(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 881**

(51) Int. Cl.:
G06Q 20/00 (2006.01)
H04L 9/32 (2006.01)
G06F 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06829408 .1**
(96) Fecha de presentación : **08.12.2006**
(97) Número de publicación de la solicitud: **1964042**
(97) Fecha de publicación de la solicitud: **03.09.2008**

(54) Título: **Procedimiento para la preparación de una tarjeta chip para servicios de firma electrónica.**

(30) Prioridad: **24.12.2005 DE 10 2005 062 307**

(45) Fecha de publicación de la mención BOPI:
27.05.2011

(45) Fecha de la publicación del folleto de la patente:
27.05.2011

(73) Titular/es: **T-MOBILE INTERNATIONAL AG.**
Landgrabenweg 151
53227 Bonn, DE

(72) Inventor/es: **Dupre, Michael**

(74) Agente: **Álvarez López, Fernando**

DESCRIPCIÓN

Procedimiento para la preparación de una tarjeta chip para servicios de firma electrónica

La invención se refiere a un procedimiento para la preparación de una tarjeta chip para servicios de firma electrónica. En especial, la invención se refiere a la preparación de tarjetas de identificación de abonados, las denominadas tarjetas SIM, para servicios de firma electrónica a través de telefonía móvil.

Una firma electrónica consiste en datos electrónicos que deben garantizar la autenticidad e integridad de informaciones electrónicas, en la mayoría de los casos, documentos electrónicos. Además, una firma electrónica debe garantizar la identidad del firmante. Esta característica debe poderse verificar, a su vez, con ayuda de la firma electrónica. Con estas propiedades, la firma electrónica debe representar el equivalente electrónico a la firma manuscrita. Según la tecnología de firma empleada, el escenario de uso existente así como la situación jurídica dada, se alcanzan estas características pretendidas de la firma electrónica.

Una firma electrónica se basa, en la mayoría de los casos, en procedimientos criptográficos asimétricos. La clave pública conocida, denominada *public key*, de un firmante permite la comprobación de su firma, que se ha generado con su clave secreta, la denominada *private key*. Sin embargo, a diferencia de las firmas cualificadas, en el caso de firmas avanzadas, las claves públicas y secretas no deben estar asociadas al firmante. Con ello, puede comprobarse la autenticidad e integridad de los datos firmados, pero no es posible una identificación del firmante mediante un certificado. En este caso, por ejemplo, procedimientos biométricos tales como, por ejemplo, la firma manuscrita que se registra durante el acto de firma y se incluye cifrada en el documento, pueden contribuir a la identificación. Para garantizar los datos biométricos, estos se incluyen adicionalmente en el valor Hash (suma de comprobación). Durante una comprobación de la firma, se comprueba entonces, además de los datos firmados, también la autenticidad e integridad de la característica de identificación.

Para la identificación del firmante y la autorización del servicio de firma se utiliza, por ejemplo, un número secreto (PIN). Hasta el momento, este PIN lo genera un proveedor de servicios, se asigna de forma unívoca (personalizada) a un usuario, y se transmite al usuario junto con la clave de firma por una vía de comunicación, por ejemplo, por carta. En este procedimiento existe el riesgo de que un tercero, a través de espionaje de los datos de firma y el PIN, utilice estos datos de forma fraudulenta y pueda hacerse pasar por el firmante. Asimismo, normalmente mediante la generación del PIN se ocasiona un coste no despreciable.

El documento US 2002/00 42879 A1 da a conocer un sistema de firma electrónica en el que se utiliza una tarjeta chip de firma electrónica con la que puede intercambiarse información entre un usuario de la tarjeta chip de firma y un portal de firmas. En la tarjeta chip de firma están almacenados datos de firma. Un usuario puede autentificarse frente a la tarjeta chip de firma introduciendo un número secreto (PIN) o datos biométricos. Si la autentificación ha sido satisfactoria, la tarjeta chip de firma genera una clave de autorización que se transmite al portal de firmas, el cual emite entonces la firma electrónica y un número de autentificación.

