(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 634 645**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04M 1/725 (2006.01)
H04W 4/00 (2009.01)
H04W 8/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.07.2014 E 14002597 (4)**

(97) Fecha y número de publicación de la concesión europea: **28.06.2017 EP 2833598**

(54) Título: **Transmisión de un identificador de acceso**

(30) Prioridad:

31.07.2013 DE 102013012791

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.09.2017

(73) Titular/es:

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

(72) Inventor/es:

AUER, MARTIN y
LEIBNER, TORSTEN

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Transmisión de un identificador de acceso

La presente invención se refiere a un procedimiento para transmitir un identificador de acceso a un aparato de telecomunicaciones por medio de una unidad de servicio.

Estado de la Técnica

Los elementos de seguridad portátiles, en particular tarjetas de valor o de prepago, tarjetas de crédito, tarjetas de débito, tarjeta de cheques, etc., son conocidos en el estado de la técnica. En estos elementos es necesario introducir un identificador de acceso, por ejemplo un número secreto o PIN, para llevar a cabo transacciones como por ejemplo la retirada de dinero en efectivo en los cajeros automáticos con estas tarjetas. Este identificador de acceso se comunica al usuario del elemento de seguridad portátil normalmente enviándole el mismo por correo y/o por mensaje de texto (SMS). El envío del identificador de acceso por correo implica que la carta puede perderse en el trayecto de envío, que acarrea cierto tiempo hasta que puede entregarse al destinatario y que el envío está sujeto a tasas relativamente elevadas. El envío del PIN al usuario por mensaje de texto (SMS) presenta el inconveniente de que los mensajes no se envían cifrados y por tanto existe el riesgo de que un tercero intercepte el mensaje SMS. Además, el usuario puede almacenar el SMS en su aparato de telefonía móvil. Esto puede resultar en que un tercero que encuentre el aparato de telefonía móvil pueda utilizar un PIN almacenado maliciosamente en combinación con el elemento de seguridad portátil. Asimismo, el remitente de un mensaje no recibe ninguna confirmación de si el destinatario ha recibido el mensaje realmente. Por tanto el remitente desconoce si el mensaje realmente ha llegado al destinatario.

Además, a partir del documento WO 2007/036341 A1 se conoce un procedimiento para desbloquear una tarjeta de telefonía móvil bloqueada por medio de un identificador de acceso del usuario. En este procedimiento se establece automáticamente un acceso del usuario a la tarjeta de telefonía móvil a solicitud de una unidad de servicio con objeto de facilitar al usuario iniciar un modo de desbloqueo y desbloquear una tarjeta de telefonía móvil bloqueada tras haber introducido incorrectamente repetidas veces el PIN de la tarjeta de telefonía móvil.

Adicionalmente, a partir del documento WO 2007/036340 A1 se conoce un procedimiento para almacenar un identificador de acceso de una tarjeta de telefonía móvil en una unidad de servicio (Provider) que permite desbloquear una tarjeta de telefonía móvil tras haber introducido incorrectamente repetidas veces el PIN, consultando el identificador de acceso almacenado.

Estas dos soluciones mencionadas anteriormente se basan en el principio de hacer posible que una tarjeta de telefonía móvil (tarjeta SIM) pueda liberarse tras haber introducido incorrectamente repetidas veces el PIN (Personal Indentification Number).

A partir del documento US 2013/0152185 A1 se desprende un procedimiento con el cual hace posible transmitir sin contacto datos de autentificación desde un registro de seguridad a una unidad móvil, en particular un teléfono móvil. Los datos de autentificación pueden almacenarte en el teléfono móvil y utilizarse para realizar transacciones.

Descripción de la Invención

La invención tiene como objetivo proporcionar un procedimiento para transmitir un identificador de acceso a un aparato de telecomunicaciones que resuelva los problemas conocidos del estado de la técnica y que también sea adecuado para permitir una transmisión segura y eficiente de un identificador de acceso de un elemento de seguridad portátil.

