(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 766 749**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G01D 4/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.12.2012 PCT/EP2012/075323**

(87) Fecha y número de publicación internacional: **07.11.2013 WO13164042**

(96) Fecha de presentación y número de la solicitud europea: **13.12.2012 E 12812909 (5)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2019 EP 2850860**

(54) Título: **Dispositivo de seguridad de un contador de energía frente a un acceso no autorizado**

(30) Prioridad:

02.05.2012 DE 102012008519

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.06.2020

(73) Titular/es:

INNOGY SE (100.0%)
Opernplatz 1
45128 Essen, DE

(72) Inventor/es:

GAUL, ARMIN;
CATER, STEPHAN y
HEIDER, MARKUS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Dispositivo de seguridad de un contador de energía frente a un acceso no autorizado

El objeto se refiere a un sistema de seguridad de un contador de energía, así como a un procedimiento para la seguridad de un contador de energía.

La proliferación de contadores de energía inteligentes, como por ejemplo en la medición inteligente, conduce a una mayor exigencia en la seguridad de la comunicación de estos contadores de energía con un punto de facturación central. Los contadores de energía se utilizan en el ámbito del registro de energía eléctrica, pero también como medidores de gas y corriente. Asimismo, se pueden combinar varios contadores de energía en una red local de contadores.

Para la simplificación de una interfaz de comunicación entre un contador de energía y un punto de facturación central se propone una puerta de enlace de comunicación (aparato de comunicación). Esta puerta de enlace de comunicación sirve como interfaz de comunicación entre la red local de contadores (LMN, Local Metering Network) y la red de área amplia (WAN Wide Area Network), a través de la cual un operador de puntos de medición o una central de facturación tiene acceso al contador de energía.

Además, el aparato de comunicación puede estar conectado a través de otra interfaz a una red domótica (HAN Home Automation Network), en la que están dispuestos diversos sistemas de control local (CLS Controllable Local Systems). Estos pueden incluir, por ejemplo, controles de plantas de generación de energía locales, como por ejemplo plantas eólicas locales y plantas solares locales. También pueden estar previstas estaciones de carga locales para la carga de vehículos de accionamiento eléctrico.

Por tanto, el aparato de comunicación representa una interfaz común de los contadores de energía dispuestos localmente y las redes de domótica dispuestas localmente en una red de área amplia, a través de la cual las personas autorizadas, en particular los operadores de puntos de medición y las centrales de facturación, pueden acceder a los aparatos dispuestos en las redes locales, en particular los contadores de energía.

Esta interfaz central representa un punto de ataque sensible para ataques de terceros. Por esta razón, esta interfaz debe estar especialmente asegurada. En particular, debe estar asegurado que la interfaz solo enviará datos de los contadores de energía cuando estos datos sean solicitados desde un punto autorizado. También se debe asegurar que el aparato de comunicación no sea operado en un entorno no autorizado, por ejemplo para conocer los secretos de cifrado del punto de facturación central.

Por esta razón, la oficina federal de Seguridad de la Información (BSI) ha creado un perfil de protección para interfaces en sistemas de medición inteligentes, que es la base para la autorización de los aparatos de comunicación mencionados que sirven como interfaz. El perfil de protección para la unidad de comunicación de un sistema inteligente de medición para materia y energía, versión 01.01.01 (Final Draft), se incorpora aquí por completo al contenido de esta solicitud. Todas las funcionalidades de la puerta de enlace mencionadas allí deben ser proporcionadas según el objeto por el aparato de comunicación según el objeto. Además, todos los contadores de energía mencionados allí, así como todas las redes de domótica y sistemas locales mencionados allí, deberían poder ser operados con un sistema de seguridad de contador de energía concreto.

Por el documento DE 10 2009 036 181 A1 es conocido un dispositivo de puerta de enlace para el registro de un consumo de recursos que puede ser asegurado frente a un acceso no autorizado a través de un módulo de identificación.

El documento WO 2011/124298 A2 muestra igualmente un dispositivo de seguridad de una comunicación de un módulo de cifrado con un contador de energía.

Especialmente con contadores de energía y puertas de enlace de comunicación ya instalados, el cumplimiento del perfil de seguridad es en parte problemático porque el aparato de comunicación existente no siempre cumple con todos los requisitos de seguridad. Especialmente en el caso de estaciones de carga ya instaladas para vehículos eléctricos, que todas son operadas con contadores eléctricos inteligentes, el cumplimiento del perfil de protección es problemático. Una adaptación de varios miles de estaciones de carga conlleva enormes costes. Por esta razón se buscan posibilidades que permitan configurar la adaptación de las estaciones de carga de la forma más simple.

Por este motivo se propone el objeto de proporcionar un sistema de seguridad de contador de energía que cumpla con los requisitos para un perfil de protección para contadores de energía de una manera particularmente simple y al mismo tiempo permita una adaptación.

Este objeto se logra mediante un sistema de seguridad de contador de energía según la reivindicación 1, así como un procedimiento según la reivindicación 18.

Se ha reconocido que el perfil de protección requiere que esté previsto un módulo de cifrado que se utilizará para el cifrado y la custodia segura de los secretos criptográficos. El módulo de cifrado debe servir en particular para la

generación de pares de claves, para la generación de valores aleatorios, en particular para la generación de números aleatorios para operaciones criptográficas y la custodia segura de pares de claves y certificados de varios participantes de la comunicación. En particular, deben estar almacenadas las claves (privada y pública) y los certificados de la interfaz o del propio módulo de cifrado. Además, deben estar almacenados los certificados del operador de punto de red o de la central de facturación. Además, el módulo de cifrado debe ser adecuado para crear una firma electrónica de datos de contenido, en particular de datos de medición del contador de energía. El módulo de cifrado también debe ser adecuado para poder verificar las firmas electrónicas de datos de contenido. En particular, debería ser posible verificar si los datos de contenido proceden realmente del contador de energía que especifica esto. Esto debería ser posible mediante una firma sobre los datos de contador por el propio contador de energía. También deben ser proporcionados cifrados de estos datos por el módulo de cifrado.

