(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 753 964**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/41 (2013.01)
G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.08.2012 PCT/EP2012/066324**

(87) Fecha y número de publicación internacional: **07.03.2013 WO13030060**

(96) Fecha de presentación y número de la solicitud europea: **22.08.2012 E 12751053 (5)**

(97) Fecha y número de publicación de la concesión europea: **02.10.2019 EP 2751950**

(54) Título: **Procedimiento para generar un software token, producto de programa informático y sistema informático de servicio**

(30) Prioridad:

02.09.2011 DE 102011082101

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.04.2020

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
Oranienstrasse 91
10969 Berlin, DE

(72) Inventor/es:

DIETRICH, FRANK y
KRAUS, MICHA

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para generar un software token, producto de programa informático y sistema informático de servicio

La presente invención hace referencia a un procedimiento para generar un software token, a un producto de programa informático, a un sistema informático de servicio, así como a un sistema de procesamiento de datos.

Por el estado de la técnica ya es conocida la utilización de software token, los cuales se denominan también como token software, con el fin de una autenticación. Una desventaja del software token es que pueden hacerse copias del mismo. Esto representaba una posibilidad de intervención para un mal uso del software token.

En particular, por el estado de la técnica se conocen software token según el estándar U-Prove, los cuales se denominan como U-Prove-tokens. Un U-Prove-token de esa clase puede asegurarse mediante hardware, dividiendo la clave privada de un U-Prove-token entre dos aparatos (véase al respecto U-Prove- Technology OverView V1.1, Revisión del borrador 1, Microsoft Corporation 2011, capítulo 6 en la página 18).

Por la solicitud de patente DE 102009027686 A1 se conoce un procedimiento para la lectura de al menos un atributo almacenado en un token de ID, en donde al token de ID se encuentra asociado un usuario. El procedimiento comprende los siguientes pasos: autenticación del usuario con respecto al token de ID, autenticación de un primer sistema informático con respecto al token de ID, después de finalizada con éxito la autenticación del usuario y del primer sistema informático con respecto al token de ID, transmisión de una indicación temporal desde el primer sistema informático hacia el token de ID para generar una contraseña con la ayuda de la indicación temporal mediante el token de ID, acceso de lectura del primer sistema informático a por lo menos un atributo almacenado en el token de ID, para la transmisión de al menos un atributo según su firma, hacia un segundo sistema informático.

Por consiguiente, el objeto de la presente invención consiste en proporcionar un procedimiento mejorado para generar un software token, así como un producto de programa informático, un sistema informático de servicio y un sistema de procesamiento de datos.

El objeto que constituye la base de la invención se soluciona respectivamente con las características de las reivindicaciones independientes. En las reivindicaciones dependientes se indican formas de realización de la presente invención.

Las formas de realización de la invención son particularmente ventajosas, ya que como fuente de datos para la generación del software token se utiliza un token de ID de un usuario, y el software token se vincula de forma criptográfica a un elemento de seguridad del mismo usuario, para de ese modo garantizar un máximo de seguridad, al mismo tiempo que un manejo cómodo.

Como un "software token", según la invención, se entienden en particular datos firmados que pueden utilizarse para la autenticación de un usuario, en particular U-Prove-tokens. En particular, los datos firmados pueden contener uno o una pluralidad de atributos de un usuario que están firmados por una instancia acreditada.

Según la invención, como un "elemento de seguridad" se entiende en particular un dispositivo que presenta al menos un área de memoria protegida, en la cual se almacenan datos, de manera que los mismos están protegidos contra manipulaciones y espionaje, como por ejemplo una tarjeta inteligente, en particular una tarjeta de módulo de identificación de abonado (SIM), una memoria USB, un módulo de plataforma confiable (TPM) u otro aparato con un área de memoria protegida mediante medidas de hardware y/o de software. Por ejemplo, el elemento de seguridad está diseñado en forma de una tarjeta, de manera que un usuario puede llevarlo fácilmente consigo.

Según la invención, como una "conexión asegurada de forma criptográfica" se entiende una conexión en la cual los datos transmitidos mediante la conexión están cifrados, para protegerlos contra manipulaciones y/o espionaje, en particular contra un copiado. Para establecer una conexión asegurada de forma criptográfica puede emplearse un procedimiento de cifrado asimétrico o un procedimiento de cifrado simétrico, en particular un intercambio de claves Diffie-Hellman (DH).

Como un "sistema informático de servicio", según la invención, se entiende en particular un sistema informático que se utiliza para prestar un servicio, a saber, la generación de un software token para un usuario.

Como una "contraseña de un solo uso" (OTP), según la invención, se entiende en particular una contraseña de un único uso o palabra de identificación de un solo uso, la cual se genera por ejemplo con la ayuda de un generador de palabra de identificación. Una OTP se utiliza para la autenticación y sólo es válida para un único proceso, por tanto, no puede usarse dos veces. Para la autenticación de un usuario, el mismo debe ingresar una contraseña de un solo uso correcta.

Como un "sistema informático del usuario", según la invención, se entiende en particular un ordenador personal (PC), un ordenador portátil u otro ordenador de un usuario, como por ejemplo un aparato electrónico que presenta la funcionalidad de un ordenador móvil u otro ordenador portable.

Como un "token de ID", según la invención, se entiende en particular un aparato electrónico portátil, como por ejemplo una así llamada memoria USB, o un documento, en particular un documento de valor o un documento de seguridad. El token de ID posee una memoria electrónica en la cual está almacenado al menos un atributo.

Como un "documento", según la invención, se entienden en particular documentos en base a papel y/o en base a plástico, como por ejemplo documentos de identidad, en particular pasaportes, documentos de identidad personal, visados, así como permisos de conducir, documentos de registro de vehículos, certificados de propiedad de vehículos, tarjetas de identificación de empresas, tarjetas sanitarias u otros documentos de identificación, así como también tarjetas inteligentes, medios de pago, en particular billetes, tarjetas bancarias y tarjetas de crédito, cartas de porte u otros comprobantes de autorización, en los cuales se encuentra integrada una memoria de datos para almacenar al menos un atributo.

Según las formas de realización de la invención, el usuario es propietario de un token de ID, como por ejemplo de un documento de identidad electrónico, en particular de un pasaporte electrónico o de un documento de identidad personal electrónico. Además, el usuario dispone de un elemento de seguridad, como por ejemplo de una tarjeta inteligente. El elemento de seguridad tiene un área de memoria protegida, en la cual está almacenada una clave secreta de un primer par de claves criptográfico asimétrico.

Entre un aparato electrónico del usuario y un sistema informático de servicio se establece una primera conexión asegurada de forma criptográfica, mediante la cual el usuario solicita la generación del software token.

El aparato electrónico puede tratarse de un terminal móvil, en particular de un dispositivo de telefonía móvil, un teléfono inteligente, un ordenador portable, un sistema informático del usuario, u otro terminal móvil que funcione con baterías, con una interfaz de comunicaciones con respecto al elemento de seguridad.

Preferentemente, la interfaz de comunicaciones está diseñada para el establecimiento de una conexión local con el elemento de seguridad, por ejemplo como interfaz de tarjeta inteligente con o sin contacto. De manera especialmente preferente, el aparato electrónico se trata de un teléfono móvil, en particular de un así llamado teléfono inteligente, y el elemento de seguridad se trata de una tarjeta inteligente de telecomunicaciones, en particular de una tarjeta SIM que se encuentra en un dispositivo lector de tarjeta inteligente integrado, del aparato electrónico.

Debido a la recepción de la petición para generar el software token, el sistema informático de servicio genera una contraseña de un solo uso con la ayuda de un generador de palabras de identificación correspondiente, y registra la contraseña de un solo uso generada como identificador de la primera conexión, para establecer una sesión. La contraseña de un solo uso se transmite al aparato electrónico mediante la primera conexión, y se emite desde el aparato electrónico, mediante una interfaz del usuario. Por ejemplo, la contraseña de un solo uso se muestra en una unidad de visualización del aparato electrónico, de manera que un usuario puede leer la contraseña de un solo uso desde la unidad de visualización.

Entre el sistema informático del usuario y el sistema informático de servicio se establece una segunda conexión asegurada de forma criptográfica. El usuario ingresa en su sistema informático del usuario la contraseña de un solo uso emitida mediante la interfaz del usuario del aparato electrónico, de manera que esa contraseña de un solo uso se transmite desde el sistema informático del usuario hacia el sistema informático de servicio, mediante la segunda conexión. Como la "transmisión de la contraseña de un solo uso" se entiende aquí también que el sistema informático del usuario deriva una identificación desde la contraseña de un solo uso, según un algoritmo predeterminado, y que esa identificación, y no obligatoriamente la propia contraseña de un solo uso, se transmite mediante la segunda conexión.

Mediante el sistema informático de servicio tiene lugar después una verificación de si la contraseña de un solo uso registrada y enviada coincide con la contraseña de un solo uso recibida, o con la identificación derivada de la misma. Sólo si es ese el caso, al menos un atributo se lee desde el token de ID del usuario, generándose con ello el software token, en donde en la generación del software token se incluye también la clave pública del primer par de claves criptográfico. El software token así generado se transmite entonces, mediante la primera conexión, al aparato electrónico, y/o mediante la segunda conexión, al sistema informático del usuario, del usuario, es decir, dentro de la sesión establecida ahora de forma exitosa, la cual contiene las primeras y las segundas conexiones.

Lo mencionado se considera especialmente ventajoso, ya que, por una parte, está asegurado que uno y el mismo usuario sea efectivamente el propietario, tanto del token de ID, como también del elemento de seguridad y, por otra parte, que los atributos que se incluyen en la generación del software token, también pertenezcan efectivamente a ese usuario.

Según una forma de realización de la invención, la visualización de la contraseña de un solo uso en la unidad de visualización del aparato electrónico, así como sistema informático del usuario, tiene lugar en forma de un patrón óptico legible por máquina, en particular en forma de un código de barras unidimensional o bidimensional, o como código de líneas bidimensional, en particular como código QR. El ingreso de la contraseña de un solo uso mediante el usuario puede tener lugar entonces de manera que el usuario registra una foto digital desde el patrón óptico legible por máquina, por ejemplo mediante una cámara digital integrada en el aparato electrónico o en el sistema

informático del usuario. El patrón óptico legible por máquina se decodifica entonces automáticamente, de manera que no se necesita el ingreso manual de la contraseña de un solo uso mediante el usuario. Lo mencionado en particular ofrece la ventaja de que pueden utilizarse contraseñas de un solo uso más largas, lo cual incrementa aún más la seguridad del procedimiento según la invención.

Según una forma de realización de la invención, el elemento de seguridad posee un área de memoria que puede leerse libremente, en la cual está almacenada una clave pública del primer par de claves. Esta clave pública se transmite desde el elemento de seguridad hacia el aparato electrónico mediante la conexión local, por tanto, no mediante una conexión de red, sino por ejemplo mediante una interfaz de tarjeta inteligente sin contacto o con contacto. La clave pública se transmite después desde el aparato electrónico hacia el sistema informático de servicio, mediante la primera conexión asegurada de forma criptográfica. La contraseña de un solo uso generada por el sistema informático de servicio es cifrada con esa clave pública, y el cifrado resultante de ello se transmite desde el sistema informático de servicio hacia el aparato electrónico, mediante la primera conexión.

Mediante la conexión local, la contraseña de un solo uso cifrada se reenvía entonces desde el aparato electrónico hacia el elemento de seguridad, donde se descifra con la ayuda de la clave secreta. La contraseña de un solo uso descifrada se transmite entonces desde el elemento de seguridad hacia el aparato electrónico, mediante la conexión local, de manera que el aparato electrónico puede emitir la contraseña de un solo uso mediante su interfaz del usuario.