Este objetivo se consigue mediante un procedimiento para transmitir un identificador de acceso a un aparato de telecomunicaciones con las características de la reivindicación independiente 1 y mediante la utilización de un aparato de telecomunicaciones u bien una unidad de servicio en un procedimiento de acuerdo con la invención. En las reivindicaciones dependientes se recogen realizaciones preferidas del procedimiento de acuerdo con la invención.

La invención se basa en la idea de proporcionar un elemento de seguridad portátil con una interfaz sin contacto y de acoplar el elemento de seguridad portátil con un aparato de telecomunicaciones por medio de esta interfaz para así transmitir un identificador de acceso del elemento de seguridad portátil al aparato de telecomunicaciones.

Por consiguiente, el procedimiento para transmitir un identificador de acceso a un aparato de telecomunicaciones de acuerdo con la invención comprende el establecimiento de una primera conexión de comunicación entre un aparato de telecomunicaciones y un elemento de seguridad portátil por medio de una interfaz inalámbrica, la transmisión de datos específicos de elemento de seguridad al aparato de telecomunicaciones por medio de la primera conexión de comunicación, la transmisión de datos específicos de elemento de seguridad y datos específicos de aparato de telecomunicaciones del aparato de telecomunicaciones desde el aparato de telecomunicaciones a una unidad de

servicio por medio de una segunda conexión de comunicación, y la transmisión de un identificador de acceso del elemento de seguridad portátil desde la unidad de servicio al aparato de telecomunicaciones por medio de la segunda conexión de comunicaciones, en caso de que la combinación de los datos específicos de elemento de seguridad y los datos específicos de aparato de telecomunicaciones sean conocidos para la unidad de servicio.

De acuerdo con la invención, el término “identificador de acceso” incluye cualquier tipo de dato asociado a un elemento de seguridad portátil y que por ejemplo se requiera para autentificar una transacción, por ejemplo la retirada de dinero de un cajero automático, por medio del elemento de seguridad portátil.

Un “elemento de seguridad portátil” en el contexto de la invención es cualquier tipo de soporte de datos portátil o tarjeta de valor con la que es posible proporcionar un servicio. Ejemplos de elementos de seguridad portátiles son tarjetas de crédito, tarjetas de giro (“girocard”), tarjetas de débito (“ec-card”), tarjetas de salud, tarjetas de chip, módulos de seguridad así como cualquier tipo de portador de datos portátil que pueda ser utilizado para acceder a determinados servicios como por ejemplo para servicios de uso temporal de vehículos (car sharing).

Un “aparato de telecomunicaciones” puede ser un aparato de telefonía móvil (un móvil), una tableta PC o similar.

Con el procedimiento de acuerdo con la invención, es posible de forma particularmente ventajosa transmitir un identificador de acceso de un elemento de seguridad portátil al aparato de telecomunicaciones tras el establecimiento de una conexión de comunicaciones, por ejemplo por medio de una comunicación de campo cercano (NFC). De este modo se elimina la necesidad de un envío del identificador de acceso por correo, costoso en tiempo y dinero. Además, el procedimiento de acuerdo con la invención es muy seguro porque se efectúa con al menos una doble protección, estableciéndose en un primer paso una primera conexión de comunicación entre aparato de telecomunicaciones y elemento de seguridad portátil y a continuación una segunda conexión de comunicación entre aparato de telecomunicaciones y unidad de servicio. De este modo durante la segunda transmisión del identificador de acceso puede asegurarse un alto nivel de seguridad porque la transmisión del identificador de acceso - según una forma de realización preferida - puede efectuarse de forma encriptada. Una ventaja adicional es que la transmisión del identificador de acceso se efectúa en tiempo real y que por tanto la unidad de servicio es capaz de monitorizar si un usuario ha recibido correctamente el identificador de acceso. A diferencia de cuando el identificador de acceso se envía por SMS, este procedimiento presenta ventajas adicionales porque cuando se envía por SMS la unidad de servicio no recibe ningún aviso de confirmación automático sobre si el usuario ha recibido realmente el identificador de acceso enviado por SMS. Por el contrario, en el procedimiento de acuerdo con la invención puede realizarse un aviso de confirmación sobre si la transmisión del identificador de acceso al aparato de telecomunicaciones fue exitosa.