El perfil de seguridad ahora requiere que tal módulo de cifrado solo se pueda operar en un entorno autenticado. Además, el módulo de cifrado debe proporcionar sus funciones solo después de realizarse la autenticación.

Se ha reconocido que estas dos condiciones no se pueden satisfacer exclusivamente cuando el módulo de cifrado está firmemente anclado en el aparato de comunicación, sino también cuando el módulo de cifrado está dispuesto en el aparato de comunicación extraíble de forma no destructiva.

Se ha reconocido según el objeto que todos los requisitos para el perfil de protección pueden cumplirse si el módulo de cifrado es operado en primer lugar en un estado inicial en el que solo está habilitado un acceso limitado a las funciones de cifrado. Preferiblemente, es posible únicamente un acceso a tales funciones de cifrado que permiten la autenticación del módulo de cifrado con respecto a un ordenador central dispuesto remoto. Además, en el estado inicial pueden estar habilitadas funciones de cifrado que aseguran la conexión correcta entre el módulo de cifrado y un contador de energía determinado.

A este respecto, por ejemplo, una posible función de cifrado habilitada en el estado inicial puede ser tal que se genere un valor aleatorio. Otra función puede ser el acceso a una clave pública de un ordenador central para verificar una firma del ordenador central a través del valor aleatorio.

Como ya se explicó al principio, en el módulo de cifrado puede estar almacenada una pluralidad de secretos criptográficos. Estos pueden ser certificados, claves públicas y claves privadas del propio módulo de cifrado. En este caso son posibles diferentes pares de claves y certificados, en particular en cada caso para la firma de números aleatorios, codificación de datos de usuario, en particular valores de medición del contador de energía y para el cifrado de tramos de comunicación. Además, los certificados y las claves públicas pueden estar almacenados por ordenadores centrales, en particular por un ordenador central del operador del puntos de medición o una central de facturación. También aquí pueden estar previstas diferentes claves y certificados para diferentes operaciones, por ejemplo la firma de números aleatorios, la codificación de datos de usuario y el cifrado de tramos de comunicación.

Para satisfacer el perfil de protección para aparatos de comunicación de contadores de energía debe garantizarse que una extracción y un uso abusivo del módulo de cifrado fuera del aparato de comunicación asociado a él sea difícil, si no completamente imposible. Por esta razón, se propone que el módulo de cifrado dispuesto extraíble de forma no destructiva, presente en su estado inicial funciones de cifrado solo limitadas. Preferiblemente estas funciones de cifrado limitadas sirven exclusivamente para la autenticación del módulo de cifrado con respecto a un ordenador central y/o viceversa. En este caso, el módulo de cifrado puede estar configurado para que pueda verificar si está conectado a un ordenador central correcto. Además, el módulo de cifrado puede estar diseñado para poder identificarse con respecto a un ordenador central.

Todas las otras funciones que son necesarias para una comunicación más segura entre el ordenador central y el aparato de comunicación pueden estar bloqueadas en el estado inicial. En particular, las funciones de cifrado para el cifrado de datos de usuario pueden estar bloqueadas.

Además, el módulo de cifrado puede estar configurado para realizar un proceso de emparejamiento con un ordenador central. En el estado de suministro, en el módulo de cifrado pueden estar almacenadas una clave pública de un ordenador central, así como un par de claves de clave pública y clave privada para el propio módulo de cifrado. El ordenador central conoce además su clave privada, así como también la clave pública del módulo de cifrado. Con estas informaciones es posible que el módulo de cifrado y el ordenador central se autentiquen uno respecto a otro y el módulo de cifrado pueda cambiar de su estado inicial a un estado de funcionamiento.

Si un secreto de cifrado ha sido potencialmente corrompido, el módulo de cifrado dispone de funciones para la realización de un proceso de emparejamiento que es suficientemente conocido. En tal proceso de emparejamiento se pueden intercambiar nuevos secretos de clave entre el ordenador central y el módulo de cifrado, utilizando los últimos secretos de cifrado existentes y reemplazándolos por secretos de cifrado recién aplicados.

Según un ejemplo de realización ventajoso se propone que el módulo de cifrado esté configurado para en el estado inicial recibir un requerimiento para la generación de un valor aleatorio. Esta puede ser una primera función de cifrado que está habilitada en el estado inicial. Por tanto, el módulo de cifrado puede recibir del ordenador central o del aparato de comunicación un requerimiento para crear un valor aleatorio. El valor aleatorio puede ser en este caso un número aleatorio. También es posible que se genere un valor aleatorio a partir de un valor de resistencia de una resistencia

dentro del módulo de cifrado. Un valor de resistencia puede fluctuar dependiendo de la temperatura y dependiendo del envejecimiento, de modo que un valor de resistencia tomado es casi estocástico. Con tal valor puede ser generado el valor aleatorio.

A este respecto se propone que el módulo de cifrado en el estado inicial esté configurado para la generación del valor aleatorio en respuesta a un requerimiento para la generación de un valor aleatorio. Por tanto, la generación del valor aleatorio puede ser otra función que está desconectada en el estado inicial.

