(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 622 868**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.07.2011 PCT/EP2011/062645**

(87) Fecha y número de publicación internacional: **09.02.2012 WO12016859**

(96) Fecha de presentación y número de la solicitud europea: **22.07.2011 E 11740617 (3)**

(97) Fecha y número de publicación de la concesión europea: **18.01.2017 EP 2567503**

(54) Título: **Procedimiento y dispositivo para la puesta a disposición protegida contra la manipulación de un certificado de clave**

(30) Prioridad:

03.08.2010 DE 102010033231

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.07.2017

(73) Titular/es:

III HOLDINGS 12, LLC (100.0%)
2711 Centerville Road, Suite 400
Wilmington, DE 19808, US

(72) Inventor/es:

BUSSER, JENS-UWE y
FRIES, STEFFEN

(74) Agente/Representante:

MILTENYI, Peter

DESCRIPCIÓN

Procedimiento y dispositivo para la puesta a disposición protegida contra la manipulación de un certificado de clave

La invención se refiere a un procedimiento y a un dispositivo para la puesta a disposición protegida contra la manipulación de un certificado de clave mediante el uso de una contraseña de un solo uso para la autorización y la protección de la integridad de una solicitud de firma de certificado.

En muchas situaciones de uso, es necesaria la conexión de un aparato de usuario en el ámbito doméstico de un usuario, la cual es establecida por un proveedor de servicios. Por ejemplo, en el caso de una red de suministro de corriente inteligente, un proveedor de energía puede prever una entrada de energía como aparato de usuario en el hogar de un usuario. Este tipo de entradas de energía sirven sobre todo para optimizar el consumo y la alimentación de energía mediante consumidores de energía y consumidores descentralizados. Estas entradas de energía sirven en este caso para el control de productores de energía, como por ejemplo, células solares o instalaciones térmicas de cogeneración del correspondiente hogar. Estas entradas de energía permiten además de ello, que el correspondiente usuario pueda participar en la provisión de energía en condiciones ventajosas para él, en cuanto que en momentos de una alta demanda de energía, alimenta energía a la red de suministro de energía. Para poder poner a disposición un sistema de suministro de energía inteligente descentralizado de este tipo, con una pluralidad de entradas de energía, es necesario, conectar los diferentes participantes o usuarios, así como los diferentes proveedores de servicios de energía o proveedores de energía, de forma segura a la red. En este caso, la identidad o la comprobación de la identidad del correspondiente aparato de usuario o entrada de energía, tiene una importancia esencial. La identidad del aparato de usuario, por ejemplo, de la entrada de energía, se asegura en este caso de manera convencional en forma de un certificado de clave y una clave privada correspondiente. El material de clave requerido se genera en este caso por parte del mismo aparato de usuario, por ejemplo, entrada de energía. Existe una pluralidad de diferentes aparatos de usuario, los cuales son instalados por diferentes proveedores de servicios en la ubicación de los usuarios, en particular en el ámbito doméstico, poniendo a disposición de los usuarios los proveedores de servicios, un servicio a través del aparato de usuario intstalado. Ejemplos de este tipo de aparatos de usuario, son además de entradas de energía, las cuales pueden servir para el intercambio de datos con un proveedor de energía, aparatos médicos para el intercambio de datos de pacientes con un proveedor de servicios, por ejemplo, un centro médico, o aparatos de alarma, por ejemplo, una alarma de incendios, para la transmisión de alarmas de incendios a un proveedor de servicios, por ejemplo, una estación de bomberos. Además de ello, existe una pluralidad de aparatos de comunicación, por ejemplo, aparatos de televisión de pago, los cuales son instalados por un proveedor de servicios en la ubicación del usuario, para transmitir datos de información, por ejemplo, películas, al usuario.

La mayoría de este tipo de aparatos de usuario puede obtenerse por libre comercio, por ejemplo, en establecimientos de electrónica. Cuando un aparato de usuario de este tipo es adquirido por un usuario e instalado en su ubicación, el usuario ha de registrarse en un servidor del proveedor de servicios, para poder obtener el servicio deseado. En este caso puede certificarse una clave pública generada por el aparato de usuario, en el marco de un procedimiento de registro en el proveedor de servicios, mediante la generación de un certificado digital, sin que se haya celebrado ya necesariamente un contrato entre el usuario y el proveedor de servicios al comprarse el aparato de usuario. Esto puede llevarse a cabo también en el marco del primer registro.

En este caso existe habitualmente no obstante el riesgo, de que un material de clave a certificar sea enviado en un mensaje para la certificación al servidor del proveedor de servicios por una persona diferente al cliente o usuario propiamente dicho, el cual quiere adquirir el servicio del proveedor de servicios, al proveedor de servicios. Esto es posible, dado que no existe ninguna conexión autenticada entre los componentes participantes, es decir, el aparato de usuario y el servidor del proveedor de servicios.

El documento US 5 825 300 A muestra un procedimiento para la distribución protegida de un certificado entre un punto de certificación y al menos un participante del punto de certificación. El documento US 2004 / 0 158 708 A1 muestra un procedimiento para el intercambio de claves criptográficas públicas entre dos participantes, los cuales comparten una contraseña secreta común. El documento DE 10 2005 009 867 A1 muestra un procedimiento para la puesta a disposición de certificados electrónicos para el uso para firmas electrónicas.