Los datos específicos de seguridad a enviar pueden incluir por ejemplo un número de identificación de tarjeta, el nombre del propietario de tarjeta, etc. Los datos específicos de aparato de telecomunicaciones pueden incluir datos que permitan una identificación clara del aparato de telecomunicaciones y/o de la tarjeta SIM (insertada). Ejemplos de ello son el MSISDN (Mobile Subscriber Integrated Services Digital Network Number), el IMEI (International Mobile Station Equipment Identity), y/o el IMSI (International Mobile Subscriber Identity).

La segunda conexión de comunicación se efectúa normalmente por medio de la red de telefonía móvil (por ejemplo GSM y/o UMTS). Alternativamente medios de transmisión tales como W-LAN son también posibles.

Según una forma de realización, la transmisión de los datos específicos de elemento de seguridad al aparato de telecomunicaciones puede efectuarse de forma encriptada. Para ello son apropiados todos los procedimientos de encriptado simétricos y asimétricos conocidos. Durante la transmisión, la interfaz inalámbrica puede estar configurada como interfaz de comunicación de campo cercano (NFC). Esto es ventajoso porque la interfaz NFC se considera muy segura debido a su cobertura de transmisión relativamente pequeña de aproximadamente 10 cm; de este modo, no es posible que atacantes o personas que puedan interceptar la transmisión accedan a alguna de las unidades de transmisión (aparato de telecomunicaciones y/o elemento de seguridad portátil) lo suficientemente cerca como para interceptar los datos transmitidos por medio de la primera conexión de comunicación.

En el contexto de la invención, una unidad de servicio puede ser un proveedor de telefonía móvil (Provider) y/o un fabricante o administrador de elementos de seguridad portátiles. En el caso de que se trate de un fabricante o un administrador de elementos de seguridad portátiles, se debe asegurar que los datos se transmiten directamente por medio de la segunda conexión de comunicación al fabricante o administrador de elementos de seguridad portátiles, o que se transmiten por medio de un proveedor de telefonía móvil al fabricante o administrador de elementos de seguridad portátiles.

De acuerdo con una forma de realización especialmente preferida, la transmisión del identificador de acceso del elemento de seguridad portátil al aparato de telecomunicaciones se efectúa de forma encriptada. De este modo puede asegurarse siempre que para un tercero no sea posible “interceptar” la transmisión de datos y por tanto obtener el identificador de acceso.

De acuerdo con una forma de realización preferida adicional de la invención, el identificador de acceso se almacena en un entorno seguro del aparato de telecomunicaciones. Un entorno seguro puede implementarse por ejemplo mediante un elemento de seguridad configurado en forma de software o hardware. Un elemento de seguridad configurado en forma de hardware puede ser por ejemplo una tarjeta SIM reemplazable o integrada fijamente, un testigo USB ("USB-token") o similar. Un elemento de seguridad configurado en forma de software puede ser por ejemplo un área de almacenamiento modificada mediante técnicas de programación adecuadas, en la cual el identificador de acceso se almacena de forma especialmente segura por medio de un encriptado adicional o similar.

Con objeto de aumentar en mayor medida la seguridad puede ser necesario restaurar la primera conexión de comunicación entre el aparato de telecomunicaciones y el elemento de seguridad portátil para consultar el identificador de acceso almacenado. Sólo entonces el identificador de acceso es representado, por ejemplo en una unidad de visualización del aparato de telecomunicaciones. De este modo, la seguridad durante la consulta del identificador de acceso almacenado en el entorno seguro del aparato de telecomunicaciones aumenta sustancialmente.