Las formas de realización de la invención son particularmente ventajosas, ya que el software token está vinculado criptográficamente al elemento de seguridad, de manera que el software token presenta el mismo nivel de fiabilidad o un nivel de fiabilidad similar que el token de ID, sin estar vinculado físicamente al elemento de seguridad. Por ejemplo, el software token puede estar almacenado en el propio elemento de seguridad, en el aparato electrónico del usuario, en el sistema informático del usuario o en otra memoria electrónica, ya que para la autenticación del usuario, adicionalmente con respecto al software token, se necesita adicionalmente también la presencia del elemento de seguridad, por ejemplo para comprobar un protocolo de desafío-respuesta, de manera que el elemento de seguridad se encuentra en posesión de la clave privada del primer par de claves, cuya clave pública también está incluida en la generación del software token. Una presentación de esa clase del software token y del elemento de seguridad, con el fin de la autenticación del usuario, puede tener lugar por ejemplo según el protocolo U-prove.

Según una forma de realización de la invención, el sistema informático de servicio posee un primer componente de programa para generar la contraseña de un solo uso, para cifrar la contraseña de un solo uso y para generar el software token En particular, por tanto, el primer componente de programa puede contener un generador de palabra de identificación para generar la contraseña de un solo uso. El sistema informático de servicio posee además un segundo componente de programa para la recepción de la contraseña de un solo uso por el sistema informático del usuario, en donde la primera conexión se establece entre el aparato electrónico y el primer componente de programa, y la segunda conexión se establece entre el sistema informático del usuario y el segundo componente de programa.

Según una forma de realización de la invención, por parte del usuario, se encuentra presente solamente el sistema informático del usuario, sin un aparato electrónico separado. Por ejemplo, el sistema informático del usuario puede tratarse de un teléfono inteligente que presenta tanto las funcionalidades de un sistema informático del usuario, como también las de un teléfono móvil, como por ejemplo un iPhone o iPad. En esos casos, las primeras y las segundas conexiones aseguradas de forma criptográfica estarían establecidas por ejemplo como dos sesiones diferentes, entre el sistema informático de servicio y el sistema informático del usuario.

Según una forma de realización de la invención, la lectura de al menos un atributo desde el token de ID tiene lugar con la ayuda de un sistema informático de proveedor de ID.

Como un "sistema informático de proveedor de ID", según la invención, se entiende en particular un sistema informático que dispone de un certificado de autorización, en el cual se encuentra especificada una autorización para la lectura de al menos un atributo desde el token de ID del usuario. El sistema informático de proveedor de ID, por ejemplo, puede estar diseñado según la solicitud DE 10 2008 000 067 A1, DE 10 2008 040 416, DE 10 2008 042 262, DE 10 2009 026 953, DE 10 2009 027 723, DE 10 2009 027 681 y/o DE 10 2010 028 133.6.

Como un "certificado" se entiende aquí un certificado digital que se denomina también como certificado de clave pública. Un certificado se trata de datos estructurados que se utilizan para asociar una clave pública de un criptosistema asimétrico a una identidad, como por ejemplo a una persona o a un dispositivo. Por ejemplo, el certificado puede corresponder al estándar X.509 o a otro estándar. En particular, el mismo puede tratarse de un certificado SSL o de un certificado TLS.

Como un "certificado de autorización" se entiende aquí un certificado que contiene una especificación de derechos de acceso a los atributos almacenados en el token de ID. Un certificado de autorización puede contener una remisión a uno o a más certificados, en particular certificados SSL o TLS, que están asociados al certificado de autorización.

Las formas de realización de la invención son particularmente ventajosas, ya que al menos un atributo se lee desde un token de ID especialmente acreditado, por ejemplo desde un documento oficial. Además, se considera especialmente ventajoso que no se requiera un almacenamiento central de los atributos. Por consiguiente, las formas de realización de la invención posibilitan un máximo nivel de fiabilidad en cuanto a la comunicación de los atributos que pertenecen a una identidad digital, combinado con una protección óptima de los datos y con un manejo extremadamente cómodo.

Según una forma de realización de la invención, las primeras y las segundas conexiones aseguradas de forma criptográfica se tratan respectivamente de conexiones de capa de transporte. Por ejemplo, las primeras y las segundas conexiones se tratan respectivamente de conexiones de Transport-Layer-Security (TLS) o Secure Sockets Layer (SSL). La tercera conexión con cifrado de extremo a extremo entre el token de ID y el sistema informático de proveedor de ID, en cambio, se establece en una capa más elevada, como por ejemplo una capa de aplicación.

Según una forma de realización de la invención, el sistema informático de servicio genera un objeto Security Assurance Markup Language (SAML) que contiene la especificación del atributo, de los atributos que deben leerse desde el token de ID, y la firma del sistema informático de servicio. El objeto SML se transmite al sistema informático de proveedor de ID. El sistema informático de proveedor de ID contiene un componente de lógica SAML, es decir, un producto de programa informático para la recepción y el procesamiento de objetos SAML.

Según una forma de realización de la invención, el sistema informático de proveedor de ID transmite al menos un atributo en forma de un objeto SAML, hacia el sistema informático de servicio, después de que el sistema informático de proveedor de ID ha leído al menos un atributo desde el token de ID y ha almacenado los atributos leídos en el objeto SAML recibido en primer lugar por el sistema informático de servicio.

Según una forma de realización de la invención, la generación del software token tiene lugar mediante el sistema informático de servicio mediante una firma ciega o como U-Prove-token.

Según una forma de realización de la invención pueden generarse varios software token para el mismo elemento de seguridad. Para ello, a cada software token se encuentra asociado un par de claves criptográfico asimétrico separado. La clave secreta de ese otro par de claves puede estar almacenada por ejemplo en una memoria del aparato electrónico, con el par de claves público del primer par de claves. Por ejemplo, el cifrado de la clave secreta puede estar almacenador en el sistema de archivos del aparato electrónico.

En otro aspecto, la presente invención hace referencia a un producto de programa informático, en particular a un medio de memoria digital, en el cual se encuentran almacenadas instrucciones de programa ejecutables para ejecutar un procedimiento según la invención.

En otro aspecto, la presente invención hace referencia a un sistema informático de servicio, así como a un sistema de procesamiento de datos que presenta al menos un sistema informático de servicio de esa clase y un sistema informático de proveedor de ID. Los componentes funcionales individuales de esos sistemas informáticos pueden de ese modo estar realizados en la misma unidad de software o en unidades de software diferentes, que por ejemplo pueden estar interconectadas unas con otras. Al sistema de procesamiento de datos pueden pertenecer el elemento de seguridad y/o el token de ID, el aparato electrónico y/o el sistema informático del usuario.

A continuación se explican con mayor detalle formas de realización de la invención, haciendo referencia a los dibujos. Las figuras muestran:

la figura 1 un diagrama de bloques de una primera forma de realización de un sistema de procesamiento de datos según la invención,

la figura 2 un diagrama de bloques de una segunda forma de realización de un sistema de procesamiento de datos según la invención,

la figura 3 un diagrama de flujo de una forma de realización de un procedimiento según la invención,

la figura 4 un diagrama UML de otra forma de realización de un procedimiento según la invención,

la figura 5 un diagrama de bloques de otra forma de realización de un sistema de procesamiento de datos según la invención,

la figura 6 un diagrama de flujo de un procedimiento para la lectura de al menos un atributo desde el token de ID,

la figura 7 un diagrama UML de otra forma de realización de un procedimiento según la invención.

Los elementos de las siguientes formas de realización que se corresponden unos con otros se indican con los mismos símbolos de referencia.

La figura 1 muestra un sistema de procesamiento de datos con un sistema informático del usuario 100 y con un token de ID 106, como por ejemplo un documento de identidad electrónico, del mismo usuario. Un sistema informático de proveedor de ID 136 se utiliza para la lectura de al menos un atributo que está almacenado en el token de ID. Por ejemplo, el sistema informático de proveedor de ID 136 puede implementar el eCard-API-Framework (marco de trabajo), tal como está especificado por la Oficina Federal de Seguridad de la Información de Alemania, en la Directiva Técnica TR-03112.

Un sistema informático de servicio 150 se utiliza para generar un software token para el usuario. Este software token tiene que estar vinculado de forma criptográfica a un elemento de seguridad 172 del mismo usuario. El intercambio de datos entre el sistema informático de servicio 150 y el elemento de seguridad 172 puede tener lugar mediante un aparato electrónico 174 del usuario.

Este aparato electrónico puede ser un terminal móvil separado, como por ejemplo un teléfono móvil, en particular un teléfono inteligente. En particular cuando el aparato electrónico 174 está diseñado como teléfono inteligente, el mismo puede cumplir también con la función del sistema informático del usuario 100, de manera que no se necesita un sistema informático del usuario 100 separado. Más bien, las funcionalidades del sistema informático del usuario 100 y del aparato electrónico 174 se cumplen mediante uno y el mismo aparato del usuario.

El sistema informático de servicio 150 puede presentar un primer componente de programa 176 que por ejemplo contiene un generador de palabra de identificación para generar una contraseña de un solo uso, el cual se utiliza para generar el software token. El sistema informático de servicio 150 puede presentar un segundo componente de programa 178 que en particular se utiliza para la recepción de la contraseña de un solo uso, por el usuario, así como también para la comunicación con el sistema informático de proveedor de ID 136.

El sistema informático de servicio 150 puede establecer una primera conexión 180 asegurada de forma criptográfica, hacia el aparato electrónico 174, y una segunda conexión 182 asegurada de forma criptográfica, hacia el sistema informático del usuario 100, como por ejemplo entre el componente de programa 176 y el aparato electrónico 174, así como entre el componente de programa 178 y el sistema informático del usuario 100.

La comunicación entre el aparato electrónico 174 y el elemento de seguridad 172 tiene lugar mediante una conexión local 184, como por ejemplo mediante una interfaz de tarjetas inteligentes del aparato electrónico 174; del mismo modo, la comunicación entre el sistema informático del usuario y el token de ID 106 tiene lugar mediante una conexión local 185 de esa clase.

El elemento de seguridad 172 tiene un área de memoria protegida 186, en la cual puede estar almacenada una clave secreta de un primer par de claves criptográfico asimétrico, la cual se encuentra asociada al elemento de seguridad 172. En un área de memoria 188 que puede leerse libremente, del elemento de seguridad 172, puede estar almacenada la clave pública correspondiente del primer par de claves.

Para generar un software token vinculado criptográficamente al elemento de seguridad 172, con la ayuda del token de ID 106, puede procederse ahora del siguiente modo:

Se establecen las conexiones 180 y 182. El usuario ingresa su petición para generar el software token, de manera que esa petición, mediante la conexión 180, se transmite al sistema informático de servicio 150, por ejemplo hacia el componente de programa 176. A continuación, mediante el sistema informático de servicio 150 se genera una contraseña de un solo uso que se transmite al usuario mediante la misma conexión 180, con la cual ha sido recibida la petición. El usuario debe ingresar esa contraseña de un solo uso, de manera que la misma, mediante la otra conexión, es decir la conexión 182, se retransmite hacia el sistema informático de servicio. Si coinciden la contraseña de un solo uso generada mediante el sistema informático de servicio 150 y la contraseña recibida, o bien una identificación derivada en base a ésta del lado del usuario, entonces, gracias a esto se asegura que ambas conexiones 180 y 182 se encuentran presentes con respecto a uno y al mismo componente.

A continuación, el sistema informático de servicio 150 genera una especificación de atributo, en la cual está especificado qué atributos tienen que leerse desde el token de ID 106. Esa especificación de atributo se envía desde el sistema informático de servicio 150 hacia el sistema informático de proveedor de ID 136, el cual a continuación, de manera conocida, lee desde el token de ID 106 los atributos especificados. Lo mencionado puede tener lugar por ejemplo conforme al eCard-API-Framework.

El sistema informático de proveedor de ID 136 responde entonces a la especificación de atributo del sistema informático de servicio 150 con los atributos leídos que, junto con la clave pública del elemento de seguridad 172, se incluyen en la generación del software token por parte del sistema informático de servicio 150. Este software token se transmite entonces desde el sistema informático de servicio, mediante una de las conexiones 180 o 182, hacia el usuario.

