarjeta microSD (Secure Digital card) o una tarjeta ICC (integrated circuit card) o un circuito integrado.

9. Terminal de telecomunicación (10) según la reivindicación 7 u 8 **caracterizado por que** la información de autorización se transmite de forma transparente a través de la primera interfaz de transmisión (18) utilizando un canal de transmisión de forma protegida, en particular, cifrada, en donde el terminal de telecomunicación (10) está configurado, en particular, de tal manera que como información de autorización se transmiten

- tanto informaciones en relación con una aplicación utilizada o que se desea utilizar dentro del primer y/o del segundo elemento seguro (12, 22) e implicada en la transmisión
- como también informaciones confidenciales y protegidas conectadas con la aplicación implicada en la transmisión (credentials informations).

10. Sistema que comprende un primer terminal de telecomunicación (10) y un segundo terminal de telecomunicación (20) para la transmisión, a través de una red de telecomunicaciones (100),

- de una información de autorización almacenada en un área de almacenamiento de un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC (interfaz Near Field Communication) o
- de una autorización asociada con un terminal de telecomunicación y que se puede utilizar por medio de una interfaz NFC

del primer terminal de telecomunicación (10) al segundo terminal de telecomunicación (20),
en donde el sistema está configurado de tal manera para almacenar la información de autorización en una primera área de almacenamiento (11) del primer terminal de telecomunicación (10) o para asociar la autorización con el

primer terminal de telecomunicación (10) y/o en donde el sistema está configurado de tal manera para almacenar la información de autorización en una segunda área de almacenamiento (21) del segundo terminal de telecomunicación (20) o para asociar la autorización con el segundo terminal de telecomunicación (20),
en donde el primer terminal de telecomunicación (10), además de la interfaz NFC, presenta una primera interfaz inalámbrica y el segundo terminal de telecomunicación (20), además de la interfaz NFC, presenta una segunda interfaz inalámbrica, en donde el sistema está configurado para la transmisión de la información de autorización del primer terminal de telecomunicación (10) al segundo terminal de telecomunicación (20) utilizando la primera y segunda interfaz inalámbrica o está configurado para la transmisión de la autorización utilizando al menos la primera interfaz inalámbrica, en donde el sistema está configurado de tal manera que el primer y segundo terminal de telecomunicación (10, 20), durante la transmisión de la información de autorización o la autorización, presentan una distancia el uno del otro que supera el alcance de la interfaz NFC, en donde la información de autorización en el primer terminal de telecomunicación (10) está almacenada en un primer elemento seguro (12) (SE, secure element), en el que también se encuentra la primera área de almacenamiento (11) y en donde la información de autorización en el segundo terminal de telecomunicación (20) está almacenada en un segundo elemento seguro (22), en el que también se encuentra la segunda área de almacenamiento (21), en donde el primer elemento seguro (12) para la transmisión de la información de autorización presenta una primera interfaz de transmisión (18) y el segundo elemento seguro (22) para la transmisión de la información de autorización presenta una segunda interfaz de transmisión (28), en donde la información de autorización se transmite de forma transparente a través de la primera y segunda interfaz de transmisión (18, 28) utilizando un canal de transmisión, en donde se produce una transmisión no transmitida a través de una instalación de servidor **caracterizado por que** la transmisión de la información de autorización o de la asociación de la autorización del primer terminal de telecomunicación (10) al segundo terminal de telecomunicación (20) autoriza al usuario del segundo terminal de telecomunicación (20)

- durante la duración de un intervalo de tiempo predeterminado o
- dentro de un área geográfica predeterminada o
- para una combinación de una condición temporal y una geográfica, para la utilización de un servicio o de una cosa,

en donde el primer terminal de telecomunicación (10) está configurado de tal manera que esta utilización limitante se establece por un usuario del primer terminal de telecomunicación (10).

11. Sistema según la reivindicación 10 **caracterizado por que** la información de autorización en el primer terminal de telecomunicación (10) está almacenada en un primer elemento seguro (12) (SE, secure element), en el que también se encuentra la primera área de almacenamiento (11) y que la información de autorización en el segundo terminal de telecomunicación (20) está almacenada en un segundo elemento seguro (22), en el que también se encuentra la segunda área de almacenamiento (21), en donde el primer y segundo elemento seguro (12, 22) es, en particular, un elemento SE (Secure Element) según el estándar GlobalPlatform o una UICC (Universal Integrated Circuit Card) o una tarjeta microSD (Secure Digital card) o una tarjeta ICC (integrated circuit card).

12. Programa informático con medios de codificación de programa, con cuya ayuda se pueden realizar los pasos de un método según una de las reivindicaciones 1 a 6, cuando el programa informático se ejecuta en el primer terminal de telecomunicación (10).

13. Producto de programa informático con un medio legible por ordenador y un programa informático almacenado en el medio legible por ordenador con medios de codificación de programa, los cuales son apropiados para que se puedan realizar los pasos de un método según una de las reivindicaciones 1 a 6, cuando el programa informático se ejecuta en el primer terminal de telecomunicación (10).