Otra función de cifrado, que puede estar desconectada en el estado inicial, es según un ejemplo de realización, la emisión del valor aleatorio. Este puede ser emitido sin cifrar y sin firmar. También es posible que en el estado inicial se calcule una firma sobre el valor aleatorio creado y esta firma sea enviada junto con el valor aleatorio. En este caso, se usa preferiblemente una clave privada del módulo de cifrado. El acceso a esta clave privada puede igualmente estar desconectado en el estado inicial.

De acuerdo con un ejemplo de realización se propone que el módulo de cifrado en el estado inicial, después de la emisión del valor aleatorio, active un contador para monitorizar la duración hasta que se produce una respuesta a la emisión del valor aleatorio. Para ello se puede monitorizar un tiempo de espera. Dentro de un cierto tiempo debe llegar una respuesta del ordenador central al valor aleatorio. Si esto no sucede, puede existir una manipulación. Si se excede el tiempo de espera, se puede incrementar un contador de errores o bloquearse el módulo de cifrado.

Una función que puede estar disponible en el estado inicial en el módulo de cifrado es el acceso a una clave pública del ordenador central. En particular, de esta forma es posible verificar una firma del ordenador central. Si, por ejemplo, el valor aleatorio ha sido firmado con una clave privada del ordenador central, esta firma puede ser verificada en el módulo de cifrado ya en el estado inicial.

Con esto es posible verificar en el estado inicial si el módulo de cifrado está en conexión de comunicación con el ordenador central. Eventualmente es posible cambiar del estado inicial a un estado de funcionamiento en el que se liberan otras funciones.

Según un ejemplo de realización se propone que el módulo de cifrado en el estado inicial después de una verificación positiva de la firma a través del valor aleatorio, cambie a un estado de funcionamiento. Es decir que, en particular, cuando se asegura que el módulo de cifrado está en conexión de comunicación con el ordenador central, este puede cambiar al estado de funcionamiento. Se puede establecer una conexión con el ordenador central, por ejemplo por una verificación de la firma del ordenador central.

Una vez que se determina que el módulo de cifrado está en conexión de comunicación con el ordenador central correcto, puede cambiarse a un estado de funcionamiento. En el estado de funcionamiento es posible un acceso a otras funciones de cifrado, que sobrepasan a las funciones de cifrado que estaban disponibles en el estado inicial.

Si en la verificación de la firma a través del valor aleatorio el módulo de cifrado determina que esta no fue creada por el ordenador central correcto, el módulo de cifrado puede permanecer en el estado inicial. Preferiblemente se incrementa un contador de errores. En caso de que el contador de errores exceda por encima de un valor límite, se puede suponer que una conexión correcta con el ordenador central ya no es posible y el módulo de cifrado puede ser bloqueado. Un acceso al estado inicial o al estado de funcionamiento es entonces imposible. Preferiblemente, en este momento todos los secretos de cifrado en la memoria del módulo de cifrado son borrados.

Según un ejemplo de realización se propone que el módulo de cifrado presente dos áreas de memoria. Las áreas de memoria tienen diferentes niveles de seguridad, que se caracterizan por que un área de memoria solo se puede alcanzar en el estado de funcionamiento. Esto significa que en el estado inicial puede estar habilitado un acceso a solo la primera área de memoria y en el estado de funcionamiento el acceso a ambas áreas de memoria. En la segunda área de memoria, que solo se puede alcanzar en el estado de funcionamiento, pueden estar almacenados todos los secretos de cifrado que son necesarios para funciones ampliadas que exceden de las funciones que son necesarias en el estado inicial.

Según un ejemplo de realización se propone que en la primera área de memoria esté almacenada una clave pública del ordenador central. En la segunda área de memoria, que solo se puede leer en el estado de funcionamiento, están almacenadas preferiblemente claves privadas, así como públicas del propio módulo de cifrado. Además pueden estar almacenadas otras claves públicas del ordenador central, que se utilizan por ejemplo para el cifrado de datos de usuario o para el cifrado de canales de comunicación. Además, en la segunda área de memoria pueden estar almacenados los certificados y las claves de los participantes de la comunicación de confianza, que en el estado de funcionamiento pueden tener acceso al módulo de cifrado y a los aparatos conectados al mismo.

Según un ejemplo de realización se propone que el módulo de cifrado sea un módulo SIM. Un módulo SIM es un denominado módulo de identidad de suscriptor. Con este módulo de identidad de suscriptor se pueden identificar unívocamente los miembros en la red de telefonía móvil. El módulo SIM dispone de todas las funcionalidades necesarias para en una red de telefonía móvil notificar a un miembro y poder establecer conexiones de voz y datos. Las funciones de cifrado que son necesarias en la red de telefonía móvil están igualmente almacenadas en el módulo SIM. Además, el módulo SIM puede incluir una memoria adicional y un área de criptografía en la que están

almacenadas las funcionalidades del módulo de cifrado. Por tanto, el módulo SIM se puede utilizar de una manera particularmente simple, por un lado, para establecer la comunicación de datos entre el aparato de comunicación y una red de área amplia y, por otro lado, para las funcionalidades de cifrado del módulo de cifrado.

Precisamente, el uso de un módulo SIM es particularmente ventajoso, ya que este puede ser insertado de una manera particularmente simple en una ranura de inserción convencional prevista para ello. El acceso al módulo SIM está igualmente estandarizado. Por tanto, el acceso al módulo de cifrado es posible por métodos convencionales y el módulo de cifrado se puede retirar del aparato de comunicación de forma no destructiva. Preferiblemente, el aparato de comunicación tiene ya incorporada una ranura de inserción para un módulo SIM.