Por ejemplo, la generación del software token puede tener lugar según el estándar U-prove. En ese caso, el sistema informático de servicio 150 actúa como emisor, en donde la generación propiamente dicha del U-prove-token tiene lugar mediante el componente de programa 176. Mediante el componente de programa 178 se pone a disposición

un servicio de emisor, por ejemplo en forma de una página web, en la cual el usuario puede ingresar la contraseña de un solo uso.

En este caso, se considera especialmente ventajoso que no se requiera un almacenamiento intermedio del software token, lo cual incrementa la seguridad del sistema. En el caso de la utilización del estándar U-prove se considera especialmente ventajoso que el usuario en sí mismo puede especificar qué datos desea proporcionar y que pueda evitarse la creación de un perfil, como por ejemplo mediante los hábitos de compra del usuario.

La figura 2 muestra otra forma de realización de un sistema de procesamiento de datos según la invención, en donde aquí el sistema informático del usuario 100 cumple también con la funcionalidad del aparato electrónico 174. Ambas conexiones 180 y 182 se establecen por tanto con respecto al sistema informático del usuario 100, como por ejemplo en dos sesiones diferentes que se desarrollan de forma paralela una con respecto a otra. De forma análoga también es posible que la funcionalidad del sistema informático del usuario 100 sea asumida por el aparato electrónico 174, en particular cuando el mismo se trata de un así llamado teléfono inteligente.

La figura 3 muestra un diagrama de flujo de una forma de realización de un procedimiento según la invención.

En el paso 10, un elemento de seguridad se pone a disposición del usuario. Por ejemplo, el usuario puede adquirir de forma gratuita un elemento de seguridad que aún no está personalizado para el usuario. Para generar un software token, en particular un U-prove-token que tiene que vincularse al elemento de seguridad, se procede del siguiente modo:

En el paso 12 tiene lugar la transmisión de una petición para generar el software token, desde el usuario hacia el sistema informático de servicio, el cual a continuación, en el paso 14, genera una contraseña de un solo uso. Esa contraseña de un solo uso, en el paso 16, se transmite desde el sistema informático de servicio hacia el usuario, a saber, mediante una primera conexión asegurada de forma criptográfica. En el paso 18, el usuario debe ingresar esa contraseña de un solo uso recibida, de manera que la contraseña de un solo uso, o una identificación derivada de la misma según un algoritmo predeterminado, se transmite desde el usuario hacia el sistema informático de servicio, a saber, mediante una segunda conexión asegurada de forma criptográfica (paso 20). Después, en el paso 22, el sistema informático de servicio verifica si la contraseña de un solo uso generada coincide con la contraseña de un solo uso recibida o con la identificación derivada de la misma. Si no es ese el caso, entonces se interrumpe en el paso 24.

En el caso contrario, a continuación, en el paso 26, uno o más atributos se leen desde el token de ID del usuario, para en base a ello, en el paso 28, generar un conjunto de datos que contiene también la clave pública del elemento de seguridad, el cual ha sido puesto a disposición del usuario en el paso 10.

En el paso 30, ese conjunto de datos es firmado por el sistema informático de servicio, para generar de ese modo el software token. En el paso 32, el software token se transmite al usuario, a saber, mediante la primera y/o la segunda conexión.

La figura 4 muestra otra forma de realización de un procedimiento según la invención, mediante un diagrama UML.

El usuario, en su aparato electrónico 174, ingresa una petición para la clave pública del elemento de seguridad 172, la cual está almacenada en el área de memoria 188 que puede leerse libremente, del elemento de seguridad 172 (véase la figura 1). Esa petición "getPubKey()" (obtener clave pública) se transmite desde el aparato electrónico 174, mediante la conexión local 184, hacia el elemento de seguridad 172.

El elemento de seguridad 172 lee a continuación la clave pública del primer par de claves criptográfico asociado al mismo, desde el área de memoria 188, y envía esa clave pública pk_d, mediante la conexión local 184, hacia el aparato electrónico 174.

Entre el aparato electrónico 174 y el sistema informático de servicio 150, es decir, en este caso, el componente de programa 176, se establece la conexión 180 mediante la cual se transmite la petición para el software token, desde el aparato electrónico 174, hacia el componente de programa 176. Mediante esa conexión 180 asegurada de forma criptográfica se transmite también la clave pública leída previamente desde el elemento de seguridad 172, desde el aparato electrónico 174, hacia el componente de programa 176.

A continuación, el componente de programa 176 genera una contraseña de un solo uso OTP_i para esa petición recibida mediante la conexión 180. Esa OTP_i se transmite desde el componente de programa 176 hacia el componente de programa 178, y es registrada por ese componente de programa 178, es decir, es almacenada de forma temporal "registerSession (OTPi)" (sesión de registro).

Además, la OTP_i es cifrada por el componente de programa 176 con la ayuda de la clave pública pkd, de lo cual resulta el cifrado c. El cifrado c es firmado digitalmente además por el componente de programa 176. El cifrado c, así como su firma Sign(c), se transmiten al aparato electrónico 174 mediante la conexión 180 asegurada.

El aparato electrónico 174 verifica entonces la firma del cifrado c. Cuando la firma del cifrado c es válida, el aparato electrónico 174 dirige una petición para la decodificación del cifrado c al elemento de seguridad 172, es decir, la petición "decode (c)" (decodificar). El elemento de seguridad 172 descifra entonces c con la ayuda de la clave secreta almacenada en el área de memoria 186 protegida y envía el resultado de esa operación de descifrado, es decir OTP_i, mediante la conexión local 184, al aparato electrónico 174.

A continuación, el aparato electrónico 174 muestra la OTP_i en su unidad de visualización y dirige además una petición "getToken()" (obtener token) al componente de programa 176, para solicitar la generación del software token. El usuario puede leer la OTP_i desde la unidad de visualización del aparato electrónico 174 e ingresarla en el sistema informático del usuario 100.

En lugar de un ingreso manual, la OTP_i puede ser detectada de forma automática por la unidad de visualización del aparato electrónico 174, mediante el sistema informático del usuario 100. Por ejemplo, la OTP_i se muestra en la unidad de visualización del aparato electrónico 174 en forma de un patrón óptico legible por máquina, por ejemplo en forma de un código QR. Ese patrón óptico legible por máquina es registrado con la ayuda de una cámara digital del sistema informático del usuario 100, mediante el registro de una foto digital, y es decodificado de forma automática, para de ese modo ingresar la OTP_i en el sistema informático del usuario. La cámara digital puede estar conectada al sistema informático del usuario o puede ser un componente integral del sistema informático del usuario 100. Por ejemplo, el sistema informático del usuario 100 puede tratarse de un ordenador portátil con una cámara web integrada en la carcasa.

La OTP_i se transmite mediante la conexión 182 segura establecida entre el sistema informático del usuario 100 y el componente de programa 178. Por ejemplo, el componente de programa 178 genera una página web que se muestra en el sistema informático del usuario 100, y en la cual el usuario ingresa la OTP_i para efectuar un "Login" (inicio de sesión).

El componente de programa 178 compara a continuación la OTP_i almacenada previamente de forma temporal con la OTP_i recibida mediante la conexión 182, desde el sistema informático del usuario 100. Si se presenta una coincidencia, el componente de programa 178 dirige entonces una petición de autenticación "AuthnRequest/“(solicitud de autenticación) al sistema informático de proveedor de ID 136, la cual es conducida hacia el sistema informático de proveedor de ID 136 mediante la conexión 182, mediante un redireccionamiento del sistema informático del usuario 100. Esa petición de autenticación puede contener una especificación de atributo, la cual especifica aquellos atributos que tienen que ser leídos desde el token de ID 106, para ingresar en el software token. Lo mencionado puede tener lugar en forma de un objeto SAML.

El sistema informático de proveedor de ID dirige un comando para la lectura de los atributos especificados "get attributes ()" (obtener atributos) hacia el token de ID 106, y recibe esos atributos cuando el sistema informático de proveedor de ID 136 puede demostrar los derechos de lectura requeridos. Los atributos leídos por el sistema informático de proveedor de ID 136 se firman, y por ejemplo se transmiten al componente informático 178, por ejemplo en forma de un objeto SAML, mediante el sistema informático del usuario 100. El componente de programa 178 transfiere internamente en el sistema informático de servicio 150 los atributos así recibidos, hacia el componente de programa 176. El componente de programa 176 genera a continuación un conjunto de datos que contiene lo atributos recibidos, así como la clave pública del elemento de seguridad 172, leída desde el área de memoria 188, y los firma de forma digital. El resultado es el software token solicitado, el cual por ejemplo mediante la conexión 180, se transmite al aparato electrónico 174.

De manera correspondiente, para el elemento de seguridad 172 pueden generarse otros software token, los cuales respectivamente contienen diferentes atributos. Para ello puede procederse de manera que para cada uno de los software token se genere otro par de claves criptográfico, por ejemplo desde el aparato electrónico 174, en donde se cifra la clave secreta de otro par de claves de esa clase con la ayuda de la clave pública del elemento de seguridad 172, la cual ha sido leída desde la memoria 188, para almacenar el cifrado de la clave secreta, por ejemplo en un sistema de archivos del aparato electrónico 174. En el caso de la presencia de otro software token, tiene lugar entonces un descifrado de ese cifrado de la clave secreta mediante el elemento de seguridad 172, transmitiendo el cifrado mediante la conexión local 184, hacia el elemento de seguridad 172.

La figura 5 muestra un diagrama de bloques de otra forma de realización de un sistema de procesamiento de datos según la invención.

En la forma de realización que se considera en este caso, las instrucciones de programa 156 pueden contener los componentes de programa 176 y 178.

El aparato electrónico 174, en este caso, está diseñado como un aparato de telefonía móvil, en particular como un teléfono inteligente, y posee una interfaz de red 189 hacia una red de telefonía móvil 190 que, a modo de ejemplo, funciona según el estándar GSM o UMTS. El sistema informático de servicio 150 posee una interfaz de red 191 correspondiente hacia la red de telefonía móvil 190, de manera que la conexión 180 puede establecerse sobre toda la red de telefonía móvil 190.

El aparato electrónico 174 posee además un procesador 192 para ejecutar instrucciones de programa 193, así como una interfaz de usuario 194 que por ejemplo contiene una unidad de visualización y un teclado, o una pantalla táctil. El aparato electrónico 174 posee además una memoria electrónica 195, así como una interfaz 196 para el establecimiento de la conexión local 184 con el elemento de seguridad 172, el cual presenta una interfaz 197 correspondiente. El elemento de seguridad 172 posee además un procesador 198 para la ejecución de instrucciones de programa 199. Para utilizar el sistema informático de servicio 150, es decir, para generar el software token, se procede en correspondencia con las formas de realización según las figuras 1-4.

Por ejemplo, el usuario 102, mediante la interfaz del usuario 194 del aparato electrónico 174 ingresa una petición para generar el software token, después de lo cual en primer lugar la clave pública se lee desde el área de memoria 188 mediante la conexión local 184. Mediante la ejecución de las instrucciones de programa 193, entonces, la "TokenRequest" (solicitud de token), junto con esa clave pública, se transmite al componente de programa 176 mediante la conexión 180; dicho componente genera a continuación la OTP_i, la cifra con la clave pública y envía el cifrado c firmado mediante la conexión 180, hacia el aparato electrónico 174.

Mediante la ejecución de las instrucciones de programa 193 se verifica la firma de c y después se envía la orden "decode(c)" (decodificar c) mediante la conexión local 184, hacia el elemento de seguridad 172. Éste responde con la OTP_i descifrada, la cual se muestra entonces en la interfaz del usuario 194, mediante la ejecución de las instrucciones de programa 193.