De acuerdo con una forma de realización preferida adicional, está previsto que para transmitir los datos específicos de seguridad y/o los datos específicos de aparato de telecomunicaciones (por medio de la segunda conexión de comunicación) sea necesario una autentificación entre el aparato de telecomunicaciones y la unidad de servicio. Para la autentificación puede utilizarse por ejemplo una clave determinada de antemano entre el aparato de telecomunicaciones y la unidad de servicio. De este modo la seguridad de la transmisión de datos aumenta sustancialmente.

El procedimiento de acuerdo con la invención es apropiado de forma especialmente ventajosa para ser utilizado en un aparato de telecomunicaciones con objeto de obtener el identificador de acceso de un elemento de seguridad portátil de la unidad de servicio después de la transmisión de los datos específicos de elemento de seguridad y los datos específicos de aparato de telecomunicaciones.

Adicionalmente, el procedimiento de acuerdo con la invención es apropiado especialmente para ser utilizado en una unidad de servicio con objeto de enviar el identificador de acceso (del elemento de seguridad portátil) al aparato de telecomunicaciones después de obtener los datos específicos de elemento de seguridad y los datos específicos de aparato de telecomunicaciones.

Breve Descripción de los Dibujos

A continuación la invención se explica en detalle con ayuda de ejemplos de realización mostrados en los dibujos a modo de ejemplo. En los dibujos:

Figura 1 muestra los componentes empleados en un procedimiento de acuerdo con la invención así como el flujo de datos en el procedimiento de acuerdo con la invención, y

Figura 2 muestra un diagrama de flujo con los pasos sustanciales del procedimiento de acuerdo con la invención.

Descripción de formas de realización preferidas de la invención

En la figura 1 se muestran esquemáticamente los componentes empleados en un procedimiento de acuerdo con la invención así como el flujo de datos que tiene lugar entre los mismos, y en la figura 2 se representa el desarrollo de un procedimiento de acuerdo con la invención en la forma de un diagrama de flujo.

La figura 1 muestra un elemento de seguridad portátil -12-, un aparato de telecomunicaciones -10- y una unidad de servicio -16-. El elemento de seguridad portátil -12- es por ejemplo una tarjeta de crédito, tarjeta de débito ("ec-card), tarjeta de salud, tarjeta de chip, módulo de seguridad o similar. En el ejemplo de realización el elemento de seguridad portátil -12- es lo que se denomina una tarjeta de interfaz dual (dual interface), que tiene al menos dos interfaces. La primera interfaz es una interfaz de contacto -13-. Por medio de ésta se efectúa un contacto galvánico con una unidad externa, por ejemplo un terminal de lectura de tarjeta (no mostrado), mediante contacto directo. Alternativamente, la primera interfaz puede ser otra interfaz cualquiera. La segunda interfaz -14- es una interfaz sin contacto. Ésta está configurada como interfaz sin contacto NFC (interfaz de comunicación de campo cercano) en el ejemplo de realización mostrado. Con la segunda interfaz -14- puede establecerse una primera conexión de comunicación -20- entre un aparato de telecomunicaciones -10- y el elemento de seguridad portátil -12-. En otras palabras, la primera conexión de comunicación -20- es una conexión sin contacto entre la segunda interfaz -14- y el aparato de telecomunicaciones -10- por medio de una interfaz inalámbrica.