Es una tarea de la presente invención proporcionar un procedimiento y un dispositivo para la puesta a disposición protegida contra la manipulación, de un certificado de clave para una clave de aparato de un aparato de usuario.

Esta tarea se soluciona según la invención mediante un procedimiento con las características indicadas en la reivindicación 1. La invención proporciona además de ello, un servidor con las características de la reivindicación 9.

En el procedimiento según la invención, se vincula lógicamente una solicitud de firma de certificado CSR (*Certificate Signing Request*), que es enviada por un componente (aún) no fiable o un aparato de usuario aún no fiable, al servidor del proveedor de servicios, con una contraseña de un solo uso OTP (*One Time Password*), la cual fue generada por un componente del futuro proveedor de servicios.

En una forma de realización posible, la contraseña de un solo uso (OTP) es generada por un servidor del proveedor de servicios para una determinada ID de aparato del aparato de usuario. En el caso de esta ID de aparato, puede

tratarse por ejemplo, de un número de serie del aparato de usuario o de una dirección Mac del aparato de usuario. El servidor almacena preferiblemente la contraseña de un solo uso OTP generada junto con la ID de aparato del aparato de usuario en una memoria de datos a la que tiene acceso el servidor.

En una forma de realización posible del procedimiento según la invención, la contraseña de un solo uso OTP del aparato de usuario generada es enviada por el proveedor de servicios mediante un soporte de datos al usuario.

En una forma de realización posible del procedimiento según la invención, la contraseña de un solo uso OTP del aparato de usuario, transportada en el soporte de datos enviado, se lee mediante una interfaz del aparato de usuario a partir del soporte de datos enviado.

En una forma de realización posible del procedimiento según la invención, el soporte de datos está integrado en el aparato de usuario y se envía de esta manera junto con el aparato de usuario al usuario. El soporte de datos se conforma por ejemplo, mediante una memoria interna del aparato de usuario.

En una forma de realización alternativa, el soporte de datos es un soporte de datos separado, el cual se conecta al aparato de usuario para la lectura de la contraseña de un solo uso OTP almacenada en éste.

En una forma de realización posible, este soporte de datos se envía por parte del proveedor de servicios o un distribuidor del aparato de usuario, junto con el aparato de usuario al usuario o cliente.

El soporte de datos se envía por ejemplo, junto con el aparato de usuario en un paquete postal al usuario. El soporte de datos puede tratarse por ejemplo, de una memoria USB, la cual se proporciona junto con el aparato de usuario en un paquete postal u otro embalaje al usuario.

En una forma de realización posible, el soporte de datos no se envía junto con el aparato de usuario, sino por separado al usuario. De esta manera se aumenta la seguridad frente a intentos de manipulación.

En una forma de realización posible del procedimiento según la invención, se produce localmente una pareja de claves de aparato criptográficas para el aparato de usuario a instalar en la ubicación del usuario. La pareja de claves de aparato comprende en este caso una clave de aparato pública y una clave de aparato privada del aparato de usuario. La pareja de claves de aparato criptográficas se genera por parte del usuario. En una forma de realización posible, la pareja de claves de aparato criptográficas es producida por el aparato de usuario mismo.

En una forma de realización posible del procedimiento según la invención, se conforma mediante el aparato de usuario una solicitud de firma de certificado CSR para la clave de aparato pública generada localmente. Esta solicitud de firma de certificado CSR se une o vincula lógicamente con la contraseña de un solo uso OTP del aparato de usuario leída a partir del soporte de datos, por ejemplo, la memoria USB.

En una forma de realización posible del procedimiento según la invención, se calcula un valor hash con clave para al menos un campo de datos de la solicitud de firma de certificado CSR en dependencia de la contraseña de un solo uso OTP del aparato de usuario y de la clave de aparato pública generada localmente.

En una forma de realización posible del procedimiento según la invención, la solicitud de firma de certificado CSR generada por el aparato de usuario, se transmite junto con la contraseña de un solo uso OTP del aparato de usuario, leída a partir del soporte de datos, por parte del aparato de usuario a través de un canal de comunicación asegurado criptográficamente al servidor del proveedor de servicios.

En una forma de realización posible del procedimiento según la invención, se verifica la solicitud de firma de certificado CSR conformada, la cual se transmite a través del aparato de usuario al servidor del proveedor de servicios, por medio del servidor, mediante la contraseña de un solo uso OTP almacenada en la memoria de datos del servidor para el aparato de usuario.

En una forma de realización posible, el servidor presenta un generador de contraseña de un solo uso, que genera para cada aparato de usuario una contraseña de un solo uso correspondiente.

En una forma de realización posible, el servidor presenta además de ello, una memoria de datos, en la cual están almacenadas las contraseñas de un solo uso OTP generadas de aparatos de usuario junto con las ID de aparatos correspondientes de los aparatos de usuario.

En otra forma de realización posible del servidor según la invención, este servidor presenta una unidad de verificación, la cual verifica una solicitud de firma de certificado CSR recibida por un aparato de usuario mediante una de las contraseñas de un solo uso OTP almacenadas en la memoria de datos.