El usuario 102 puede entonces consultar la página web del componente de programa 178, para lo cual se establece la conexión 182 mediante la red 116, entre el componente de programa 178 y el sistema informático del usuario 100. El usuario 102 lee la OTP_i desde la unidad de visualización de la interfaz del usuario 194 e ingresa esa OTP_i, mediante el teclado del sistema informático del usuario 100, en la página web del componente de programa 178. Si la OPT_i generada y la OTP_i recibida de este modo coinciden, el componente de programa 178 genera la solicitud de autenticación "AuthnRequest" (véase la figura 4). En la forma de realización considerada en este caso, esto da inicio a la siguiente secuencia de pasos, para leer al menos un atributo desde el token de ID 106:

1. Autenticación del usuario 102 con respecto al token de ID 106.

El usuario 102 debe autenticarse con respecto al token de ID 106. En el caso de una implementación con PIN el usuario 102 ingresa para ello su PIN, por ejemplo mediante el sistema informático del usuario 100 o mediante un terminal de tarjeta inteligente conectado al mismo. Mediante la ejecución de las instrucciones de programa 130, el token de ID 106 verifica entonces la corrección del PIN ingresado. Si el PIN ingresado coincide con el valor de referencia del PIN almacenado en el área de memoria 120 protegida, entonces el usuario 102 se valida como autenticado. Puede procederse de forma análoga cuando para la autentificación se utiliza una característica biométrica del usuario 102, del modo antes descrito.

2. Autenticación del sistema informático de proveedor de ID 136 con respecto al token de ID 106.

Para ello se establece una tercera conexión entre el token de ID 106 y el sistema informático de proveedor de ID 136, mediante el sistema informático del usuario 100 y la red 116. Por ejemplo, el sistema informático de proveedor de ID 136 transmite su certificado 144 mediante esa tercera conexión, hacia el token de ID 106. Mediante las instrucciones de programa 134 se genera entonces un así llamado desafío, es decir un número aleatorio. Ese número aleatorio se cifra con la clave pública del sistema informático de proveedor de ID 136, contenida en el certificado 144. El cifrado resultante es enviado por el token de ID 106, mediante la tercera conexión, hacia el sistema informático de proveedor de ID 136. El sistema informático de proveedor de ID 136 descifra el cifrado con la ayuda de su clave privada 142, obteniendo así el número aleatorio. El sistema informático de proveedor de ID 136, mediante la tercera conexión, retransmite el número aleatorio hacia el token de ID 106. Mediante la ejecución de las instrucciones de programa 134 se verifica allí si el número aleatorio recibido por el sistema informático de proveedor de ID 136 coincide con el número aleatorio generado originalmente, es decir, el desafío. Si es ese el caso, entonces el sistema informático de proveedor de ID 136 se valida como autenticado con respecto al token de ID 106. El número aleatorio puede utilizarse como clave simétrica para el cifrado de extremo a extremo.

3. Después de que el usuario 102 se ha autenticado de forma exitosa con respecto al token de ID 106, y después de que el sistema informático de proveedor de ID 136 se ha autenticado de forma exitosa con respecto al token de ID 106, el sistema informático de proveedor de ID 136 obtiene una autorización de lectura para la lectura de uno, de varios o de todos los atributos almacenados en el área de memoria 124 protegida. El alcance de los derechos de lectura puede estar especificado en el certificado 144 del sistema informático de proveedor de ID 136. Debido a un comando de lectura correspondiente que envía el sistema informático de proveedor de ID 136, mediante la tercera conexión, al token de ID 106, los atributos solicitados se leen desde el área de memoria 124 protegida y se cifran ejecutando las instrucciones de programa 132. Los atributos cifrados se transmiten al sistema informático de proveedor de ID 136 mediante la tercera conexión, y allí se descifran mediante la ejecución de las instrucciones de programa 148. Debido a esto, el sistema informático de proveedor de ID 136 tiene conocimiento de los atributos leídos desde el token de ID 106.

Esos atributos son firmados por el sistema informático de proveedor de ID con la ayuda de su certificado 144 y, mediante el sistema informático del usuario 100 o de forma directa, se transmiten al sistema informático de servicio 150. Gracias a esto se informa al sistema informático de servicio 150 sobre los atributos leídos desde el token de ID 106, de manera que el sistema informático de servicio 150, con la ayuda de esos atributos, puede generar el software token.

Mediante la necesidad de la autenticación del usuario 102 con respecto al token de ID 106, y mediante la autenticación del sistema informático de proveedor de ID 136 con respecto al token de ID 106, se proporciona el ancla de confianza necesario, de manera que el sistema informático de servicio 150 puede estar seguro de que los atributos del usuario 102, que le fueron comunicados desde el sistema informático de proveedor de ID 136, son correctos y no están falsificados.

Dependiendo de la forma de realización, el orden de la autenticación puede ser diferente. Por ejemplo, puede preverse que primero el usuario 102 deba autenticarse con respecto al token de ID 106 y a continuación deba autenticarse el sistema informático de proveedor de ID 136. Sin embargo, en principio también es posible que primero deba autenticarse el sistema informático de proveedor de ID 136 con respecto al token de ID 106, y sólo a continuación deba autenticarse el usuario 102.

En el primer caso, el token de ID 106 por ejemplo está configurado de manera que el mismo sólo se habilita mediante el ingreso de un PIN correcto o de una característica biométrica correcta, mediante el usuario 102. Sólo esa habilitación permite el inicio de las instrucciones de programa 132 y 134 y, con ello, la autenticación del sistema informático de proveedor de ID 136.

En el segundo caso ya es posible también un inicio de las instrucciones de programa 132 y 134 cuando el usuario 102 aún no se ha autenticado con respecto al token de ID 106. En ese caso, por ejemplo, las instrucciones de programa 134 están configuradas de manera que el sistema informático de proveedor de ID 136 sólo puede realizar un acceso de lectura al área de memoria 124 protegida, para la lectura de uno o de varios de los atributos, después de que ha sido señalizada la autenticación exitosa también del usuario 102, desde las instrucciones de programa 130.

Se considera especialmente ventajosa la utilización del token de ID 106 por ejemplo para aplicaciones E-Commerce y E-Government, a saber, de forma continua y con seguridad jurídica, debido al ancla de confianza formada por la necesidad de la autenticación del usuario 102 y del sistema informático de proveedor de ID 136 con respecto al token de ID 106. Además, se considera especialmente ventajoso el hecho de que no se requiere una memoria central de los atributos de diferentes usuarios 102, de modo que con ello se solucionan los problemas de protección de datos, presentes en el estado de la técnica. En lo que respecta a la comodidad de la aplicación del procedimiento, se considera especialmente ventajoso el hecho de que no se requiere un registro previo del usuario 102 para la utilización del sistema informático de proveedor de ID 136.

La figura 6 muestra un procedimiento correspondiente para la lectura de al menos un atributo. En el paso 200, una petición de servicio para generar el software token se envía desde el sistema informático del usuario hacia el sistema informático de servicio. Por ejemplo, el usuario pone en funcionamiento un navegador de Internet del sistema informático del usuario e ingresa una URL para solicitar una página web del sistema informático de servicio. En la página web solicitada el usuario ingresa entonces su petición de servicio, en la cual puede especificar los atributos que deben leerse. La especificación de atributo también puede estar predeterminada de forma fija.

En el paso 204, la especificación de atributo se transmite desde el sistema informático de servicio hacia el sistema informático de proveedor de ID, a saber, de forma directa o mediante el sistema informático del usuario.

Para brindar al sistema informático de proveedor de ID la posibilidad de leer atributos desde su token de ID, el usuario se autentica en el paso 206 con respecto al token de ID.

En el paso 208 se establece una conexión entre el token de ID y el sistema informático de proveedor de ID. En este caso, la misma se trata preferentemente de una conexión asegurada, por ejemplo según un así llamado procedimiento de mensajería segura.

En el paso 210 tiene lugar al menos una autenticación del sistema informático de proveedor de ID con respecto al token de ID, mediante la conexión establecida en el paso 208. De manera adicional puede preverse también una autenticación del token de ID con respecto al sistema informático de proveedor de ID.

Después de que tanto el usuario, como también el sistema informático de proveedor de ID, han sido autenticados de forma exitosa con respecto al token de ID, el sistema informático de proveedor de ID obtiene desde el token de ID la autorización de acceso para la lectura de los atributos. En el paso 212, el sistema informático de proveedor de ID envía uno o varios comandos de lectura para leer desde el token de ID los atributos requeridos según la especificación de atributo. Los atributos se transmiten mediante cifrado de extremo a extremo, mediante la conexión asegurada, hacia el sistema informático de proveedor de ID y allí se descifran.

Los valores de atributo leídos, en el paso 214, son firmados por el sistema informático de proveedor de ID. En el paso 216, el sistema informático de proveedor de ID envía los valores de atributo firmados, mediante la red. Los valores de atributo firmados alcanzan el sistema informático de servicio de forma directa o mediante el sistema informático del usuario. En el último caso, el usuario puede tener la posibilidad de tener conocimiento de los valores de atributo firmados y/o de complementarlos mediante otros datos. Puede preverse que los valores de atributo firmados eventualmente se retransmitan con los datos completados sólo después de la habilitación mediante el usuario, desde el sistema informático del usuario, hacia el sistema informático de servicio. Gracias a esto se logra la mayor transparencia posible para el usuario en cuanto a los atributos enviados desde el sistema informático de proveedor de ID, hacia el sistema informático de servicio.

El software token, por ejemplo, puede estar almacenado en la memoria 195 del aparato electrónico 174 y/o en el área de memoria 188 del elemento de seguridad 172.

Para la autenticación del usuario 102, por ejemplo para aplicaciones E-Government, E-Commerce o M-Commerce, o con el fin de un control de acceso, por ejemplo a un edificio, el usuario 102 puede ahora utilizar el elemento de seguridad 172 en combinación con el software token, en donde debido a la formación criptográfica del software token al elemento de seguridad 172 se proporciona un nivel de seguridad particularmente alto.

La figura 7 muestra otra forma de realización de la invención que es análoga a la forma de realización según la figura 4, en donde aquí la realización del procedimiento comienza con la ayuda del sistema informático del usuario 100. En el paso 1, con la ayuda del sistema informático del usuario 100, en el sistema informático de servicio 150, es decir, en este caso, en el componente de programa 178, se ingresa una petición para generar el software token; es decir, primero para generar una contraseña de un solo uso, para establecer la sesión requerida para ello. En la figura 7 esto se indica con la referencia "getOTP()" (obtener OTP). El ingreso de la petición al sistema informático de servicio 150, por ejemplo, puede tener lugar de manera que con la ayuda del sistema informático del usuario 100 se solicita una página web del sistema informático de servicio 150, en la cual la petición correspondiente del usuario se ingresa mediante el navegador del sistema informático del usuario 100. Por ejemplo, para ello se establece en primer lugar la primera conexión 180 asegurada de forma criptográfica, y en la forma de realización considerada en este caso, a saber, entre el sistema informático del usuario 100 y el sistema informático de servicio 150, para transmitir getOTP(), mediante esa conexión 180.

En el paso 2, el sistema informático de servicio 150 genera la contraseña de un solo uso OTP_i solicitada. El generador de contraseñas de un solo uso correspondiente puede estar contenido aquí en el componente de programa 178. A continuación, en el paso 3, la OTP_i se almacena como identificador de la primera conexión 180 asegurada de forma criptográfica establecida entre el sistema informático del usuario 100 y el sistema informático de servicio 150, es decir que la OTP_i se registra para establecer una sesión. En el paso 4, la OTP_i se transmite entonces mediante la primera conexión 180 asegurada de forma criptográfica, desde el sistema informático de servicio 150 hacia el sistema informático del usuario 100, por ejemplo en forma de un código QR.

Debido a la recepción del código QR, el mismo se muestra en la unidad de visualización del sistema informático del usuario 100. El usuario puede entonces utilizar su aparato electrónico 174 para registrar de forma automática el código QR mostrado en la unidad de visualización del sistema informático del usuario 100. Para ello puede utilizarse un escáner óptico integrado en el aparato electrónico 174, o una cámara digital. De manera especialmente preferente, el aparato electrónico 174 se trata en este caso de un teléfono móvil, en particular un teléfono inteligente, con una así llamada cámara digital, es decir, un así llamado móvil fotográfico. En este caso, el usuario puede fotografiar con su móvil fotográfico el código QR mostrado en la unidad de visualización del sistema informático del usuario 100.