De acuerdo con el procedimiento, en un primer paso -S1- (ver figura 2) primero se estable una primera conexión de comunicación -20- entre el elemento de seguridad portátil -12- y el aparato de telecomunicaciones -10- por NFC. Esto se efectúa mientras el elemento de seguridad portátil -12-, en particular la interfaz NFC -14- (NFC-API), se dispone cerca de una interfaz NFC (no mostrada) del aparato de telecomunicaciones -10-. A continuación, los datos específicos de elemento de seguridad, denominados credenciales (Credentials), del elemento de seguridad portátil

-12- se transmiten al aparato de telecomunicaciones -10- por medio de la primera conexión de comunicación -20- por NFC (paso -S2-). En estos datos específicos de elemento de seguridad pueden incluirse por ejemplo un número que identifique claramente al elemento de seguridad portátil -12-, el nombre del propietario del elemento de seguridad portátil, la fecha de validez del elemento de seguridad portátil, etc. La transmisión de los datos puede efectuarse de forma encriptada, simétrica o asimétricamente.

En un siguiente paso -S3- se establece una segunda conexión de comunicación -22- entre el aparato de telecomunicaciones -10- y la unidad de servicio -16-. Por medio de esta segunda conexión de comunicación -22- se transmiten a una unidad de servicio -16- tanto los datos específicos de elemento de seguridad que fueron transmitidos al aparato de telecomunicaciones -10- por medio de la primera conexión de comunicación -20- como los datos específicos de aparato de telecomunicaciones, tales como por ejemplo el MSISDN, el IMEI y/o el IMSI.

La unidad de servicio -16- puede ser por ejemplo un proveedor de telefonía móvil y/o un fabricante o administrador de elementos de seguridad portátiles. La transmisión de los datos por medio de la segunda conexión de comunicación -22- se efectúa preferiblemente por medio de una conexión de telefonía móvil, en particular por medio de GSM o UMTS. Alternativamente, la segunda conexión de comunicación -22- puede ser también una conexión de internet sin cable (W-LAN).

Tanto el establecimiento de la primera conexión de comunicación -20- como el establecimiento de la segunda conexión de comunicación -22- puede iniciarse mediante llamada a una aplicación o programa de software en el aparato de telecomunicaciones -10- que a su vez llama a las dos conexiones de comunicación -20-, -22- una después de la otra y retransmite los datos necesarios. En vez de llamar a una aplicación para iniciar la transmisión de datos, el establecimiento o inicio de las conexiones de comunicación -20-, -22- puede ser integrada también en una aplicación bancaria preexistente de una institución financiera o similar.

La unidad de servicio -16- comprueba si tiene disponible un identificador de acceso asociado al elemento de seguridad -12- para la combinación de los datos específicos de elemento de seguridad del elemento de seguridad portátil -12- y los datos específicos de aparato de telecomunicaciones del aparato de telecomunicaciones -10-. Con objeto de proporcionar una conexión o enlace entre elemento de seguridad portátil -12- y aparato de comunicaciones -10-, un usuario puede especificar un MSISDN de un aparato de telecomunicaciones -10- a emplear en el procedimiento de acuerdo con la invención por ejemplo en la solicitud del elemento de seguridad portátil -12-. Tan pronto como los datos específicos de elemento de seguridad y el MSISDN asociado del aparato de telecomunicaciones -10- se han transmitido, o han llegado, a la unidad de servicio -16- por medio de la segunda conexión de comunicación -22-, la unidad de servicio -16- puede asignar a los datos un respectivo identificador de acceso y transmitir este identificador de acceso desde la unidad de servicio -16- al aparato de telecomunicaciones -10- por medio de la segunda conexión de comunicación -22-.