En una forma de realización posible, la unidad de verificación del servidor verifica adicionalmente una firma de la solicitud de firma de certificado CSR recibida mediante una clave de aparato pública del aparato de usuario.

La solicitud de firma de certificado puede ser recibida por el servidor por ejemplo, a través de una red de datos del aparato de usuario intstalado. Esta red de datos puede tratarse por ejemplo, de Internet.

En una forma de realización posible del servidor según la invención, la contraseña de un solo uso OTP de un aparato de usuario, generada por el generador de contraseñas de un solo uso del servidor, se deposita en un soporte de datos integrado en el aparato de usuario, enviándose el aparato de usuario junto con el soporte de datos integrado en éste, directa o indirectamente desde el proveedor de servicios a través de los socios de distribución al usuario.

En una forma de realización alternativa, la contraseña de un solo uso generada por el generador de contraseñas de un solo uso del servidor del proveedor de servicios, se deposita en un soporte de datos separado del aparato de usuario, el cual se envía junto con el aparato de usuario o por separado del aparato de usuario directamente desde el proveedor de servicios o a través de socios de distribución para la instalación del aparato de usuario.

En una forma de realización posible del servidor según la invención, se trata en el caso del servidor del servidor de un proveedor de servicios, el cual pone a disposición a través del aparato de usuario instalado un servicio de forma permanente a un usuario.

En lo sucesivo se describen formas de realización posibles del procedimiento según la invención y del servidor según la invención haciendo referencia a las figuras que acompañan para la explicación de la invención.

La Fig. 1 muestra un diagrama de señal para la explicación del procedimiento según la invención;

La Fig. 2 muestra un diagrama de bloques de una posible forma de realización del servidor según la invención para la puesta a disposición protegida contra manipulación del certificado de clave.

Como puede verse en la Fig. 1, un aparato de usuario 1 dispone en el procedimiento según la invención, de una conexión de comunicación con un servidor 2. En el caso de la conexión de comunicación puede tratarse de una o varias redes de datos inalámbricas o por cable.

El aparato de usuario 1 puede ser un aparato de usuario instalado de manera fija en el ámbito doméstico de un usuario, pero también un terminal móvil. En el caso del aparato de usuario 1 se trata por ejemplo, de una entrada de energía para el intercambio de datos con un proveedor de energía. En el caso del aparato de usuario 1 puede tratarse además de ello también, de un aparato médico para el intercambio de datos de pacientes con un proveedor de servicios sanitarios o de un aparato de alarma para la transmisión de mensajes de alarma a un proveedor de servicios, por ejemplo, a una estación de bomberos. Puede tratarse además de ello, en el caso del aparato de usuario 1, de un aparato de comunicación para el intercambio de datos con un proveedor de servicios, por ejemplo, de un aparato de televisión de pago para la recepción de datos multimedia.

El servidor 2 puede ser por ejemplo, el servidor de un proveedor de servicios, que pone a disposición del usuario del aparato de usuario 1 un servicio. Si se trata en el caso del aparato de usuario 1 por ejemplo, de una entrada de energía de un cliente de una empresa de suministro de corriente, el servidor 2 del proveedor de corriente puede alimentar al usuario por ejemplo regularmente con datos de facturación, los cuales indican, cuanta energía ha consumido el usuario del aparato de usuario 1 de la red de corriente o cuanta energía ha alimentado el usuario a la red de corriente. Son posibles otros servicios. El servidor 2 del distribuidor de red de corriente puede enviar por ejemplo al aparato de usuario 1 del usuario datos referentes a una previsión del tiempo en el área del aparato de usuario 1. Si el aparato de usuario 1 se encuentra por ejemplo, en el sur de Baviera, el servidor 2 suministrará al aparato de usuario 1 datos de previsión del tiempo para esta región, de manera que el usuario “Mr. Charles” pueda su sistema de energía solar para una red de suministro de corriente de energía de manera adaptada al tiempo previsto. Para poder hacer uso de estos servicios, se pone a disposición del aparato de usuario 1 un certificado de clave Z para una clave de aparato del aparato de usuario 1 de manera protegida contra la manipulación mediante el servidor 2. El servidor 2 solo pone a disposición el certificado de clave Z al aparato de usuario 1, en caso de que se verifique exitosamente una solicitud de firma de certificado CSR (*Certificate Signing Request*) recibida del aparato de usuario 1 mediante el servidor 2 mediante una contraseña de un solo uso OTP (*One Time Password*) generada por el servidor 2 para el aparato de usuario 1.