Según un ejemplo de realización se propone que el módulo de cifrado cambie al estado inicial después de un estado sin corriente. De este modo se asegura que cada vez que el módulo de cifrado se haya quedado sin tensión, se adopte el estado inicial y, por tanto, se evite un ataque a un módulo de cifrado ya desconectado. En particular, después de la extracción del módulo de cifrado del aparato de comunicación, este cambia al estado inicial y en primer lugar debe autenticarse con respecto al ordenador central.

De acuerdo con un ejemplo de realización se propone que el módulo de cifrado genere un segundo valor aleatorio después de una verificación positiva de la firma a través del valor aleatorio. Con este segundo valor aleatorio es posible por ejemplo verificar si el módulo de cifrado está realmente conectado al contador de energía correcto. La creación del segundo valor aleatorio puede ser idéntica a la creación del primer valor aleatorio.

Según un ejemplo de realización se propone que se envíe igualmente el segundo valor aleatorio. La creación del segundo valor aleatorio y la emisión del segundo valor aleatorio pueden estar habilitadas en un estado inicial ampliado. El estado inicial ampliado puede ser, por ejemplo, un estado que está entre el estado inicial y el estado de funcionamiento. Después de que el módulo de cifrado en el estado inicial ha realizado una autenticación con el ordenador central, normalmente cambia al estado de funcionamiento. Sin embargo, también es posible que se realice un cambio en el estado inicial ampliado comprobando en primer lugar si el módulo de cifrado también está conectado al contador de energía correcto. En este estado inicial ampliado se pueden alcanzar las funciones del estado inicial, así como otras funciones, que incluyen en particular la creación de un segundo valor aleatorio y la verificación de una firma a través del segundo valor aleatorio con la clave pública de un contador de energía. Asimismo es posible que el módulo de cifrado tenga acceso a la clave pública de un contador de energía.

Por esta razón se propone, de acuerdo con un ejemplo de realización, que el módulo de cifrado preferiblemente en el estado inicial o en el estado inicial ampliado permita un acceso a una verificación de una firma creada con una clave privada del contador de energía a través de un valor aleatorio, de modo que en particular permita un acceso a la clave pública del contador de energía.

Según un ejemplo de realización se propone que el módulo de cifrado en el estado de funcionamiento supervise a intervalos una conexión con el ordenador central y/o el contador de energía. Esta seguridad ampliada evita que el módulo de cifrado pueda ser espiado mientras que está en el estado de funcionamiento. Tan pronto como el módulo de cifrado determina que ya no está en conexión de comunicación con el ordenador central y/o el contador de energía, este puede volver al estado inicial y un ataque se hace más difícil. La verificación de la conexión al contador de energía se puede realizar a una frecuencia que es más alta que la frecuencia de la verificación de la conexión al ordenador central.

De acuerdo con un ejemplo de realización se propone que el módulo de cifrado transmita al ordenador central al menos un valor del grupo de datos de posición, datos de identificación del contador de energía, datos del libro de registro del contador de energía, lectura de contador del contador de energía, datos del libro de registro del ordenador de control, al menos después del cambio del estado inicial al estado de funcionamiento. Estos datos pueden ser leídos después del cambio al estado de funcionamiento en primer lugar por el contador de energía. A continuación, estos datos pueden ser cifrados con la clave pública del ordenador central en el módulo de cifrado. Los datos leídos del contador de energía pueden haber sido previamente firmados por el contador de energía. Los datos firmados y cifrados pueden ser transmitidos desde el módulo de cifrado a través del aparato de comunicación al ordenador central. En el ordenador central, en primer lugar se puede verificar la autenticidad de los valores recibidos y descifrados verificando la firma del contador de energía. Posteriormente, los valores recibidos pueden ser comparados con los valores almacenados en el ordenador central. Los últimos valores almacenados se pueden comparar con los valores recibidos y, en particular, en los datos de posición y datos de identificación preferiblemente no deben haber tenido lugar variaciones. En los datos del libro de registro y las lecturas del contador solo se permite una variación para las entradas más recientes. Con ayuda de la comparación de los datos recibidos desde del módulo de cifrado y los datos almacenados en el ordenador central, es posible determinar si el módulo de cifrado está realmente conectado al contador de energía correcto. Además, se puede verificar si el módulo de cifrado está conectado al aparato de comunicación correcto. Finalmente, también se puede verificar si el módulo de cifrado está dispuesto en la posición correcta. Debido al hecho de que el contador de energía puede firmar sus datos de identificación, así como la lectura de su contador y los datos del libro de registro, la manipulación de estos datos se dificulta aún más.

Según un ejemplo de realización, se propone que el contador de energía sea un amperímetro, en particular un medidor inteligente. En particular, el medidor inteligente está dispuesto en una estación de carga para vehículos eléctricos.

Dentro de la estación de carga está dispuesto preferiblemente un aparato de control de carga, en el que está dispuesto el aparato de comunicación. Dentro del aparato de comunicación puede estar prevista una ranura de inserción para recibir el módulo de cifrado. Este es preferiblemente un criptochip extraíble, que en particular es una tarjeta SIM.

Otro aspecto es un procedimiento para la seguridad de un contador de energía que comprende la operación de un módulo de cifrado dispuesto en un aparato de comunicación extraíble de forma no destructiva en un estado inicial, la generación de un valor aleatorio en el módulo de cifrado, de modo que el módulo de cifrado en el estado inicial solo permita un acceso limitado a su función de cifrado.