El código QR registrado de forma óptica con la ayuda del aparato electrónico 174 se decodifica entonces mediante la ejecución de un módulo de programa correspondiente, mediante el aparato electrónico 174, para de ese modo ingresar la OTP_i en el aparato electrónico 174 (paso 5).

En el paso 6, el aparato electrónico 174 solicita la clave pública desde el elemento de seguridad 172, y en el paso 7 obtiene esa clave pública, de forma análoga a los dos primeros pasos mostrados en la figura 4. Además, la OTP_i se transmite desde el aparato electrónico 174 hacia el elemento de seguridad 172. El elemento de seguridad 172 genera una firma s de la OTP_i, y transfiere esa firma s al aparato electrónico 174.

En el paso 8 se establece la segunda conexión 182 asegurada de forma criptográfica entre el aparato electrónico 174 y el sistema informático de servicio 150. En el paso 8, además, desde el aparato electrónico 174, hacia el sistema informático de servicio 150, es decir, en este caso, el primer componente de programa 176, se envía una señal mediante la conexión 182, para transmitir un comando getToken (OTP_i, pkd,s).

Con esa señal se solicita la generación del software token, en donde junto con esa petición se transmiten la OTP_i, la clave pública del elemento de seguridad 172 pkd, así como la firma s.

En el paso 9, mediante el componente de programa 176, la firma s se verifica con la ayuda de la clave pública pkd. En el caso de que la verificación sea exitosa, en el paso 10 la OTP_i, y preferentemente también la clave pública pkd, se transmite desde el componente de programa 176 hacia el componente de programa 178, y el componente de

programa 178 la compara con la OTP_i registrada. Además, la clave pública pkd se almacena en el sistema informático de servicio 150, es decir, por ejemplo por el componente de programa 178, para a continuación poder utilizarse en el paso 21 para generar el software token. Por ejemplo, el almacenamiento de la clave pública pkd tiene lugar con la OTP_i como identificador, para asociar la clave pública pkd a la sesión.

En el caso de la coincidencia de la OTP_i recibida mediante la segunda conexión, desde el aparato electrónico 174 hacia el sistema informático de servicio 150 e ingresada en el paso 10 en el componente de programa 178, con la OTP_i previamente registrada, la sesión ha sido establecida con éxito y puede realizarse el siguiente acceso de lectura al token de ID 106. Para ello puede ser necesario que el usuario, en el paso 12, ingrese una confirmación correspondiente en el sistema informático de servicio 150. Los pasos 13 a 18 subsiguientes son análogos a los pasos correspondientes de la figura 4.

En el paso 19, los atributos provenientes de la respuesta del sistema informático de proveedor de ID 136 son leídos por el componente de programa 178 y en el paso 20 se transfieren al componente de programa 176. El componente de programa 176, con la ayuda de esos atributos y de la clave pública pkd recibida en el paso 8, genera entonces el software token, y en el paso 22 transmite el software token, por ejemplo mediante la segunda conexión, al aparato electrónico 174. En los pasos 23 y 24 tiene lugar un aviso del sistema informático del usuario 100 con respecto a la generación exitosa del software token.

Lista de símbolos de referencia

100 Sistema informático del usuario

102 Usuario

104 Interfaz

106 Token de ID

108 Interfaz

110 Procesador

112 Instrucciones del programa

114 Interfaz de red

116 Red

118 Memoria electrónica

120 Área de memoria protegida

122 Área de memoria protegida

124 Área de memoria protegida

126 Área de memoria

128 Procesador

130 Instrucciones del programa

132 Instrucciones del programa

134 Instrucciones del programa

136 Sistema informático proveedor de ID

138 Interfaz de red

140 Memoria

142 Clave privada

144 Certificado

145 Procesador

146 Instrucciones del programa

148 Instrucciones del programa

149 Instrucciones del programa

150 Sistema informático de servicio

152 Interfaz de red

154 Procesador

156 Instrucciones del programa

172 Elemento de seguridad

174 Aparato electrónico

176 Primer componente de programa

178 Segundo componente de programa

180 Primera conexión asegurada de forma criptográfica

182 Segunda conexión asegurada de forma criptográfica

184 Conexión local

185 Conexión local

186 Área de memoria protegida

188 Área de memoria que puede leerse libremente

189 Interfaz de red

190 Red de telefonía móvil

191 Interfaz de red

192 Procesador

193 Instrucciones del programa

194 Interfaz del usuario

195 Memoria

196 Interfaz

197 Interfaz

198 Procesador

199 Instrucciones del programa

REIVINDICACIONES

1. Procedimiento para generar un software token con los siguientes pasos:

- puesta a disposición de un elemento de seguridad (172), en donde el elemento de seguridad se trata de un aparato de un usuario, en donde en un área de memoria protegida (186) del elemento de seguridad está almacenada una clave secreta de un primer par de claves criptográfico asimétrico,

- establecimiento de una conexión (180) asegurada de forma criptográfica entre un aparato electrónico (174; 100) del usuario y un sistema informático de servicio (150),

- transmisión de una petición para generar el software token, desde el aparato electrónico hacia el sistema informático de servicio, mediante la primera conexión,

- generación de una contraseña de un solo uso debido a la recepción de la petición mediante el sistema informático de servicio,

- registro de la contraseña de un solo uso como identificador de la primera conexión mediante el sistema informático de servicio,

- transmisión de la contraseña de un solo uso, desde el sistema informático de servicio hacia el aparato electrónico, mediante la primera conexión,

- emisión de la contraseña de un solo uso mediante una interfaz del usuario (194) del aparato electrónico,

- establecimiento de una segunda conexión (182) asegurada de forma criptográfica entre un sistema informático del usuario (100; 174) y el sistema informático de servicio,

- ingreso de la contraseña de un solo uso en el sistema informático del usuario,

- transmisión de la contraseña de un solo uso ingresada, desde el sistema informático del usuario hacia el sistema informático de servicio, mediante la segunda conexión,

- verificación mediante el sistema informático de servicio, de si la contraseña de un solo uso registrada coincide con la contraseña de un solo uso recibida mediante la segunda conexión, y sólo si es ese el caso, lectura de al menos un atributo almacenado en un token de ID (106) del usuario, generación del software token que está vinculado al elemento de seguridad (172) mediante la firma de al menos un atributo y de la clave pública del primer par de claves criptográfico mediante el sistema informático de servicio, transmisión del software token mediante el sistema informático de servicio, mediante la primera conexión, hacia el aparato electrónico, y/o transmisión del software token, mediante la segunda conexión, hacia el sistema informático del usuario.

2. Procedimiento según la reivindicación 1, en donde en un área de memoria (188), que puede leerse libremente, del elemento de seguridad, está almacenada una clave pública del primer par de claves, con los siguientes pasos adicionales:

- transmisión de la clave pública, desde el elemento de seguridad hacia el aparato electrónico, mediante una conexión local (184),

- transmisión de la clave pública, desde el aparato electrónico hacia el sistema informático de servicio, mediante la primera conexión asegurada de forma criptográfica,

- cifrado de la contraseña de un solo uso mediante el sistema informático de servicio con la clave pública, en donde la contraseña de un solo uso cifrada, mediante la primera conexión, se transmite desde el sistema informático de servicio, hacia el aparato electrónico,

- transmisión de la contraseña de un solo uso cifrada, desde el aparato electrónico, hacia el elemento de seguridad, mediante la conexión local,

- descifrado de la contraseña de un solo uso mediante el elemento de seguridad con la clave secreta del primer par de claves,

- transmisión de la contraseña de un solo uso descifrada, desde el elemento de seguridad hacia el aparato electrónico, mediante la conexión local, para la emisión mediante el aparato electrónico.

3. Procedimiento según la reivindicación 1 ó 2, en donde el sistema informático de servicio presenta un primer componente del programa (176) para generar la contraseña de un solo uso, para el cifrado de la contraseña de un solo uso y para generar el software token, así como un segundo componente de programa (178) para la recepción de la contraseña de un solo uso por el sistema informático del usuario, en donde la primera conexión se encuentra

establecida entre el aparato electrónico y el primer componente de programa, y la segunda conexión entre el sistema informático del usuario y el segundo componente de programa, con los siguientes pasos adicionales:

- transmisión de la contraseña de un solo uso desde el primer componente de programa hacia el segundo componente de programa, en donde el segundo componente de programa efectúa la verificación de si la contraseña de un solo uso recibida por el primer componente coincide con la contraseña de un solo uso recibida por el sistema informático del usuario mediante la segunda conexión,

- recepción de al menos un atributo leído desde el token de ID, mediante el segundo componente de programa,

- transmisión de al menos un atributo desde el segundo componente de programa hacia el primer componente de programa.

4. Procedimiento según la reivindicación 1, 2 ó 3, en donde el aparato electrónico se trata de un terminal móvil.

5. Procedimiento según la reivindicación 1, 2 ó 3, en donde el sistema informático del usuario cumple con la función del sistema informático del usuario.

6. Procedimiento según una de las reivindicaciones precedentes, en donde para la lectura de al menos un atributo desde el token de ID se realizan los siguientes pasos adicionales:

- autenticación del usuario (102) con respecto al token de ID,

- autenticación de un sistema informático de proveedor de ID (136) con respecto al token de ID,

- después de finalizada con éxito la autenticación del usuario y del sistema informático de proveedor de ID con respecto al token de ID, acceso de lectura del sistema informático de proveedor de ID a por lo menos un atributo almacenado en el token de ID, mediante la tercera conexión, transmisión de al menos un atributo desde el sistema informático de proveedor de ID hacia el sistema informático de servicio, en donde la tercera conexión se establece entre el token de ID y el sistema informático de proveedor de ID, mediante el sistema informático del usuario, con cifrado de extremo a extremo.

7. Procedimiento según la reivindicación 6, en donde al menos un atributo es firmado por el sistema informático de proveedor de ID, y mediante el sistema informático del usuario se transmite al sistema informático de servicio.

8. Procedimiento según la reivindicación 7, en donde el sistema informático de proveedor de ID transmite al menos un atributo, en forma de un objeto SAML, hacia el sistema informático de servicio.

9. Procedimiento según una de las reivindicaciones precedentes, en donde el software token es generado por el sistema informático de servicio mediante una firma digital ciega o como un U-prove-token.

10. Procedimiento según una de las reivindicaciones precedentes, en donde al software token está asociado un segundo par de claves criptográfico asimétrico, en donde la clave secreta del segundo par de claves, con la clave pública del primer par de claves, de manera cifrada, está almacenada en una memoria (195) del aparato electrónico.

11. Procedimiento según una de las reivindicaciones precedentes, en donde el token de ID se trata de un documento con una memoria electrónica (118) integrada en el cuerpo del documento, en donde en la memoria electrónica está almacenado al menos un atributo.

12. Procedimiento según una de las reivindicaciones precedentes, en donde el aparato electrónico (100) está diseñado como sistema informático, y en donde el sistema informático del usuario está diseñado como ordenador móvil (174), en donde en un área de memoria (188), que puede leerse libremente, del elemento de seguridad, está almacenada una clave pública del primer par de claves, con los siguientes pasos adicionales:

- transmisión de la clave pública, desde el elemento de seguridad hacia el ordenador móvil (174), mediante una conexión local (184),

- transmisión de la clave pública y de la contraseña de un solo uso ingresada, desde el ordenador móvil (174) hacia el sistema informático de servicio, mediante la segunda conexión asegurada de forma criptográfica.

13. Procedimiento según una de las reivindicaciones precedentes, en donde la emisión de la contraseña de un solo uso tiene lugar mediante la visualización de un patrón óptico legible por máquina en una unidad de visualización, y en donde el ingreso de la contraseña de un solo uso tiene lugar mediante la detección automática del patrón óptico.

14. Producto de programa informático con instrucciones de programa ejecutables para ejecutar un procedimiento según una de las reivindicaciones precedentes.