El servidor 2 comprende preferiblemente un generador de contraseña de un solo uso, que genera para cada aparato de usuario 1 una contraseña de un solo uso correspondiente. El generador de contraseña de un solo uso del servidor 2 del proveedor de servicio genera una contraseña de un solo uso OTP para una ID de aparato del aparato de usuario 1. En el caso de esta ID de aparato puede tratarse por ejemplo, de un número de serie de un aparato fabricado. Alternativamente puede tratarse en el caso de la ID de aparato, también de una dirección MAC del aparato de usuario 1. Es posible además de ello, que en el caso de la ID se trate de una ID de usuario del usuario o del cliente. Esta contraseña de un solo uso OTP generada se almacena mediante el servidor 2 inicialmente en una memoria de datos del servidor 2. En esta memoria de datos se encuentran una pluralidad de contraseñas de uno solo uso OTP generadas de diferentes aparatos de usuario 1, que se almacenan respectivamente con correspondientes ID de aparato de los respectivos aparatos de usuario 1. La contraseña de un solo uso OTP del aparato de usuario 1 generada es enviada además de ello por el proveedor de servicios mediante un soporte de datos al usuario. El envío de la contraseña de un solo uso OPT generada se produce, como se indica mediante la línea a rayas en la Fig. 1, por un canal de comunicación separado o por correo. La contraseña de un solo uso OTP del aparato de usuario 1 transportada en el soporte de datos enviado, se lee en una forma de realización posible

mediante una interfaz del aparato de usuario 1 a partir del aparato de datos enviado y recibido por el usuario. En una forma de realización posible, el soporte de datos está integrado en el aparato de usuario 1 y conforma una parte del aparato de usuario 1. En esta forma de realización, el aparato de usuario 1 es enviado por el proveedor de servicios junto con el aparato de usuario a un usuario o cliente, por ejemplo, en un paquete. El usuario activa entonces el aparato de usuario 1, leyéndose entonces automáticamente la contraseña de un solo uso OTP almacenada en el soporte de datos integrado del aparato de usuario 1, eventualmente tras la introducción de una correspondiente contraseña. Un proveedor de energía envía por ejemplo entradas de energía a clientes, almacenándose en una memoria interna o soporte de datos del aparato de usuario o de la entrada de energía 1 una correspondiente contraseña de un solo uso OTP del aparato de usuario 1 con acceso seguro. Para la activación de la entrada de energía 1 por parte del usuario se lee eventualmente tras una correspondiente solicitud de contraseña entonces la contraseña de un solo uso OTP almacenada desde la memoria interna.

En una forma de realización alternativa, el soporte de datos no está integrado en el aparato de usuario 1, sino que conforma un soporte de datos separado. En el caso de este soporte de datos puede tratarse por ejemplo, de una memoria USB. En esta forma de realización, este soporte de datos es enviado por el proveedor de servicios junto con el aparato de usuario 1, por ejemplo, en un paquete al usuario. El usuario activa el aparato de usuario 1 e inserta el soporte de datos, por ejemplo, una memoria USB, en una interfaz del aparato de usuario, para que el aparato de usuario pueda leer la contraseña de un solo uso a partir del aparato de memoria.

En otra forma de realización posible el soporte de datos no se envía junto con el aparato de usuario en un paquete, sino que se envía por separado al usuario. El soporte de datos se envía por ejemplo, en un paquete postal separado al usuario. En el caso del soporte de datos separado no ha de tratarse obligatoriamente de un soporte de datos que puede ser palpado físicamente, puede tratarse en este caso por ejemplo también, de un paquete de datos electrónico, el cual se transmite por ejemplo a través de una red local o Internet al aparato de usuario 1 por separado del aparato de usuario. El paquete de datos puede comprender por ejemplo como datos de uso, la contraseña de un solo uso OTP transportada del aparato de usuario 1. Es posible además de ello, que la contraseña de un solo uso OTP para el aparato de usuario 1 se envíe por un canal de comunicación separado, por ejemplo, por correo electrónico al usuario. El envío separado del aparato de usuario 1 de la contraseña de un solo uso OTP correspondiente aumenta la seguridad frente a manipulaciones.

Por parte del usuario se genera localmente una pareja de claves de aparato criptográfica para el aparato de usuario 1 a instalar en la ubicación del usuario. En una forma de realización posible, la pareja de claves de aparato criptográfica es generada por el aparato de usuario 1 mismo. La pareja de claves de aparato criptográfica generada localmente comprende una clave de aparato criptográfica pública K_{pub} y una clave de aparato criptográfica privada K_{priv} del aparato de usuario 1. A continuación, se configura mediante el aparato de usuario 1 una solicitud de firma de certificado CSR para la clave de aparato pública K_{pub} generada localmente y se transmite al servidor 2, por ejemplo, a través de una red de datos. En este caso, la solicitud de firma de certificado CSR, que se conforma mediante el aparato de usuario 1, está unida con la contraseña de un solo uso OTP del aparato de usuario 1 que se lee del soporte de datos, en particular vinculada lógicamente. Para la conexión de la contraseña de un solo uso OTP leída, con la solicitud de firma de certificado CSR, existen diferentes posibilidades.

En una primera forma de realización, la solicitud de firma de certificado CSR presenta diferentes características CSR, en correspondencia con el estándar PKCS#9 y PKCS#10, por ejemplo, una *Attribut Challenge Password* (contraseña de comprobación de característica). Esta característica se proporciona para solicitar una revocación de un certificado. En una forma de realización posible, esta característica del mensaje CSR se utiliza para el transporte de la contraseña de un solo uso OTP leída desde el soporte de datos. En este caso, la contraseña de un solo uso OTP preferiblemente no se transmite en texto claro, sino que se transmite codificada criptográficamente, en cuanto que se calcula por ejemplo un valor hash con clave HMAC a través de uno o varios campos de datos de la solicitud de firma de certificado CSR. En este caso se calcula un valor hash con clave HMAC para al menos un campo de datos de la solicitud de firma de certificado CSR en dependencia de la contraseña de un solo uso OTP del aparato de usuario 1. Alternativamente es posible que se defina una característica adicional para la solicitud de firma de certificado CSR, la cual permite el transporte de parámetros de seguridad adicionales. En otra variante se firma de tal manera un nuevo contendor de datos o receptáculo de datos para la solicitud de firma de certificado CSR, que a través de la totalidad de la solicitud de firma de certificado CSR se calcula un valor HMAC, aceptándose igualmente la contraseña de un solo uso OTP como clave.