Los procedimientos antes mencionados también pueden realizarse como un programa informático o como un programa informático almacenado en un medio de almacenamiento. En este caso, un microprocesador para llevar a cabo las etapas del procedimiento respectivas puede estar programado adecuadamente por un programa informático en el lado del módulo de cifrado y/o en el lado del ordenador central.

Las características de los procedimientos y dispositivos se pueden combinar libremente entre sí. En particular, las características y características parciales de la descripción y/o de las reivindicaciones dependientes e independientes, incluso en caso de elusión total o parcial de las características o características parciales de las reivindicaciones independientes, solas o combinadas libremente entre sí, pertenecen a la invención.

A continuación se explicará más detalladamente el objeto con referencia a un dibujo que muestra ejemplos de realización. En el dibujo muestran:

Figura 1: una topología de un sistema de seguridad de contador de energía;

Figura 2 una estructura esquemática de un módulo de cifrado;

Figura 3: un diagrama de estado de un módulo de cifrado;

Figura 4: una secuencia de mensajes para la autenticación de un ordenador central con respecto al módulo de cifrado;

Figura 5: una secuencia de mensajes para la autenticación de un contador de energía con respecto al módulo de cifrado; y

Figura 6: una secuencia de mensajes para confirmar con respecto a un ordenador central que el módulo de cifrado está conectado a un contador de energía autenticado.

En la Figura 1 está representado un sistema con una red local de puntos de medición 2. En la red local de puntos de medición 2 está dispuesta una pluralidad de contadores de energía 4, que en el ejemplo mostrado son preferiblemente medidores inteligentes para el registro de corriente eléctrica. Los contadores de energía 4 están conectados a un aparato de comunicación 6. El aparato de comunicación 6 también se entiende como una puerta de enlace, ya que representa una interfaz entre la red de puntos de medición 2 y una red de área amplia 8. El aparato de comunicación 6 dispone preferiblemente de funcionalidades de enrutamiento y puede comunicarse con la red de área amplia 8 , por ejemplo a través de radiotelefonía móvil, en particular GSM, GPRS, UMTS, LTE o comunicaciones por radio similares.

En la red de área amplia 8 pueden estar previstos ordenadores centrales 10, un ordenador central 10 puede ser en particular un ordenador central 10 de un operador de puntos de medición. No obstante, un ordenador central 10 también puede ser una central de facturación. Preferiblemente, un ordenador central 10 es un ordenador autorizado al que está permitido el acceso al contador de energía 4.

Además, en la figura 1 se puede reconocer que el aparato de comunicación 6 también proporciona una interfaz entre una red de domótica 12 y la red de área amplia 8. En la red de domótica 12 hay preferiblemente varios dispositivos locales 14, que por ejemplo son dispositivos de generación de energía, estaciones de carga para vehículos eléctricos o similares. Estos dispositivos locales 14 pueden comunicarse igualmente a través del aparato de comunicación 6 con la red de área amplia 8 o el ordenador central 10 dispuesto en ella.

El acceso al contador de energía 4 es crítico para la seguridad. A este respecto, debe garantizarse que por la red de área amplia 8 solo ordenadores centrales autorizados 10 puedan acceder a los contadores de energía 4 o los datos contenidos en ellos a través del aparato de comunicación 6. Además, debe garantizarse que el aparato de comunicación 6 solo se comunica por fuera con aquellos ordenadores centrales 10 que están autorizados. Por esta razón se propone el concepto de protección, como se explicó al principio. Este concepto de protección prevé que esté dispuesto un módulo de cifrado 16 dentro del aparato de comunicación 6. El módulo de cifrado 16 proporciona las funcionalidades de cifrado para el aparato de comunicación 6.

Como tal, el aparato de comunicación 6 puede ser transparente para la comunicación entre el módulo de cifrado 16 y el ordenador central 10. También el aparato de comunicación 6 para la comunicación entre el módulo de cifrado 16 y los respectivos contadores de energía 4 puede ser transparente. El aparato de comunicación 6 proporciona preferiblemente las interfaces de comunicación que son necesarias para la comunicación entre el módulo de cifrado 16 y la red de área amplia 8 o la red de puntos de medición 2.

La Figura 2 muestra un módulo de cifrado 16, que está diseñado preferiblemente como módulo de identidad de suscriptor (SIM) y, además de las funcionalidades necesarias para la comunicación por telefonía móvil, a través de una interfaz 16a, proporciona otras funcionalidades criptográficamente relevantes. Para este propósito, el módulo de cifrado 16a tiene un microprocesador 16b que puede acceder a una memoria 16c con dos áreas de memoria 16c' y 16c".

Finalmente, en el módulo de cifrado 16 está prevista una memoria de programa 16d, en la que están almacenadas las instrucciones de programa para el microprocesador. Con la ayuda de estas instrucciones de programa es posible operar el módulo de cifrado 16 de acuerdo con el objeto. En particular, es posible operar el microprocesador 16b del módulo de cifrado 16 de tal manera que en un estado inicial solo sea posible el acceso a funciones limitadas.

En particular, en el estado inicial solo es posible el acceso al área de memoria 16c' y no al área de memoria 16c". En el área de memoria 16c' está almacenada preferiblemente una clave pública de un ordenador central 10. Con la ayuda de esta clave pública, es posible verificar la autenticidad de un mensaje firmado por el ordenador central 10. Otra funcionalidad que está disponible para el microprocesador 16b en el estado inicial es la creación de un valor aleatorio, por ejemplo un valor aleatorio alfanumérico o un número aleatorio. Este valor aleatorio también puede ser pseudoaleatorio, siendo medido un valor de resistencia que depende de la temperatura. Este ruido dependiente de la temperatura del valor de la resistencia es pseudoaleatorio y, por tanto, lo suficientemente seguro para el procedimiento descrito.