15. Sistema informático de servicio para generar un software token vinculado a un elemento de seguridad (172), con:

- medios (154, 176, 191) para establecer una primera conexión (180) asegurada de forma criptográfica hacia un aparato electrónico (174),

- medios (154, 176, 191) para la recepción de una petición para generar el software token por el aparato electrónico de un usuario, mediante la primera conexión,

- medios (154, 176) para generar una contraseña de un solo uso debido a la recepción de la petición,

- medios (154, 176, 191) para la transmisión de la contraseña de un solo uso, mediante la primera conexión, hacia el aparato electrónico,

- medios (152, 154, 178) para establecer una segunda conexión (182) asegurada de forma criptográfica hacia un sistema informático del usuario (100) del usuario,

- medios (152, 154, 178) para la recepción de la contraseña de un solo uso por el sistema informático del usuario, mediante la segunda conexión,

- medios (154, 178) para verificar si la contraseña de un solo uso generada coincide con la contraseña de un solo uso recibida,

- medios (152, 154, 176, 178, 191) para generar el software token que está vinculado al elemento de seguridad (172), mediante la firma de al menos uno atributo leído desde un token de ID del usuario y de una clave pública asociada al elemento de seguridad del usuario, así como para la transmisión del software token mediante la primera conexión, hacia el aparato electrónico y/o mediante la segunda conexión, hacia el sistema informático de usuario, con la condición previa de que la verificación haya dado como resultado una coincidencia de la contraseña de un solo uso generada y de la recibida.

16. Sistema de procesamiento de datos con un sistema informático de servicio (150) según la reivindicación 15 y con un sistema informático de proveedor de ID (136), en donde el sistema informático de proveedor de ID presenta

- medios (138) para la recepción de una especificación de atributo por el sistema informático de servicio, en donde la especificación de atributo especifica al menos un atributo,

- medios (142, 144, 145, 146) para la autenticación con respecto al token de ID,

- medios (138, 145, 148) para la lectura de al menos un atributo desde el token de ID mediante una conexión protegida con cifrado de extremo a extremo,

en donde la lectura de al menos un atributo presupone que se han autenticado un usuario asociado al token de ID y el sistema informático de proveedor de ID con respecto al token de ID.

17. Sistema de procesamiento de datos según la reivindicación 16, con el elemento de seguridad, en donde el elemento de seguridad se trata de un aparato, en donde el elemento de seguridad presenta un área de memoria protegida (186), en la cual está almacenada una clave secreta del primer par de claves.

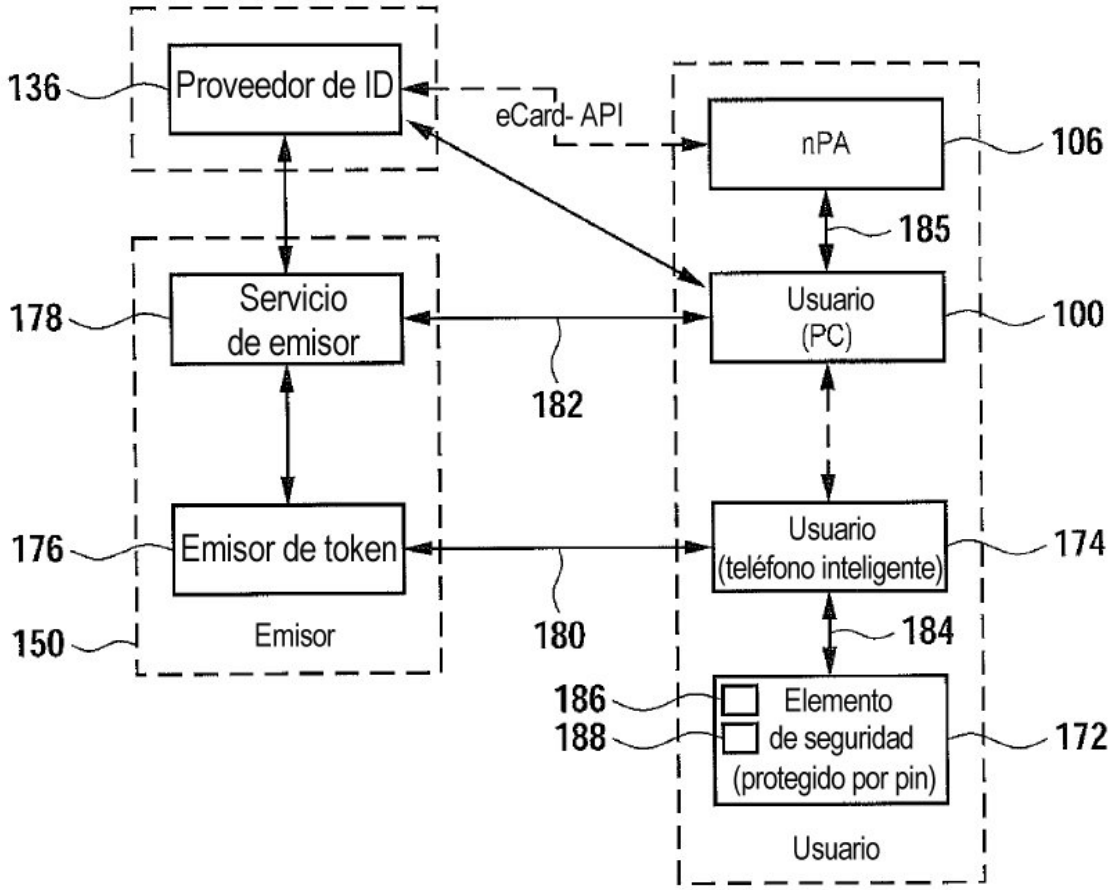

136
Proveedor de ID
eCard- API
nPA
106
185
178
Servicio
de emisor
Usuario
(PC)
100
182
176
Emisor de token
Usuario
(teléfono inteligente)
174
150
Emisor
180
184
186
188
Elemento
de seguridad
(protegido por pin)
172
Usuario

Fig. 1

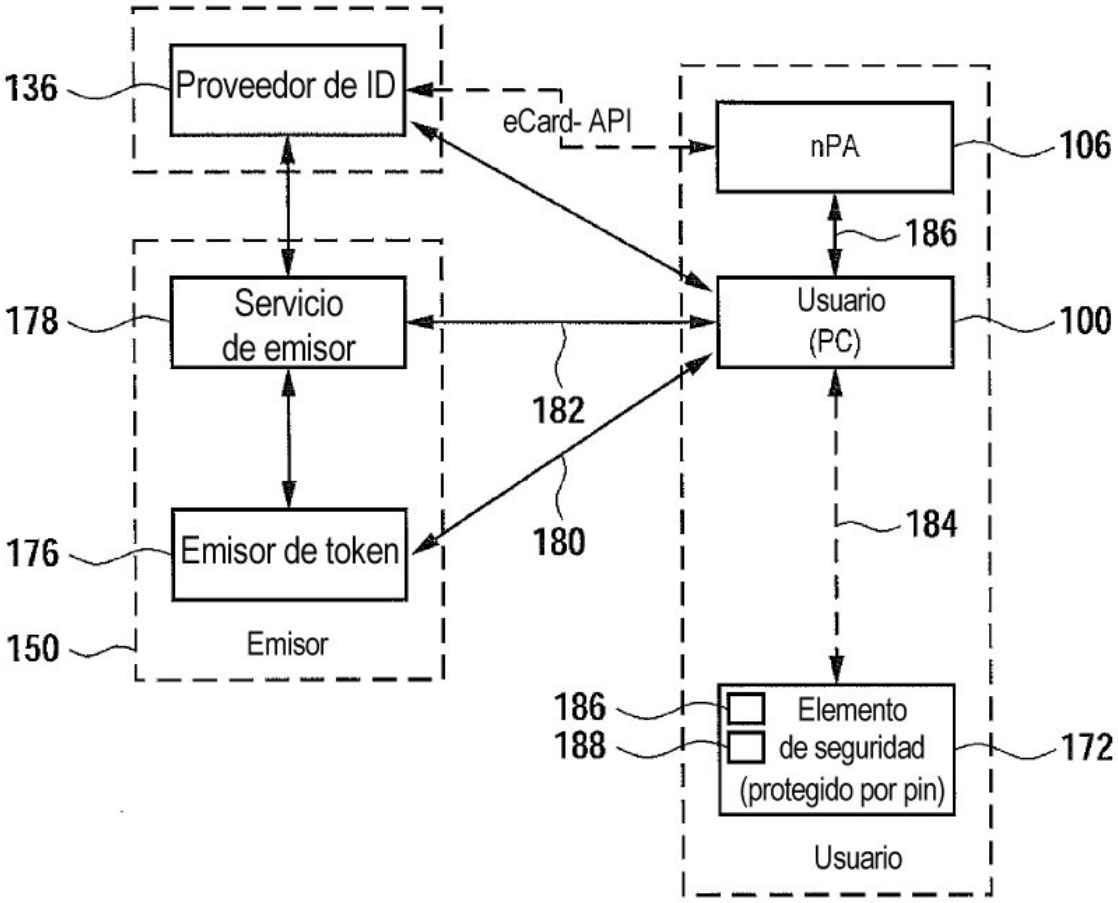

136
Proveedor de ID
eCard- API
nPA
106
186
178
Servicio
de emisor
Usuario
(PC)
100
182
184
176
Emisor de token
180
150
Emisor
186
188
Elemento
de seguridad
(protegido por pin)
172
Usuario