En otra variante, la solicitud de firma de certificado CSR conformada por el aparato de usuario 1 se transmite junto con la contraseña de un solo uso OTP del aparato de usuario, leída del soporte de datos, desde el aparato de usuario a través de un canal de comunicación asegurado criptográficamente al servidor 2 del proveedor de servicios. En esta forma de realización, la contraseña de un solo uso OTP puede transmitirse en texto claro. Preferiblemente no obstante, la contraseña de un solo uso OTP se transmite de manera codificada para el aumento de la seguridad. En otra variante ventajosa, la contraseña de un solo uso OTP leída se transmite a través de una conexión de transporte codificada. En este caso se mantiene sin modificación el orden de transmisión original para la transmisión de la solicitud de firma de certificado CSR, dado que a diferencia de un encapsulamiento en un contenedor de datos decidido, en esta forma de realización se realiza un encapsulamiento a través de un protocolo de seguridad. El usuario o el cliente abren en este caso por ejemplo, una conexión TLS autenticada unilateralmente con el servidor 2 del proveedor de servicios, autenticándose el proveedor de servicios mediante certificado. El aparato de usuario 1 o

el cliente se autentifica por su parte a través de la conexión TLS con la contraseña de un solo uso OTP, por ejemplo, a través de una conexión http de mensaje cifrado. A través de la conexión de datos autenticada de esta manera por ambos lados, puede enviarse ahora la solicitud de firma de certificado CSR. La solicitud de firma de certificado CSR conformada, la cual es transmitida por el aparato de usuario 1 al servidor 2 del proveedor de servicios, se verifica mediante el servidor 2 a través de la contraseña de un solo uso OTP ya almacenada en su memoria de datos para el correspondiente aparato de usuario 1.

En caso de que la solicitud de firma de certificado CSR recibida por el aparato de usuario 1 sea verificada con éxito por el servidor 2 mediante la contraseña de un solo uso OTP almacenada para el aparato de usuario 1 en la memoria de datos del servidor 2, el servidor 2 pone a disposición un certificado de clave Z_k para la clave de aparato pública K_{pub} para el aparato de usuario 1. Este certificado de clave Z_k puesto a disposición lo puede usar el aparato de usuario 1 a continuación para la utilización del correspondiente servicio.

La Fig. 2 muestra un diagrama de bloques para la representación de una posible forma de realización del servidor 2 según la invención. El servidor 2 sirve para la puesta a disposición protegida contra la manipulación del certificado de clave Z_k para una clave de aparato, en particular una clave de aparato pública K_{pub}, del aparato de usuario 1. Este aparato de usuario 1 está instalado en la ubicación del usuario, el cual obtiene a través del aparato de usuario 1 del servidor 2 un servicio, por ejemplo, la transmisión de determinados datos de información. El servidor 2 pone a disposición el certificado de clave Z_k para el aparato de usuario 1, en caso de que una solicitud de firma de certificado CSR recibida por el aparato de usuario 1 por ejemplo, a través de una red de datos, sea verificada con éxito por el servidor 2 mediante una contraseña de un solo uso OTP generada y almacenada por el servidor 2 para el aparato de usuario 1.