El documento 200210023217A1 da a conocer un procedimiento para la fabricación de dispositivos electrónicos para la generación de firmas digitales. En un entorno seguro, se genera un par asimétrico de claves y se almacena, junto con otras informaciones, en el dispositivo electrónico.

Un procedimiento para la preparación de una tarjeta chip para servicios de firma electrónica no se indica en el estado de la técnica antes indicado.

Por tanto, el objetivo de la invención consiste en proponer un procedimiento para la preparación de una tarjeta chip para servicios de firma electrónica que sea sencillo de realizar y ofrezca una buena seguridad frente a ataques.

Este objetivo se consigue mediante un procedimiento con las características de la reivindicación 1.

Según la invención, se propone un procedimiento en el que se intercambian informaciones entre un usuario de la tarjeta chip y un portal de firmas, y un par asimétrico de claves y un PIN de firma asociado al par asimétrico de claves se generan directamente en la tarjeta chip mediante una aplicación de software que puede ejecutarse directamente en la tarjeta chip.

Por tanto, se facilita un procedimiento para preparar una aplicación de tarjeta chip para servicios de firma. La aplicación de tarjeta chip genera internamente un par asimétrico de claves, es decir, una clave secreta y una clave

pública, y un PIN de firma y envía la clave pública de forma segura a un portal de firmas para el registro. Una identificación de usuario, por ejemplo, un número de telefonía móvil, y un denominado *token*, por ejemplo, un número aleatorio, se utilizan para identificar y autentificar al usuario frente al portal de firmas o la tarjeta chip. El procedimiento según la invención se caracteriza, entre otras cosas, por lo siguiente:

- el PIN de firma se genera dentro de la tarjeta chip y, a continuación, se le indica al usuario. Se suprime una costosa personalización y transmisión del PIN al usuario.
- no se requiere ningún terminal especial para la ejecución del procedimiento: es suficiente con cualquier teléfono móvil con herramientas de aplicación SIM.

A continuación, el portal de firmas está en condiciones de permitir firmar transacciones mediante la tarjeta chip. No se requiere necesariamente un certificado.

La ventaja de la invención consiste en que se suprime una personalización relativamente costosa necesaria hasta el momento de un PIN de firma en el portal de firmas y una transmisión al usuario. Dado que se suprime la generación de un PIN de firma a través de otra parte y una transmisión del PIN de firma al usuario, también se reduce el riesgo de espionaje y uso fraudulento de estos datos. Otra ventaja consiste en que el PIN de firma se predetermina al usuario de la tarjeta chip y, por tanto, se selecciona automáticamente un PIN de firma lo más “aleatorio / seguro” posible.

En las reivindicaciones dependientes se indican configuraciones ventajosas y variantes preferidas de la invención.

Mediante la figura 1 se explica detalladamente un desarrollo simplificado del procedimiento según la invención.

Según la invención, se establece un portal de firmas 10 que coordina la realización de servicios de firma y registra y gestiona a cualquier usuario que desee utilizar servicios de firma electrónica. Un usuario que desee utilizar servicios de firma electrónica necesita una tarjeta de chip electrónica 11 en la que está instalada una aplicación de software correspondiente para la preparación y realización de servicios de firma. Para la introducción y emisión de datos en o desde la tarjeta de chip 11 es necesario un terminal 12 que pueda leer datos de la tarjeta chip y pueda escribir datos en la tarjeta chip así como que disponga de dispositivos correspondientes de introducción y emisión para los datos, tales como, por ejemplo, un teclado y un campo de indicación. Además, se requieren medios de comunicación correspondientes con los que el terminal 12 y la tarjeta chip 11 operada con el terminal puedan comunicarse con el servidor de firmas 10. De forma ventajosa, un teléfono móvil moderno puede utilizarse como terminal 12 dado que dispone de unidades de introducción y emisión correspondientes y dispositivos de tratamiento de datos relativamente potentes. Además, el teléfono móvil puede utilizarse directamente como medio de comunicación para el establecimiento de una conexión de comunicación entre la tarjeta chip 11 y el portal de firmas 10. No obstante, como terminal también puede servir, por ejemplo, un ordenador personal, que, por ejemplo, está conectado a través de Internet con el portal de firmas. En el siguiente ejemplo se describe el uso de un teléfono móvil como terminal. Se presupone que el usuario es al mismo tiempo abonado de una red de telefonía móvil en la que puede registrarse el terminal.