En el área de memoria 16c pueden estar almacenadas otras claves privadas y públicas de diferentes miembros del mercado, así como del ordenador central 10, los contadores de energía 4, así como del propio módulo de cifrado 16.

La Figura 3 muestra un diagrama de estado de un módulo de cifrado 16. El módulo de cifrado 16 puede tener un estado de partida 18. Desde el estado de partida 18, el módulo de cifrado puede cambiar al estado inicial 20 por aporte de energía.

En el estado inicial 20, el módulo de cifrado 16 puede realizar funciones limitadas. Estas incluyen recibir un comando 22 para la generación de un valor aleatorio. En respuesta a este comando 22, el módulo de cifrado 16 cambia al estado de espera 24, en el que en primer lugar envía el valor aleatorio generado y luego espera la recepción de un valor aleatorio firmado por el ordenador central 10. En el estado de espera 24 está en marcha un temporizador, que mide una duración hasta la recepción de una firma. Cuando ha expirado 26 el temporizador, el módulo de cifrado 16 cambia al estado de error 28. También cuando recibe una firma no válida, el módulo de cifrado 16 cambia al estado 28.

Esto puede significar que en el estado de espera 24, no solo se espera la recepción del valor aleatorio firmado, sino que también se verifica la validez de una firma recibida. Esto puede suceder de modo que el módulo de cifrado 16 accede a la clave pública del ordenador central 10 almacenada en el área de memoria 16c' y, utilizando esta clave, así como el valor aleatorio creado en el módulo de cifrado 16 y por tanto allí conocido, puede verificar la firma del ordenador central a través del valor aleatorio. Si la firma generada es errónea, entonces se cambia al estado de error 28.

Tan pronto como el módulo de cifrado 16 ha cambiado al estado de error 28, se pone en marcha en primer lugar otro temporizador, lo que provoca un tiempo muerto del módulo de cifrado 16. Durante este tiempo el módulo de cifrado no funciona. La duración del temporizador puede depender del número de intentos fallidos, es decir, de la frecuencia con la que el módulo de cifrado ha cambiado al estado de error 28. La duración puede crecer exponencialmente, de modo que el tiempo de bloqueo aumenta en un factor con cada intento fallido. Solo después de la expiración del período de bloqueo, el módulo de cifrado 16 cambia (30) de nuevo al estado inicial 20.

Además, un contador de errores puede incrementarse y si el contador de errores excede de un valor límite en el estado de error, el módulo de cifrado 16 puede cambiar (34) a un modo de reinicio 32.

En el modo de reinicio 32 se pueden intercambiar nuevos pares de claves con el ordenador central 10. También es posible que sean almacenadas todas las claves y/o certificados almacenados en el módulo de cifrado 16 o en las memorias 16c' y 16c". También se puede iniciar un proceso de emparejamiento con el ordenador central 10 conocido en sí, en el cual utilizando por última vez la clave existente se intercambian nuevos pares de claves y certificados. Después de que se haya realizado un emparejamiento, puede tener lugar por ejemplo un cambio (36) en el estado inicial 32.

En el estado inicial 20, el módulo de cifrado 16 puede además recibir un comando externo para generar nuevas claves, después de lo cual cambia (38) igualmente al modo de reinicio 32.

En el estado de espera 24, como ya se mencionó, el módulo de cifrado 16 puede realizar una verificación de una firma a través del valor aleatorio utilizando la clave pública del ordenador central 10 almacenada en la memoria 16c. Si en esta verificación se constata que el ordenador central correcto 10 ha firmado el valor aleatorio proporcionado por el módulo de cifrado 16, el módulo de cifrado 16 cambia (40) a un estado de funcionamiento 42. En el estado de funcionamiento 42 están liberados entre otros el acceso al área de memoria 16c", así como activadas diversas funcionalidades del microprocesador 16b. Entre otras, estas funcionalidades son el cifrado y la firma de la informaciones, en particular el cifrado y la firma de lecturas de contador de aparatos de medición del contador de

energía 4. Además, una funcionalidad, la verificación de firmas del contador de energía 4 para monitorizar que el módulo de cifrado 16 continúa conectado al contador de energía correcto 4.

Durante el estado de funcionamiento 42 se verifica a intervalos, preferiblemente a intervalos regulares, preferiblemente a intervalos constantes, si el módulo de cifrado 16 está en conexión de comunicación con el ordenador central 10. Esto se puede hacer mediante el intercambio de valores aleatorios y firmas para garantizar que también el ordenador central correcto 10 esté disponible como participante en la comunicación.

Preferiblemente, a intervalos más cortos se puede verificar si el módulo de cifrado 16 está conectado al aparato de comunicación 6. Esto también se puede realizar mediante el intercambio de firmas y claves.

Durante el estado de funcionamiento 42, el módulo de cifrado 16 garantiza el intercambio seguro y autenticado de informaciones entre el ordenador central 10 y los contadores de energía 4 a través del aparato de comunicación 6. Por tanto, el módulo de cifrado 16 dispone de la posibilidad de intercambiar datos relevantes para la facturación entre el contador de energía 4 y el ordenador central 10.