Como se representa en la Fig. 2, el servidor 2 comprende un generador de contraseñas de un solo uso 2A, el cual genera para cada aparato de usuario 1, el cual es entregado por ejemplo por el proveedor de servicios al usuario, una contraseña de un solo uso OTP correspondiente. El servidor 2 presenta una memoria de datos 2B, en la cual, las contraseñas de un solo uso OTP generadas de los diferentes aparatos de usuario 1, se almacenan junto con correspondientes ID de aparato de los aparatos de usuario. En la forma de realización representada en la Fig. 2, la memoria de datos 2B está contenida en el servidor 2. En una forma de realización alternativa, el servidor 2 tiene acceso a una memoria de datos 2B externa, por ejemplo, a través de una red. El servidor 2 recibe la solicitud de firma de certificado CSR a través de una interfaz 2C a través de una red de datos, la cual está unida con el aparato de usuario 1. En el caso de la red, puede tratarse en este caso de una o varias redes de datos, a través de las cuales se transmite la solicitud de firma de certificado CSR del aparato de usuario 1 al servidor 2. En una forma de realización posible, esta red de datos es Internet. La red de datos puede presentar además de ello también, una red de telefonía móvil. En el caso del aparato de usuario 1, puede tratarse de un aparato de usuario de instalación fija o de un aparato móvil, por ejemplo, un teléfono móvil. El servidor 2 comprende además de ello una unidad de verificación 2D, la cual verifica una solicitud de firma de certificado CSR recibida por el aparato de usuario mediante una contraseña de un solo uso OTP almacenada en la memoria de datos 2B. Si la verificación tiene éxito, la unidad de verificación 2D controla un generador de certificados 2E del servidor 2 de tal manera, que se genera un certificado de clave Z_k digital para la clave de aparato K_{pub} del correspondiente aparato de usuario 1. Este certificado de clave Z_k se transmite a continuación a través de la interfaz 2C al aparato de usuario 1 para su uso posterior. En una forma de realización posible el servidor 2 genera mediante el generador OTP 2A una contraseña de un solo uso OTP, que junto con la correspondiente ID de aparato se almacena en la memoria de datos 2B. El servidor 2 transmite además de ello fuera de línea la contraseña de un solo uso OTP generada al aparato de usuario 1, en cuyo caso se trata por ejemplo, de una entrada de energía de un hogar privado. El aparato de usuario 1 o el cliente genera en primer lugar localmente el material de clave, esto quiere decir, una pareja de claves de aparato que comprende una clave de aparato pública K_{pub} y una clave de aparato privada K_{priv}. A continuación, el aparato de usuario 1 genera la solicitud de firma de certificado CSR, calculándose para una determinada característica, por ejemplo, la característica contraseña de comprobación, un valor hash con clave a través de partes de CSR. Con este valor hash con clave calculado, el servidor 2 es capaz a continuación, de verificar la posesión de la contraseña de un solo uso OTP. En una forma de realización posible, la asociación se produce en el servidor 2 por ejemplo, a través de un llamado nombre distinguido DN (*Distinguished Name*). Aquí el aparato de usuario 1 puede introducir un identificador, por ejemplo, su número de serie o su dirección Mac.

En una forma de realización posible especial, se lleva a cabo el siguiente desarrollo:

$CSR_{ATT} \in CSR$

$CRS_{ATT} = HMAC_{OTP}$

$HMAC_{OTP} = HMAC(OTP,m) = H[(OTP\_xOR\_OPAD)] \| H[(OTP\_xOR\_IPAD) \| m)]$

donde

$m = V \mid |ID| \mid K_{pub}$

v = Nº de versión del estándar de certificado

ID = ID del aparato del aparato de usuario (número de serie o dirección MAC)

K_{pub} = clave de aparato criptográfica pública

y

OPAD, IPAD secuencias de signos predeterminadas

son pasos adicionales:

- SIGN (CSR_{ATT}, K_{priv}) = SIGN ($HMAC_{OTP}$, K_{priv})

- TRANSMITT (CSR_{ATT}; SIGN)

- VERIFY (SIGN, K_{pub})

- VERIFY (CSR_{ATT}; (OTP,m))

En esta forma de realización, la unidad de verificación 2D del servidor 2 verifica una firma (SIGN) de la solicitud de firma de certificado CSR recibida mediante una clave de aparato pública K_{pub} del aparato de usuario 1.

A continuación, se verifica una característica (CSR_{ATT}) de la solicitud de firma de certificado (CSR) mediante la unidad de verificación 2D del servidor 2 mediante la contraseña de un solo uso OTP generada y almacenada para el aparato de usuario 1 por el servidor 2. Esto puede ocurrir debido a que la unidad de verificación 2D calcula el valor hash con clave (HMAC) con la ecuación indicada más arriba, para comprobar si el aparato de usuario 1 o el cliente disponen de la contraseña de un solo uso OTP correcta.

En otra forma de realización posible, el servidor 2 genera en primer lugar la contraseña de un solo uso OTP y la envía fuera de línea al aparato de usuario 1 o al usuario. El usuario o el aparato de usuario 1 generan en primer lugar localmente el material de clave y abren entonces una conexión autenticada unilateralmente mediante TSL con el servidor (PEA-Registry). El cliente 1 se autentica con su contraseña de un solo uso OTP. A continuación, se envía la solicitud de firma de certificado CSR a través de la conexión de datos autenticada por ambos lados. El servidor 2 puede generar a continuación un certificado Z y reenviarlo al cliente o al aparato de usuario 1.

En el procedimiento según la invención para la puesta a disposición protegida frente a la manipulación, de un certificado de clave Z, se conecta una solicitud de firma de certificado CSR con una contraseña de un solo uso OTP, permitiendo esta conexión a un proveedor de servicios vender aparatos de usuario 1, por ejemplo, entradas de energía en el comercio libre, los cuales preferiblemente están configurados de tal manera, que en caso de una personalización por parte de un usuario puede realizarse una conexión a un aparato de usuario 1. Esto ocurre a través de la conexión a la CSR. El material de clave producido por el aparato de usuario 1 se verifica entonces a través del certificado Z_k por parte del proveedor de servicios. Para todas las demás conexiones de datos puede usarse ahora este certificado Z con la clave privada K_{priv} correspondiente.

El procedimiento y el sistema según la invención ofrecen en particular la ventaja, de que puede reducirse el esfuerzo para la generación de clave y la administración por parte del proveedor de servicios. El procedimiento y el sistema según la invención posibilitan además de ello, una puesta en marcha sencilla por parte del usuario. Puede usarse además de ello en el procedimiento según la invención, una infraestructura de certificación existente, dado que debido a la integración de la contraseña de un solo uso OTP en una característica CSR, solo se modifica la semántica de la característica.