Paso 1:

El usuario, que ya es conocido en el portal de firmas, establece a través de su terminal 12 una conexión con el portal de firmas 10 registrándose allí mediante una identificación de usuario. En función de la identificación de usuario utilizada, el usuario la introduce si el portal de firmas no puede determinarla automáticamente. Por ejemplo, como código de usuario puede utilizarse el número de teléfono móvil del usuario, que se transmite automáticamente al portal de firmas (función CLIP). En cuanto el usuario ha establecido una conexión con el portal de firmas 10, activa en el portal de firmas 10 una función para la generación de un nuevo par de claves en la tarjeta chip 11.

Paso 2:

El portal de firmas 10 genera a continuación un *token*, por ejemplo, un número largo en forma de un número aleatorio, y lo almacena en un conjunto de datos correspondiente asociado al usuario. El *token* se envía al usuario por una vía independiente, por ejemplo, por carta.

Paso 3:

El usuario confirma la recepción del *token*, por ejemplo, con su firma.

Paso 4:

En la tarjeta chip 11 está instalada una aplicación de software 11a correspondiente que ahora puede ser iniciada por el usuario. Esto puede hacerlo, por ejemplo, el mismo usuario una vez que ha recibido un mensaje corto (SMS) del portal de firmas (activador) o puede suceder automáticamente mediante un OTA-SMS.

Paso 5:

La aplicación de software 11 solicita al usuario el *token* que se le ha enviado, por ejemplo, con el comando UICC proactivo “GET INPUT”. El usuario introduce el *token* a través del teclado del terminal 12. La aplicación de software 11a genera internamente un nuevo par asimétrico de claves. Se elimina un par de claves ya existente eventualmente, por ejemplo, si el usuario deseara renovar el par de claves o el PIN de firma vinculado a este.

Paso 6:

La aplicación de software 11a genera, utilizando el *token*, un PIN de firma y se lo proporciona al usuario en la pantalla del terminal 12, por ejemplo, con el comando UICC proactivo “DISPLAY TEXT”. Esto permite que el PIN de firma, fuera de la tarjeta chip 11, solo sea conocido por el usuario y, sin embargo, se seleccione de forma aleatoria.

Paso 7:

La aplicación de software 11a registra la clave pública en el portal de firmas 10. Para ello, con la clave secreta (privada) generada nuevamente genera una firma mediante una estructura de datos que contiene al menos la clave pública y el *token*, así como, en caso necesario, una identificación de usuario. La firma y la clave pública, así como, en caso necesario, la identificación de usuario son enviadas por la aplicación de software 11a al portal de firmas 10. La transmisión puede realizarse, por ejemplo, a través de SMS de la red de telefonía móvil. Si estos datos se envían por SMS, el número de teléfono móvil puede utilizarse como identificación de usuario, que se comunica automáticamente al receptor (aquí: el portal de firmas 10) durante el envío del SMS. Con ello, el portal de firmas 10 puede asignar el SMS de forma unívoca al usuario.

El portal de firmas 10 que ha generado el *token* y, por tanto, lo conoce, verifica la firma y autentifica con ello al usuario. La firma sirve al portal de firmas 10 como justificante de que el usuario posee la clave privada correspondiente.