Si el módulo de comunicación 16 en el estado de funcionamiento 42 determina que ya no está en conexión de comunicación con el ordenador central 10 o un contador de energía determinado 4 o el aparato de comunicación 6, puede cambiar (44) al estado inicial 20. Por tanto está garantizado que durante el estado de funcionamiento 42, el módulo de cifrado 16 siempre se encuentra en el entorno que conoce y, en caso de un error en el entorno o la retirada del módulo de cifrado 16 del entorno, este cambia al estado inicial 20 y ya no es posible el acceso a otras funcionalidades. Esto evita de forma fiable una manipulación de los datos relevantes para la facturación transmitidos por los contadores de energía 4, ya que estos solo pueden ser procesados correctamente por el módulo de cifrado 16 si este permanece asegurado en el entorno conocido por él.

La Figura 4 muestra la secuencia de un proceso de desconexión, tal como ocurre cuando el módulo de cifrado 16 cambia del estado inicial 20 al estado de funcionamiento 42. Aquí está representada esquemáticamente la secuencia de mensajes entre el aparato de comunicación 6, el contador de energía 4, el módulo de cifrado 16 y el ordenador central 10.

En el estado inicial 20, el módulo de cifrado 16 puede recibir del aparato de control 6 un requerimiento 50 para la generación de un valor aleatorio. Después de esto, el módulo de cifrado 16 en el estado inicial 20 crea el valor aleatorio A, que preferiblemente es un valor aleatorio alfanumérico. Este valor aleatorio A también puede ser un valor binario.

Posteriormente, el módulo de cifrado 16 envía el valor aleatorio A generado al aparato de comunicación 6.

El aparato de comunicación 6 dirige el valor aleatorio A de forma transparente al ordenador central 10.

En el ordenador central 10 se crea una firma S1 a través del valor aleatorio A con la clave privada PrGWA del ordenador central 10. Esta firma S1 es transmitida desde el ordenador central 10 de vuelta al aparato de comunicación 6.

El aparato de comunicación 6 reenvía la firma S1 de forma transparente al módulo de cifrado 16, que ahora se encuentra en el estado de espera 24.

En el estado de espera 24, el módulo de cifrado 16 recibe la firma S1 y accede a la clave pública PubGWA del ordenador central 10 que está almacenada en el área de memoria 16c'. Con la ayuda de la clave pública PubGWA se realiza una verificación de la firma S1 junto con el valor aleatorio A conocido en el módulo de cifrado 16. En caso de una verificación correcta, el módulo de cifrado 16 cambia al estado de funcionamiento 42 y notifica (52) esto al aparato de comunicación 6. En caso de error, el módulo de cifrado 16 cambia al estado de error 28.

La Figura 5 muestra una secuencia de otro sistema de seguridad del módulo de cifrado 16 antes de que cambie al estado de funcionamiento 42.

Por ejemplo, es posible que después de una verificación positiva de la firma S1 y la notificación (52) al aparato de comunicación 6, el módulo de cifrado 16 no cambie inmediatamente al estado de funcionamiento 42, sino que adopte un estado intermedio. En este estado intermedio, el módulo de cifrado 16 transmite otro valor aleatorio B al aparato de comunicación 6. El aparato de comunicación 6 transmite este valor aleatorio B al contador de energía 4 de forma transparente.

En el contador de energía 4 es calculada una firma S2 a través del valor aleatorio B con una clave privada PrZ. La firma S2 es transmitida desde el contador 4 a través del aparato de comunicación 6 al módulo de cifrado 16. En el módulo de cifrado 16 se libera el acceso a una clave pública PubZ del contador de energía 4 en el estado intermedio. Con la ayuda de esta clave es posible una verificación de la firma S2 a través del valor aleatorio B. Si la verificación es positiva, esto se notifica (54) al aparato de comunicación 6 y el módulo de cifrado 16 cambia al estado de funcionamiento 42.

La Figura 6 muestra otra secuencia de un procedimiento en el que el ordenador central 10 puede verificar si el módulo de cifrado 16 está en el alcance de la comunicación.

Para ello, el ordenador central 10 transmite un valor aleatorio C de forma transparente a través del aparato de control 6 a un contador de energía 4. En el contador de energía 4 se crea una firma S3 a través del valor aleatorio C con la clave privada PrZ del contador de energía 4.

La firma S3 se transmite de forma transparente a través del aparato de comunicación 6 en primer lugar al módulo de cifrado 16. En el módulo de cifrado 16 en primer lugar se realiza en primer lugar una verificación de la firma S3. Para ello, el módulo de cifrado 16 ha recibido del aparato de control 6 igualmente el valor aleatorio C (no representado). Si la firma S3 es correcta, lo que se realiza con la ayuda de la clave pública PubZ del contador de energía 4, el módulo de cifrado 16 crea una firma S4 a través de la firma S3 con su clave privada PrV.

La firma S4, así como la firma S3, se transmiten a continuación de forma transparente a través del aparato de comunicación 6 al ordenador central 10. En el ordenador central 10, la firma S4 se puede verificar a través de la firma S3 usando la clave pública PubV del módulo de cifrado 16. En caso de una verificación positiva, en el ordenador central 10 está garantizado que, por un lado, el módulo de comunicación 16 puede comunicarse con el ordenador central 10 a través del aparato de control 6. Además, se asegura que el módulo de cifrado 16 está conectado al contador de energía correcto 4, ya que de lo contrario el módulo de cifrado 16 no habría creado la firma S4. Esto asegura que el módulo de cifrado 16 se encuentra en el entorno correcto, en particular conectado al contador de energía correcto 4 y puede cifrar y firmar sus informaciones y datos relevantes para la facturación para una comunicación con el ordenador central 10.