REIVINDICACIONES

1. Procedimiento para la puesta a disposición protegida contra la manipulación de un certificado de clave (Z) para una clave de aparato (K_{pub}) de un aparato de usuario (1), que se instala en la ubicación de un usuario, mediante un servidor (2) de un proveedor de servicios que pone a disposición del usuario una prestación de servicios a través del aparato de usuario (1), poniendo el servidor (2) el certificado de clave (Z) a disposición del aparato de usuario (1) en caso de que una solicitud de firma de certificado (CSR) recibida por el aparato de usuario (1) sea verificada con éxito por el servidor (2) mediante una contraseña de un solo uso (OTP) generada por el servidor (2) para el aparato de usuario (1), generándose localmente mediante el aparato de usuario (1) una pareja de claves de aparato criptográficas para el aparato de usuario (1) a instalar en la ubicación del usuario, la cual comprende una clave de aparato pública (K_{pub}) y una clave de aparato privada (K_{priv}) del aparato de usuario, formándose mediante el aparato de usuario (1) una solicitud de firma de certificado (CSR) para la clave de aparato pública (K_{pub}) generada localmente, conectándose lógicamente la solicitud de firma de certificado (CSR) con la contraseña de un solo uso (OTP) del aparato de usuario (1) leída a partir de un soporte de datos y calculándose un valor hash con clave (HMAC) para al menos un campo de datos de la solicitud de firma de certificado (CSR) dependiendo de la contraseña de un solo uso (OTP) del aparato de usuario (1) y de la clave de aparato pública (K_{pub}) generada localmente.

2. Procedimiento según la reivindicación 1, en donde el servidor (2) del proveedor de servicios genera la contraseña de un solo uso (OTP) para una ID de aparato del aparato de usuario (1) y la almacena junto con la ID de aparato del aparato de usuario (1) en una memoria de datos (2B) del servidor (2).

3. Procedimiento según las reivindicaciones 1 o 2, en donde la contraseña de un solo uso (OTP) generada del aparato de usuario es enviada por el proveedor de servicios mediante el soporte de datos al usuario.

4. Procedimiento según la reivindicación 3, en donde la contraseña de un solo uso (OTP) del aparato de usuario (1), transportada en el soporte de datos enviado, se lee mediante una interfaz del aparato de usuario (1) desde el soporte de datos enviado.

5. Procedimiento según la reivindicación 4, en donde el soporte de datos está integrado en el aparato de usuario (1) o formando un soporte de datos separado que se conecta al aparato de usuario para leer la contraseña de un solo uso (OTP).

6. Procedimiento según la reivindicación 5, en donde el proveedor de servicios envía el soporte de datos junto con el aparato de usuario (1) o por separado al usuario.

7. Procedimiento según la reivindicación 1, en donde la solicitud de firma de certificado (CSR) formada por el aparato de usuario (1), junto con la contraseña de un solo uso (OTP) del aparato de usuario (1) leída a partir del soporte de datos, es transmitida por el aparato de usuario (1) a través de un canal de comunicación asegurado criptográficamente al servidor (2) del proveedor de servicios.

8. Procedimiento según una de las reivindicaciones 1-7, en donde la solicitud de firma de certificado (CSR) formada, que es transmitida por el aparato de usuario (1) al servidor (2) del proveedor de servicios, es verificada por el servidor (2) mediante la contraseña de un solo uso (OTP) almacenada en la memoria de datos (2B) del servidor (2) para el aparato de usuario (1).

9. Servidor (2) para llevar a cabo un procedimiento según al menos una de las reivindicaciones 1-8 para la puesta a disposición protegida contra la manipulación de un certificado de clave (Z) para una clave de aparato pública (K_{pub}) de un aparato de usuario (1), que se instala en la ubicación de un usuario, el cual recibe a través del aparato de usuario (1) un servicio del servidor (2), poniendo el servidor (2) el certificado de clave (Z) a disposición del aparato de usuario (1), en caso de que una solicitud de firma de certificado (CSR) recibida por el aparato de usuario (1) sea verificada con éxito por el servidor (2) mediante una contraseña de un solo uso (OTP) generada y almacenada por el servidor (2) para el aparato de usuario (1).

10. Servidor según la reivindicación 9, presentando el servidor (2):

- un generador de contraseñas de un solo uso (2A), que genera para cada aparato de usuario (1) una contraseña de un solo uso (OTP) correspondiente,

- una memoria de datos (2B), en la cual están almacenadas las contraseñas de un solo uso (OTP) generadas de aparatos de usuario junto con los correspondientes ID de aparato de los aparatos de usuario, y

- una unidad de verificación (2D) que verifica una solicitud de firma de certificado (CSR) recibida por un aparato de usuario (1) mediante una contraseña de un solo uso (OTP) almacenada en la memoria de datos (2B).

11. Servidor según la reivindicación 10, en donde la contraseña de un solo uso (OTP), generada por el generador de contraseñas de un solo uso (2A), de un aparato de usuario (1) se almacena o bien en un soporte de datos integrado en el aparato de usuario (1) y el aparato de usuario (1) se envía al usuario para la instalación o bien la contraseña de

un solo uso (OTP) generada del aparato de usuario (1) se deposita en un soporte de datos separado del aparato de usuario (1), que se envía junto con el aparato de usuario (1) o por separado del aparato de usuario (1) al usuario para la instalación del aparato de usuario (1).