La firma introducida a través de la estructura de datos que contiene el *token* autentifica al usuario frente al portal de firmas. Un ataque es tanto más difícil cuanto más larga es la secuencia de caracteres del *token*. Además, el portal de firmas puede permitir indicar una huella dactilar del usuario a través de la clave pública, que también puede calcular y visualizar la aplicación de software 11a en la tarjeta chip 11 y que el propio usuario debe verificar y, dado el caso, confirmar frente al portal de firmas 10.

Si el usuario ha olvidado su PIN de firma, puede iniciar nuevamente en cualquier momento el procedimiento descrito para la generación de un nuevo par de claves y un PIN de firma asociado. En este caso, debe eliminarse el par de claves existente en el portal de firmas. La aplicación de tarjeta chip elimina también el par de claves existente y genera nuevamente tanto la clave como el PIN.

REIVINDICACIONES

1. Procedimiento para la preparación de una tarjeta chip (11) para servicios de firma electrónica en los que se intercambian informaciones entre un usuario de la tarjeta chip y un portal de firmas (10), caracterizado por los siguientes pasos:
- registro del usuario en el portal de firmas (10),
- generación de un *token* asociado al usuario a través del portal de firmas (10) y almacenamiento del *token* en el portal de firmas (10),
- transmisión del *token* desde el portal de firmas (10) al usuario,
- generación del par asimétrico de claves compuesto por una clave pública y una clave secreta, y un PIN de firma asociado al par asimétrico de claves por medio de una aplicación de software (11a) que puede ejecutarse en la tarjeta chip (11) y utilizando el *token*,
- comunicación del PIN de firma al usuario a través de la tarjeta chip,
- transmisión de la clave pública y una firma desde la tarjeta chip al portal de firmas (10),
- registro de la clave pública del usuario junto con el *token* asociado al usuario en el portal de firmas.

2. Procedimiento según la reivindicación 1, caracterizado porque el PIN de firma se genera sin ayuda o influencia del usuario.

3. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque la firma contiene el *token* y, alternativamente, datos adicionales para la identificación del usuario, habiéndose cifrado el *token* y los datos adicionales con la clave secreta del usuario.

4. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque el *token* se transmite al usuario desde el portal de firmas a través de una vía no electrónica.

5. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque el usuario y su clave pública son autentificados por el portal de firmas mediante la firma.

6. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque como *token* se utiliza un número aleatorio generado por el portal de firmas.

7. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque para la comunicación entre la tarjeta chip (11) y el usuario se utiliza un terminal (12).

8. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque para la comunicación entre la tarjeta chip (1) y el portal de firmas (11) se utiliza un terminal (12) compatible con un sistema de comunicación móvil.

9. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque el terminal (12) se utiliza como dispositivo de entrada de datos, dispositivo de emisión de datos y como dispositivo para la comunicación para el intercambio de datos entre la tarjeta chip (11) y el portal de firmas (10).

10. Procedimiento según una de las reivindicaciones anteriores, caracterizado porque el terminal (12) es un teléfono móvil.

11. Aplicación de software (11a) con un código de programa que, ejecutado en una tarjeta chip (11), realiza un procedimiento según una de las reivindicaciones 1 a 10.

12. Producto de programa de tratamiento de datos que comprende una aplicación de software (11a) ejecutable en una tarjeta chip (11) para la realización del procedimiento según una de las reivindicaciones 1 a 10.