Fig. 2

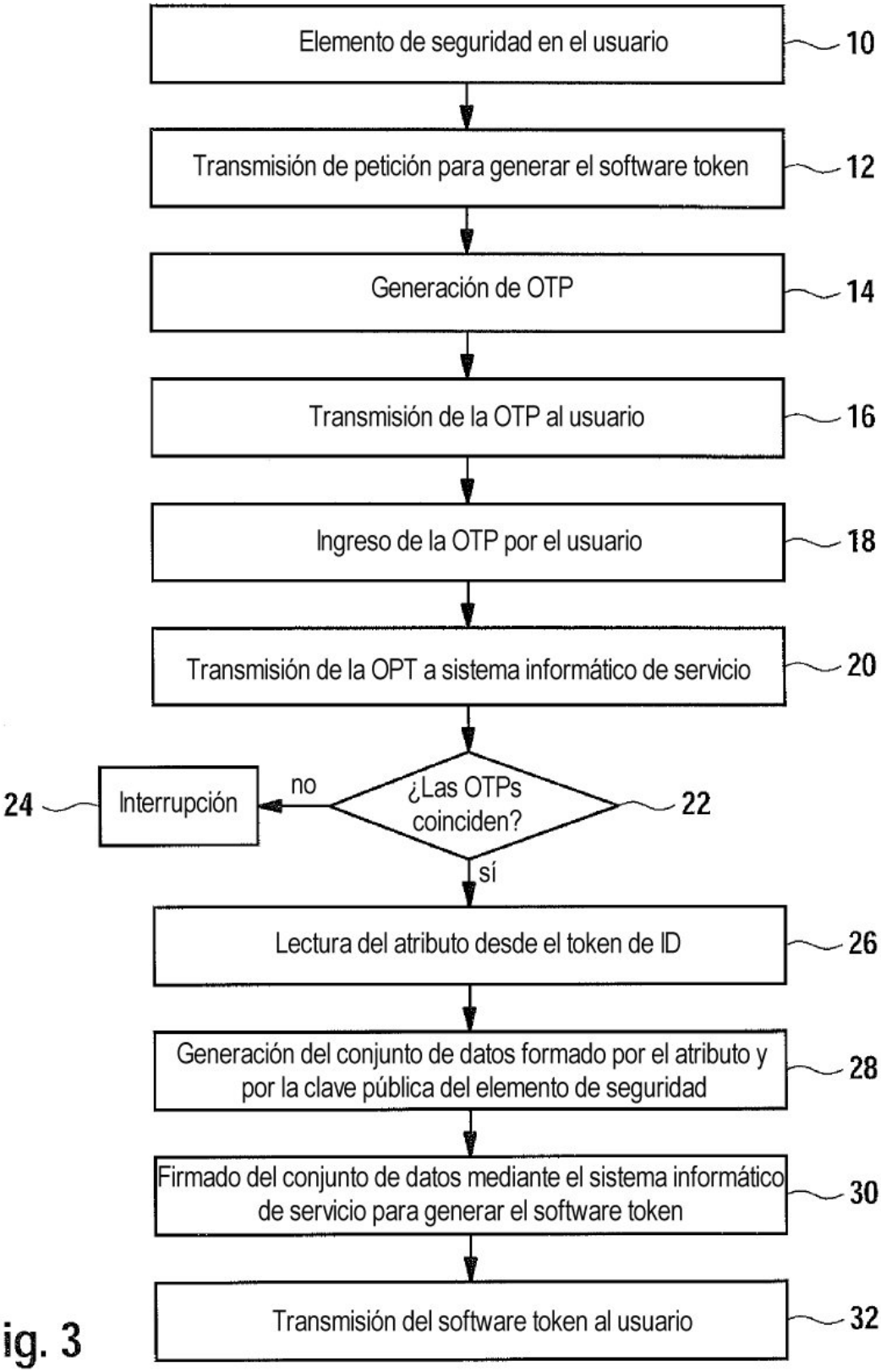

Elemento de seguridad en el usuario
10
Transmisión de petición para generar el software token
12
Generación de OTP
14
Transmisión de la OTP al usuario
16
Ingreso de la OTP por el usuario
18
Transmisión de la OPT a sistema informático de servicio
20
¿Las OTPs coinciden?
22
no
24
Interrupción
sí
Lectura del atributo desde el token de ID
26
Generación del conjunto de datos formado por el atributo y por la clave pública del elemento de seguridad
28
Firmado del conjunto de datos mediante el sistema informático de servicio para generar el software token
30
Transmisión del software token al usuario
32

Fig. 3

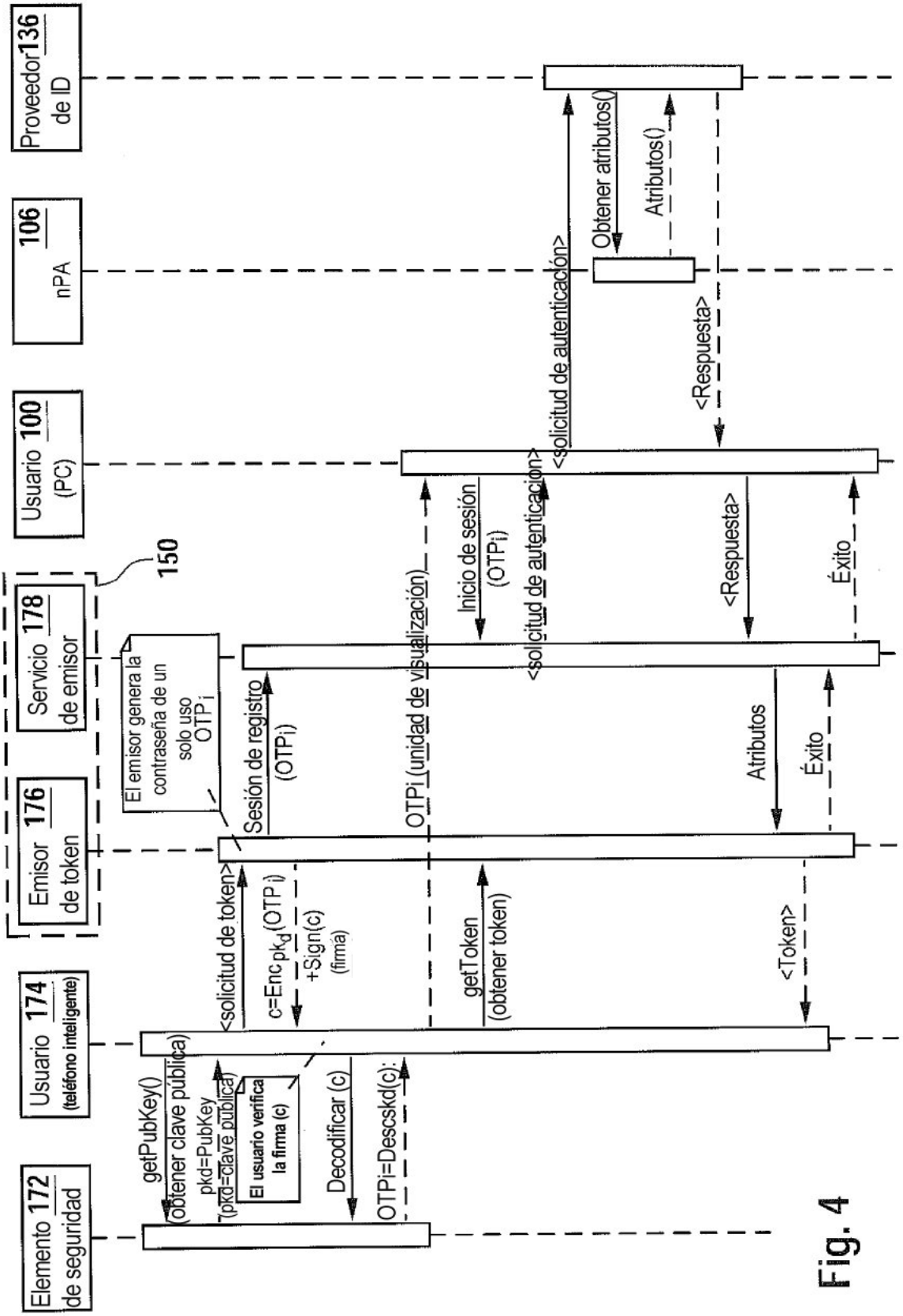

Proveedor 136 de ID
106 nPA
Usuario 100 (PC)
150
Servicio 178 de emisor
Emisor 176 de token
Usuario 174 (teléfono inteligente)
Elemento 172 de seguridad
Obtener atributos()
Atributos()
<solicitud de autenticación>
<Respuesta>
Inicio de sesión (OTPi)
<solicitud de autenticación>
<Respuesta>
Éxito
El emisor genera la contraseña de un solo uso OTPi
Sesión de registro (OTPi)
OTPi (unidad de visualización)
Atributos
Éxito
<solicitud de token>
c=Enc pkd(OTPi)
+Sign(c) (firma)
getToken (obtener token)
<Token>
getPubKey() (obtener clave pública)
pkd=PubKey (pkd=clave pública)
El usuario verifica la firma (c)
Decodificar (c)
OTPi=Descskd(c):

Fig. 4

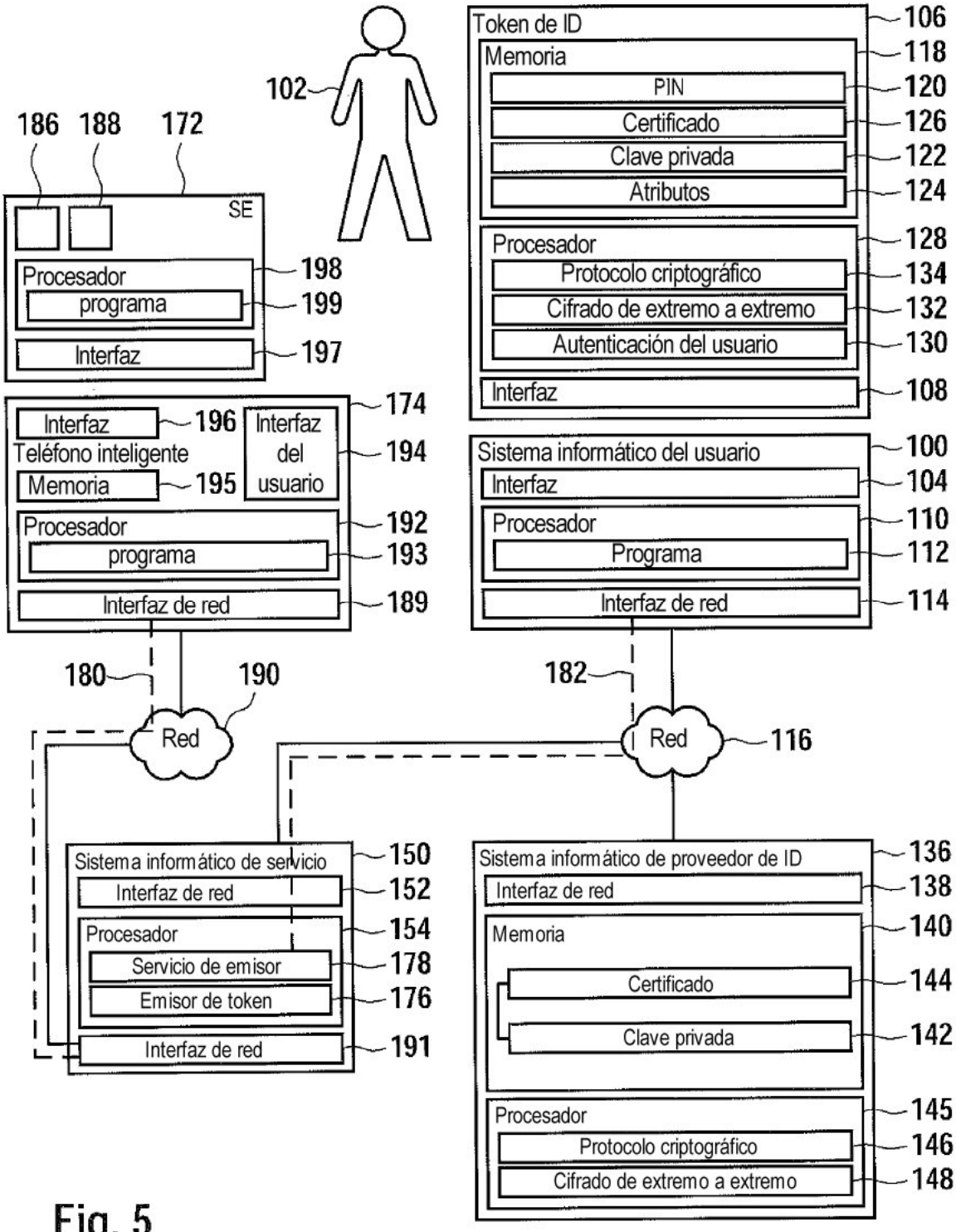

102
186
188
172
SE
Procesador
programa
198
199
Interfaz
197
Token de ID
106
Memoria
118
PIN
120
Certificado
126
Clave privada
122
Atributos
124
Procesador
128
Protocolo criptográfico
134
Cifrado de extremo a extremo
132
Autenticación del usuario
130
Interfaz
108
Interfaz
196
Teléfono inteligente
Memoria
195
Interfaz del usuario
174
194
Procesador
programa
192
193
Interfaz de red
189
Sistema informático del usuario
100
Interfaz
104
Procesador
Programa
110
112
Interfaz de red
114
180
190
182
Red
Red
116
Sistema informático de servicio
150
Interfaz de red
152
Procesador
154
Servicio de emisor
178
Emisor de token
176
Interfaz de red
191
Sistema informático de proveedor de ID
136
Interfaz de red
138
Memoria
140
Certificado
144
Clave privada
142
Procesador
145
Protocolo criptográfico
146
Cifrado de extremo a extremo
148