La transmisión de datos por medio de la segunda conexión de comunicación -22- puede efectuarse igualmente de forma encriptada y en un entorno seguro. El entorno seguro puede realizarse por ejemplo en un elemento de seguridad autónomo especial y ser manejado por un Trusted Security Manager (TSM). Adicionalmente, es posible almacenar los datos transmitidos al aparato de telecomunicaciones -10- en una zona segura (SE; Secure Element) del aparato de telecomunicaciones -10-. Esto tiene la ventaja de que el usuario puede también visualizar el identificador de acceso del elemento de seguridad portátil -12- después de haberse transmitido satisfactoriamente el identificador de acceso al aparato de telecomunicaciones -10- si no hay conexión de datos a la unidad de servicio -16-, es decir con una segunda conexión de comunicación -22- desconectada. El elemento seguro o la zona segura pueden tener diferentes factores de forma: un chip integrado fijamente en el aparato de telecomunicaciones -10-, una tarjeta SIM adecuadamente adaptada o una tarjeta micro-SD insertable en el aparato de telecomunicaciones -10- especialmente para este propósito.

El identificador de acceso puede visualizarse por medio de la unidad de visualización -30- del aparato de telecomunicaciones -10-.

Con objeto de aumentar adicionalmente la seguridad en el caso de que se actualice la visualización del identificador de acceso del elemento de seguridad -12-, almacenada en el aparato de telecomunicaciones -10-, por medio de la unidad de visualización -30-, puede preverse que la primera conexión de comunicación -20- pueda establecerse sólo cuando la interfaz de comunicación de campo cercano -14- del elemento de seguridad portátil -12- se sitúe cerca del aparato de telecomunicaciones -10-. El identificador de acceso se visualiza en la unidad de visualización -30- del aparato de telecomunicaciones -10- sólo cuando existe la primera conexión de comunicación -20-.

En resumen, los pasos básicos del procedimiento de acuerdo con la invención pueden representarse como sigue (ver figura 2):

Inicialmente, en un primer paso -S1-, se establece una conexión de comunicación -20- entre un aparato de telecomunicaciones -10- y un elemento de seguridad portátil -12-. Esta primera conexión de comunicación -20- puede establecerse por ejemplo mediante una comunicación de campo cercano (NFC).

A continuación, en un siguiente paso -S2-, datos específicos de elemento de seguridad, como por ejemplo el número de identificación del elemento de seguridad -12-, se transmiten al aparato de telecomunicaciones -10- por medio de la primera conexión de comunicación -20-. La transmisión puede efectuarse de forma encriptada.

Después, en un tercer paso -S3-, los datos específicos de elemento de seguridad y los datos específicos de aparato de telecomunicaciones, como por ejemplo el MSISDN, el IMEI y/o el IMSI, se transmites a una unidad de servicio -16- por medio de una segunda conexión de comunicación -22-.

La unidad de servicio -16- comprueba si tiene almacenado un identificador de acceso para la combinación de los datos específicos de elemento de seguridad y los datos específicos de aparato de telecomunicaciones. Si éste es el caso entonces, en un siguiente paso -S4-, envía el identificador de acceso al aparato de telecomunicaciones -10-. Ahí, el identificador de acceso puede almacenarse en un entorno seguro y, incluso aunque no exista la segunda conexión de comunicación -22-, ser representado en la unidad de visualización -30- del aparato de telecomunicaciones -10-. Un entorno seguro puede estar configurado en forma de hardware o software. Un elemento de seguridad configurado en forma de hardware puede ser por ejemplo una tarjeta SIM reemplazable o integrada fijamente, un testigo USB o similar. Un elemento de seguridad configurado en forma de software puede ser por ejemplo un área de almacenamiento (SE; Secure Element) modificada mediante técnicas de programación adecuadas, en la cual el identificador de acceso se almacena de forma especialmente segura por medio de un encriptado adicional o similar.