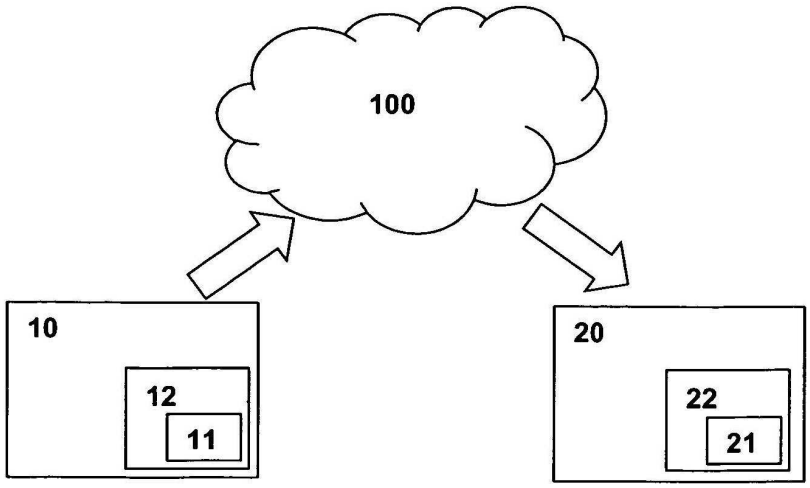

Fig. 1

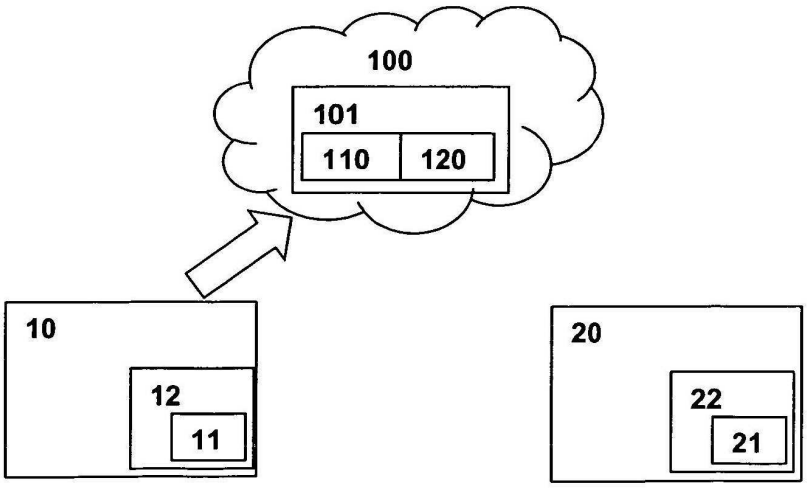

Fig. 2

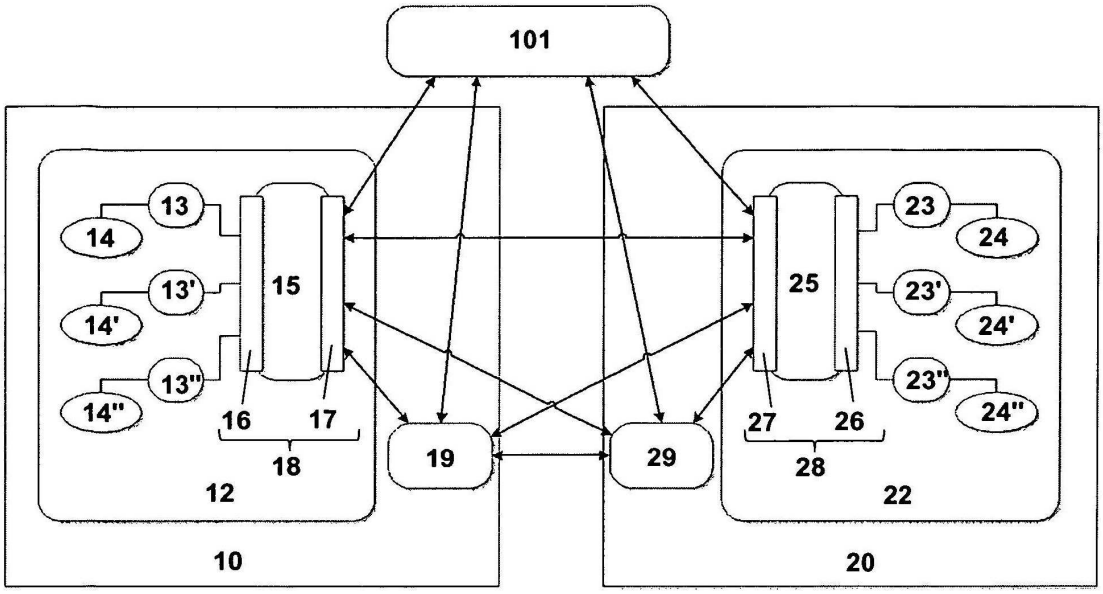
101
13
14
13'
14'
13"
14"
15
16
17
18
12
10
19
29
25
23
24
23'
24'
23"
24"
27
26
28
22
20

Fig. 3