Fig. 5

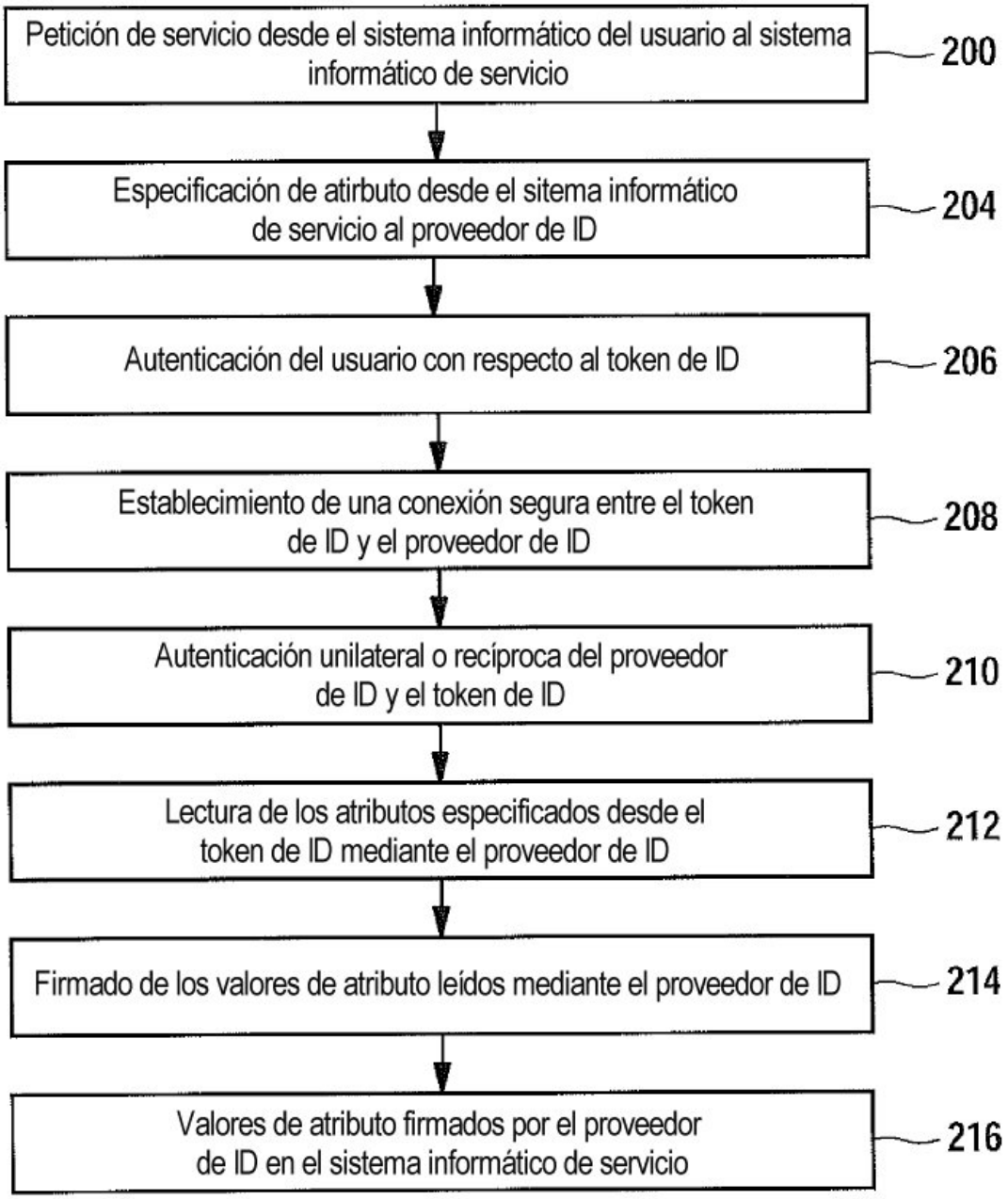

Petición de servicio desde el sistema informático del usuario al sistema informático de servicio
200
Especificación de atirbuto desde el sitema informático de servicio al proveedor de ID
204
Autenticación del usuario con respecto al token de ID
206
Establecimiento de una conexión segura entre el token de ID y el proveedor de ID
208
Autenticación unilateral o recíproca del proveedor de ID y el token de ID
210
Lectura de los atributos especificados desde el token de ID mediante el proveedor de ID
212
Firmado de los valores de atributo leídos mediante el proveedor de ID
214
Valores de atributo firmados por el proveedor de ID en el sistema informático de servicio
216

Fig. 6

Fig. 7

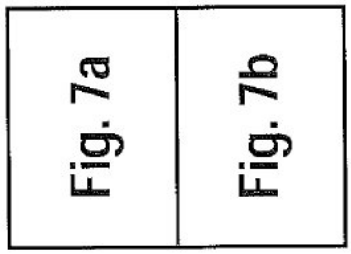


Fig. 7a
Fig. 7b

Fig. 7a

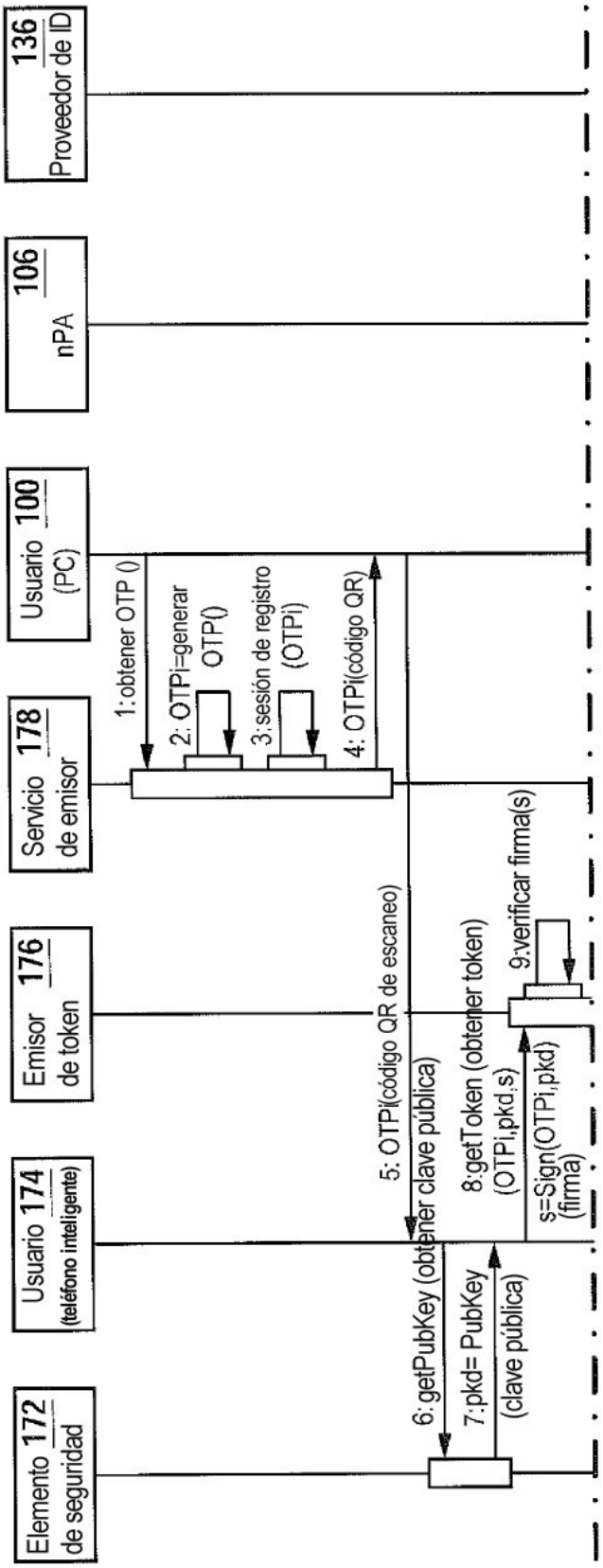
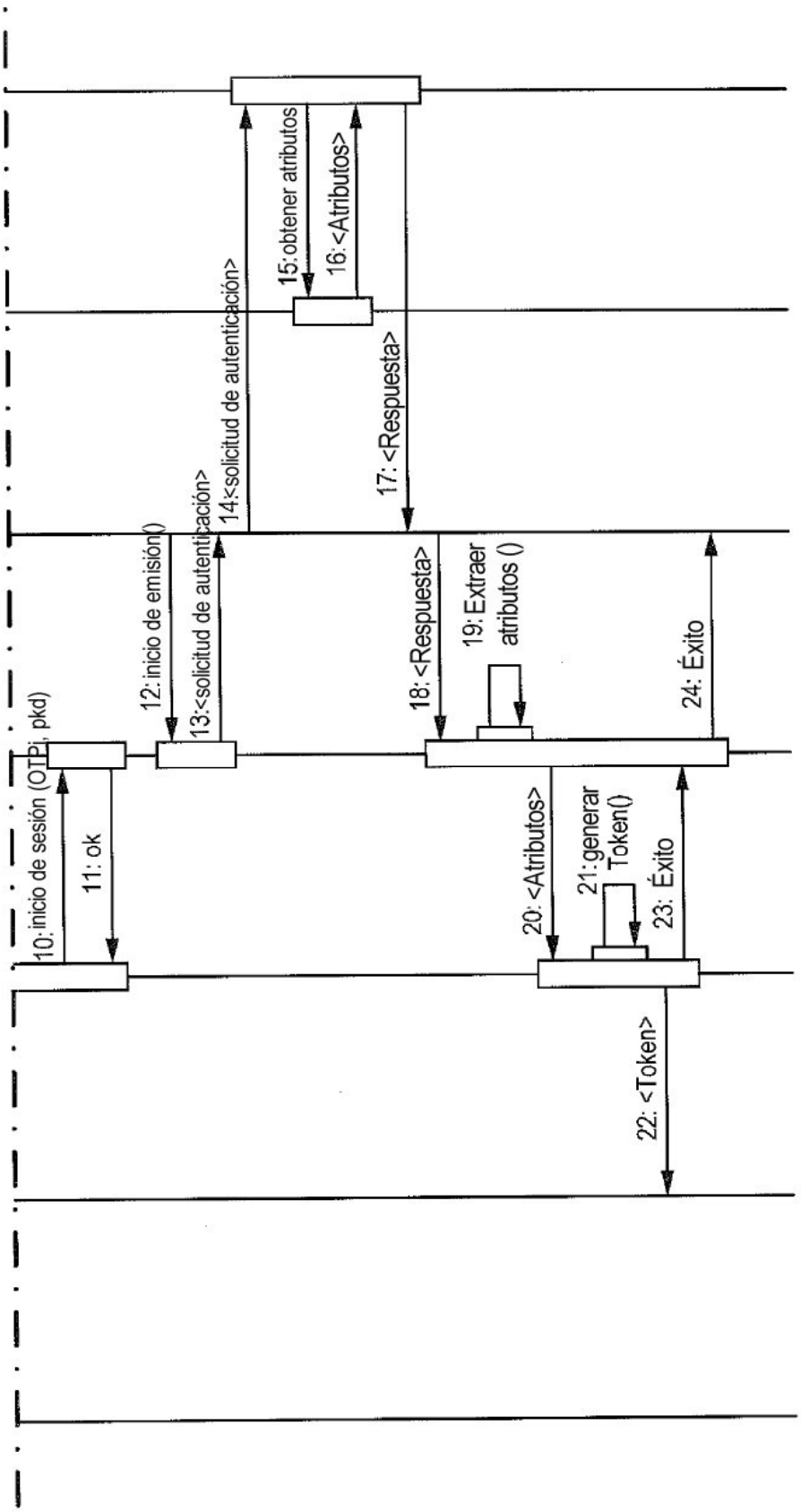

Elemento 172 de seguridad
Usuario 174 (teléfono inteligente)
Emisor 176 de token
Servicio 178 de emisor
Usuario 100 (PC)
106 nPA
136 Proveedor de ID
1: obtener OTP ()
2: OTPi=generar OTP()
3: sesión de registro (OTPi)
4: OTPi(código QR)
5: OTPi(código QR de escaneo)
6: getPubKey (obtener clave pública)
7: pkd= PubKey (clave pública)
8: getToken (obtener token) (OTPi,pkd,s)
9: verificar firma(s)
s=Sign(OTPi,pkd) (firma)

Fig. 7b


10: inicio de sesión (OTP; pkd)
11: ok
12: inicio de emisión()
13:<solicitud de autenticación>
14:<solicitud de autenticación>
15: obtener atributos
16: <Atributos>
17: <Respuesta>
18: <Respuesta>
19: Extraer atributos ()
20: <Atributos>
21: generar Token()
22: <Token>
23: Éxito
24: Éxito