Lista de signos de referencia

-10-	Aparato de telecomunicaciones
-12-	Elemento de seguridad
-13-	Primera interfaz
-14-	Segunda interfaz
-16-	Unidad de servicio
-20-	Primera conexión de comunicación
-22-	Segunda conexión de comunicación
-30-	Unidad de visualización
-S1- - -S4-	Pasos de procedimiento

REIVINDICACIONES

1. Procedimiento de transmisión de un identificador de acceso a un aparato de telecomunicaciones, que comprende los siguientes pasos:
- Establecer una primera conexión de comunicación (20) entre un aparato de telecomunicaciones (10) y un elemento de seguridad portátil (12) por medio de una interfaz inalámbrica,
- Transmitir datos específicos de elemento de seguridad desde el elemento de seguridad (12) al aparato de telecomunicaciones (10) por medio de la primera conexión de comunicación (20),
- Transmitir datos específicos de elemento de seguridad del elemento de seguridad (12) y datos específicos de aparato de telecomunicaciones del aparato de telecomunicaciones (10) desde el aparato de telecomunicaciones (10) a una unidad de servicio (16) por medio de una segunda conexión de comunicación (22), y
- Transmitir un identificador de acceso del elemento de seguridad portátil (12) desde la unidad de servicio (16) al aparato de telecomunicaciones (10), siendo el identificador de acceso representado en una unidad de visualización (30) del aparato de telecomunicaciones (10).

2. Procedimiento, según la reivindicación 1, **caracterizado por que** la interfaz inalámbrica en la primera conexión de comunicación (20) es una conexión de comunicación de campo cercano.

3. Procedimiento, según la reivindicación 1 o 2, **caracterizado por que** la transmisión de los datos específicos de elemento de seguridad al aparato de telecomunicaciones (10) se efectúa de forma encriptada.

4. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado por que** la unidad de servicio (16) incluye un proveedor de telefonía móvil y/o un fabricante o administrador de elementos de seguridad portátiles.

5. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado por que** los datos específicos de aparato de telecomunicaciones incluyen el MSISDN, el IMEI y/o el IMSI del aparato de telecomunicaciones (10), en particular de una tarjeta SIM dispuesta en el mismo.

6. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado por que** la transmisión del identificador de acceso del elemento de seguridad portátil (12) al aparato de telecomunicaciones (10) se efectúa de forma encriptada.

7. Procedimiento ,según una de las reivindicaciones anteriores, **caracterizado por que** el identificador de acceso se almacena en un entorno de seguridad del aparato de telecomunicaciones (10).

8. Procedimiento, según la reivindicación 7, **caracterizado por que** para consultar el identificador de acceso almacenado se requiere el establecimiento de la primera conexión de comunicación (20) entre el aparato de telecomunicaciones (10) y el elemento de seguridad portátil (12) por medio de la interfaz inalámbrica.

9. Procedimiento, según una de las reivindicaciones anteriores, **caracterizado por que** para transmitir los datos específicos de elemento de seguridad y/o los datos específicos de aparato de telecomunicaciones a la unidad de servicio (16) se requiere una autentificación.