12. Servidor según una de las reivindicaciones 9-11, en donde el servidor (2) es un servidor de un proveedor de servicios que pone a disposición de un usuario un servicio a través del aparato de usuario (1) instalado, presentando el aparato de usuario (1):

- una entrada de energía para el intercambio de datos con un proveedor de energía,

- un aparato médico para el intercambio de datos de pacientes con un proveedor de servicios,

- un aparato de alarma para la transmisión de mensajes de alarma a un proveedor de servicios, o

- un aparato de comunicación para el intercambio de datos con un proveedor de servicios.

13. Servidor según una de las reivindicaciones 11 o 12, en donde la contraseña de un solo uso (OTP), generada por el generador de contraseñas de un solo uso (2A) del servidor (2) de un aparato de usuario (1) se envía al usuario almacenada en un soporte de datos de memoria USB.

14. Servidor según una de las reivindicaciones 10-13, en donde la unidad de verificación (2D) del servidor (2) verifica, mediante una clave de aparato pública (K_{pub}) del aparato de usuario (1), una firma de la solicitud de firma de certificado (CSR) recibida.

FIG 1

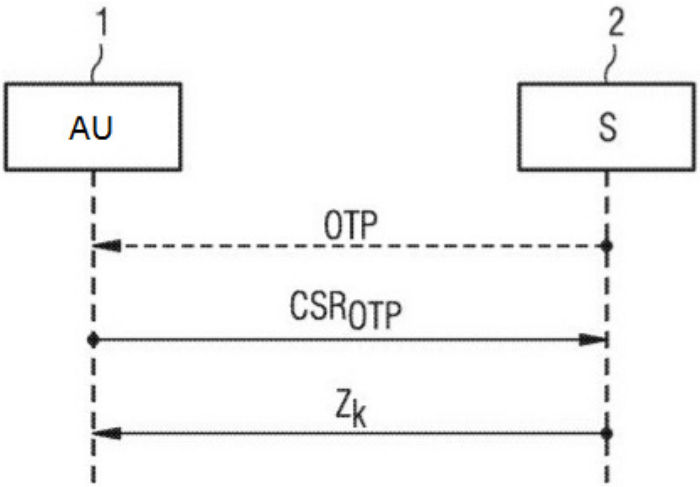
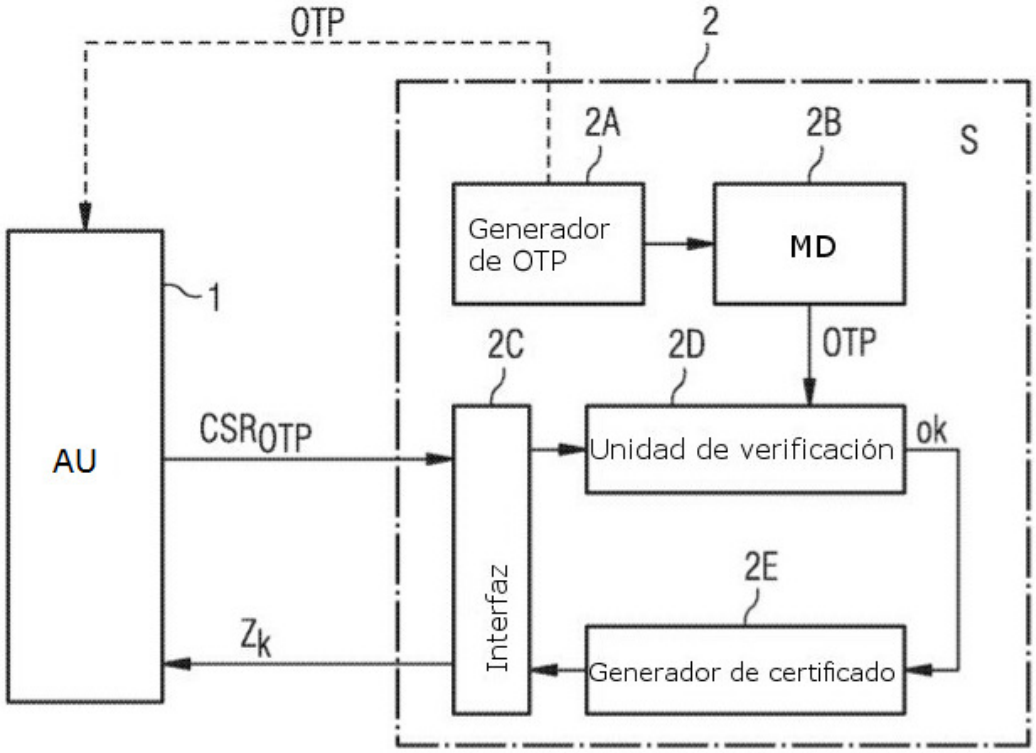

1
2
AU
S
OTP
CSR_OTP
Z_k

FIG 2


OTP
2
2A
2B
S
Generador de OTP
MD
1
2C
2D
OTP
AU
CSR_OTP
Unidad de verificación
ok
2E
Z_k
Interfaz
Generador de certificado