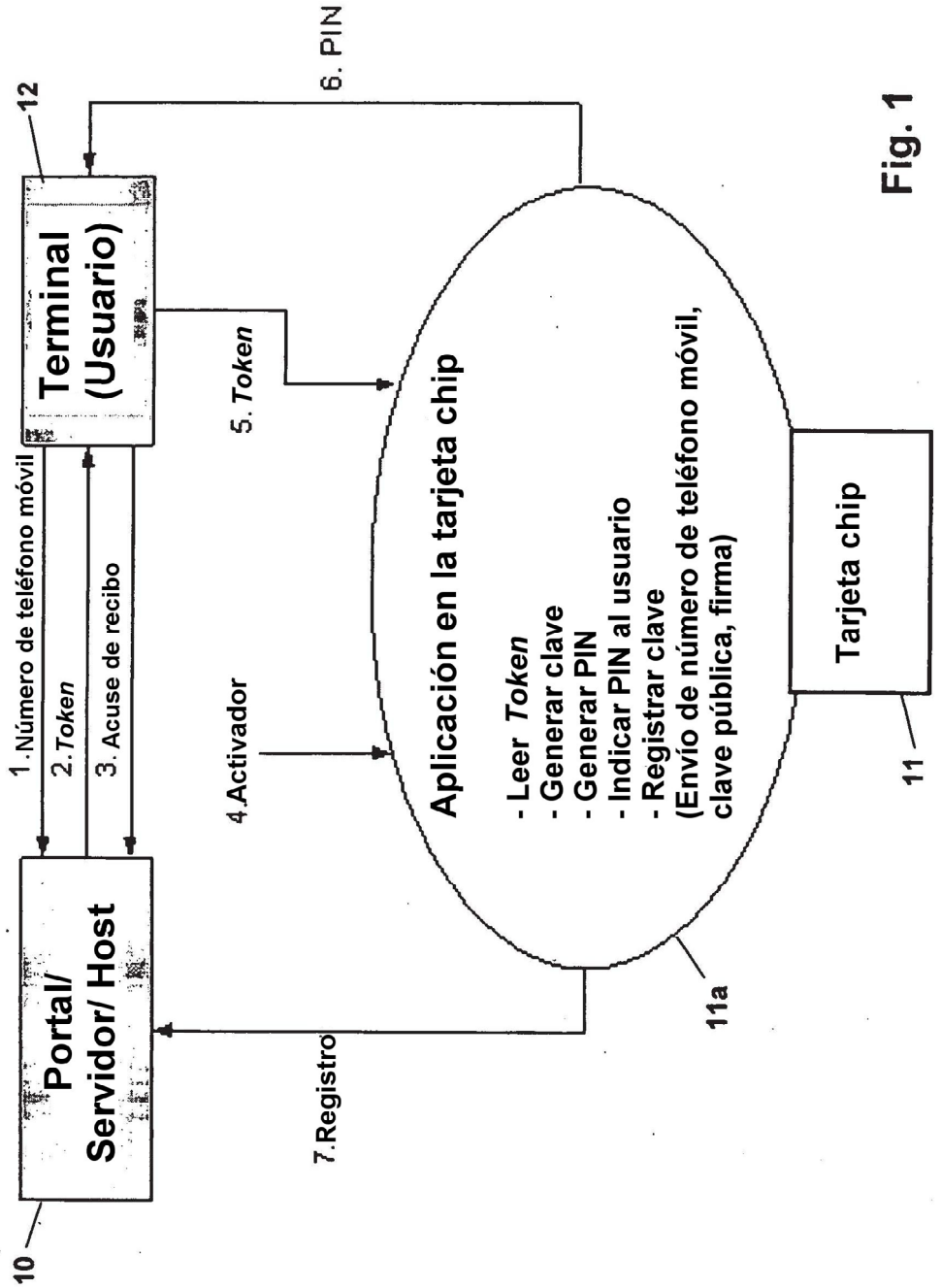
12
6. PIN
Terminal (Usuario)
5. Token
1. Número de teléfono móvil
2. Token
3. Acuse de recibo
4. Activador
Aplicación en la tarjeta chip
- Leer Token
- Generar clave
- Generar PIN
- Indicar PIN al usuario
- Registrar clave
(Envío de número de teléfono móvil, clave pública, firma)
Tarjeta chip
11
11a
Portal/ Servidor/ Host
7. Registro
10

Fig. 1