Fig. 1

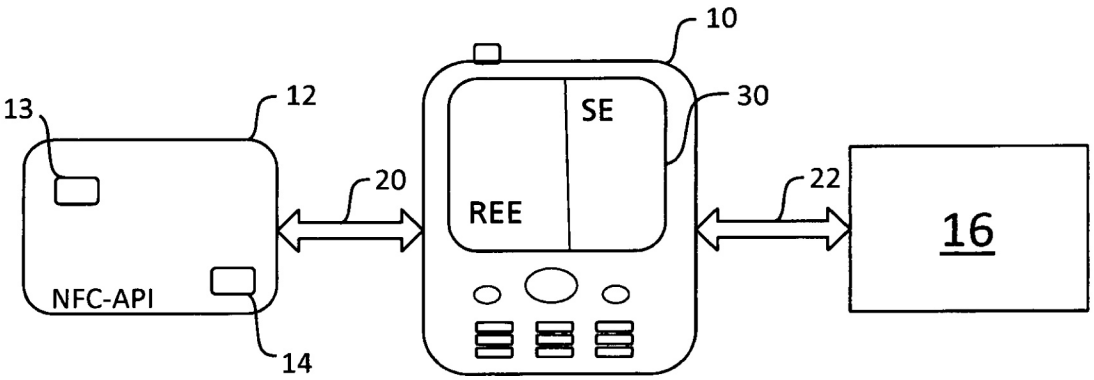
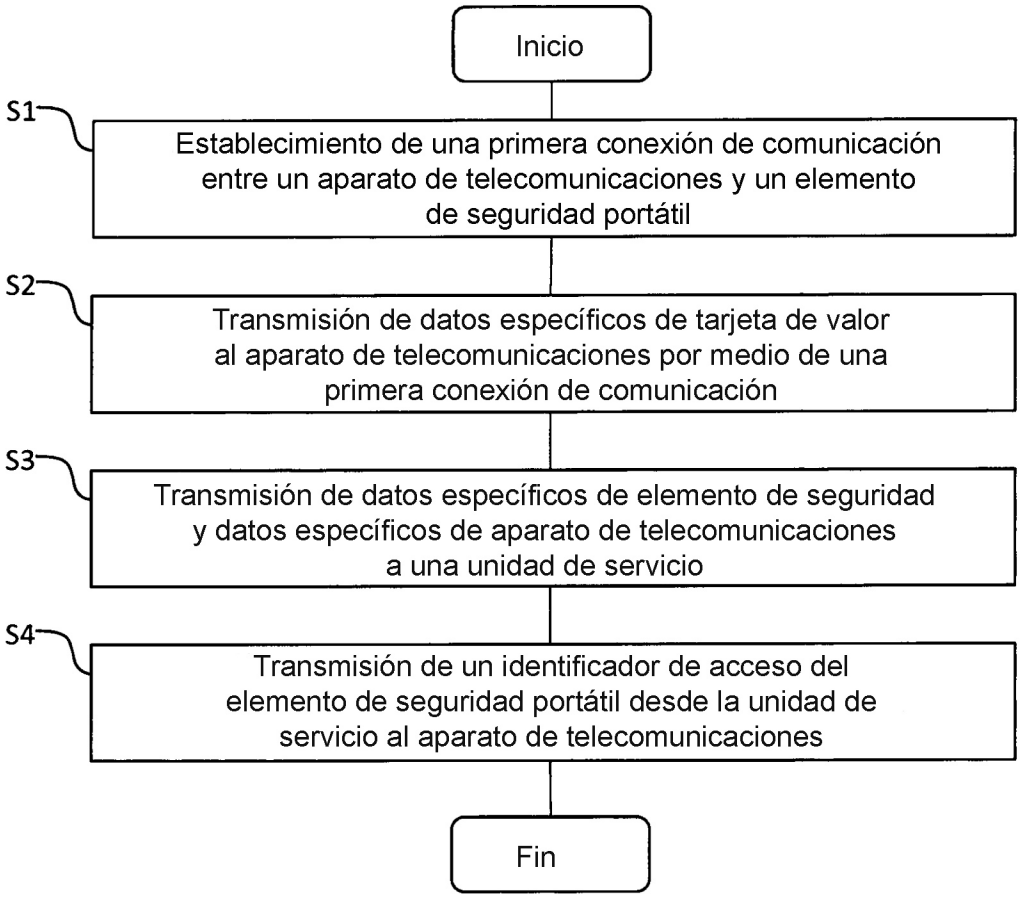

10
13
12
SE
30
20
REE
22
16
NFC-API
14

Fig. 2


Inicio
S1
Establecimiento de una primera conexión de comunicación entre un aparato de telecomunicaciones y un elemento de seguridad portátil
S2
Transmisión de datos específicos de tarjeta de valor al aparato de telecomunicaciones por medio de una primera conexión de comunicación
S3
Transmisión de datos específicos de elemento de seguridad y datos específicos de aparato de telecomunicaciones a una unidad de servicio
S4
Transmisión de un identificador de acceso del elemento de seguridad portátil desde la unidad de servicio al aparato de telecomunicaciones
Fin