Con la ayuda del módulo de cifrado mostrado es posible cumplir un perfil de protección para puertas de enlace de medidores inteligentes sin que el módulo de cifrado tenga que estar firmemente anclado en el aparato de comunicación 6. Asimismo es posible prever un módulo de cifrado 16 en el aparato de comunicación 6 que pueda ser extraido de forma no destructiva, que está asegurado con respecto al mal uso por los procedimientos mostrados.

REIVINDICACIONES

1. Sistema de seguridad de contador de energía con

- un aparato de comunicación (6) que se puede conectar a un contador de energía (4),

- un módulo de cifrado (16) dispuesto en el aparato de comunicación (6) de modo que puede ser retirado de forma no destructiva,

- en el que el módulo de cifrado (16) en el estado inicial (20) permite un acceso limitado a sus funciones, y

- el módulo de cifrado (16) en el estado inicial (20) está diseñado para la emisión de un valor aleatorio,

caracterizado por que

- el módulo de cifrado (16) en el estado inicial (20) permite un acceso a una verificación de una firma creada a través del valor aleatorio con una clave privada de un ordenador central alejado espacialmente del aparato de comunicación (6), y

- por que el módulo de cifrado (16) en el estado inicial (20) tras una verificación positiva de la firma a través del valor aleatorio cambia a un estado de funcionamiento (42) en el que permite el acceso a otras funciones de cifrado.

2. Sistema de seguridad de contador de energía según la reivindicación 1, caracterizado por que el módulo de cifrado (16) está diseñado para en el estado inicial (20) recibir un requerimiento para la generación de un valor aleatorio y/o por que el módulo de cifrado (16) está diseñado para en el estado inicial (20) generar el valor aleatorio en respuesta a un requerimiento para la generación del valor aleatorio.

3. Sistema de seguridad de contador de energía según la reivindicación 1 o 2, caracterizado por que el módulo de cifrado (16) está diseñado para en el estado inicial (20) emitir una firma creada con una clave privada del módulo de cifrado (16) a través del valor aleatorio, y/o por que el módulo de cifrado (16) en el estado inicial (20) activa un contador después de la emisión del valor aleatorio para monitorizar la duración hasta que llega una respuesta a la emisión del valor aleatorio.

4. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el módulo de cifrado (16) en el estado inicial (20) permite un acceso a una verificación de una firma creada con una clave privada de un contador central alejado espacialmente del aparato de comunicación (6) a través del valor aleatorio, en el que se permite un acceso a una clave pública del contador central, y/o por que el módulo de cifrado (16) en el estado inicial (20) después de una verificación negativa de la firma a través del valor aleatorio permanece en el estado inicial (20) e incrementa un contador de errores.

5. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el módulo de cifrado (16) presenta dos áreas de memoria, de modo que en el estado inicial (20) es posible un acceso solo a la primera área de memoria y en el estado de funcionamiento (42) es posible un acceso a la primera y segunda áreas de memoria, y/o por que en la primera área de memoria está almacenada una clave pública del ordenador central.

6. Sistema de seguridad de contador de energía según la reivindicación 4, caracterizado por que en el estado inicial (20) cuando es sobrepasado un valor límite por el contador de errores el módulo de cifrado (16) borra sus áreas de memoria.

7. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el módulo de cifrado (16) es un módulo SIM.

8. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el módulo de cifrado (16) después de un estado sin corriente cambia al estado inicial (20).

9. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el módulo de cifrado (16) después de una verificación positiva de la firma a través del valor aleatorio crea un segundo valor aleatorio.

10. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el módulo de cifrado (16) emite el segundo valor aleatorio.

11. Sistema de seguridad de contador de energía según la reivindicación 10, caracterizado por que el módulo de cifrado (16) en el estado inicial (20) permite un acceso a una verificación de una firma creada con una clave privada del contador de energía (4) a través del segundo valor aleatorio, siendo posible así un acceso a una clave pública del contador de energía (4).

12. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el módulo de cifrado (16) en el estado de funcionamiento (42) monitoriza a intervalos una conexión con el ordenador central y/o el contador de energía (4).

13. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el módulo de cifrado (16) al menos después del cambio del estado inicial (20) al estado de funcionamiento (42) transmite al ordenador central al menos un valor del grupo:

- datos de posición,

- datos de identificación del contador de energía (4),

- datos del libro de registro del contador de energía (4),

- lectura del contador de energía (4),

- datos del libro de registro del aparato de comunicación (6).

14. Sistema de seguridad de contador de energía según una de las reivindicaciones anteriores, caracterizado por que el contador de energía (4) es un amperímetro, en particular un contador inteligente.

15. Procedimiento para la seguridad de un contador de energía (4) que comprende:

- operación de un módulo de cifrado (16) dispuesto en un aparato de comunicación (6) de forma que se puede retirar de forma no destructiva en un estado inicial (20),

- creación de un valor aleatorio en el módulo de cifrado (16),

- en el que el módulo de cifrado (16) en el estado inicial (20) solo permite un acceso limitado a sus funciones de cifrado,

caracterizado por que

- en el módulo de cifrado (16) en el estado inicial (20) es posible un acceso a una verificación a través del valor aleatorio de una firma creada con una clave privada de un ordenador central alejado espacialmente del aparato de comunicación (6), y

- por que el módulo de cifrado (16) en el estado inicial (20) después de una verificación positiva de la firma a través de valor aleatorio cambia a un estado de funcionamiento (42) en el que es posible un acceso a otras funciones de cifrado.

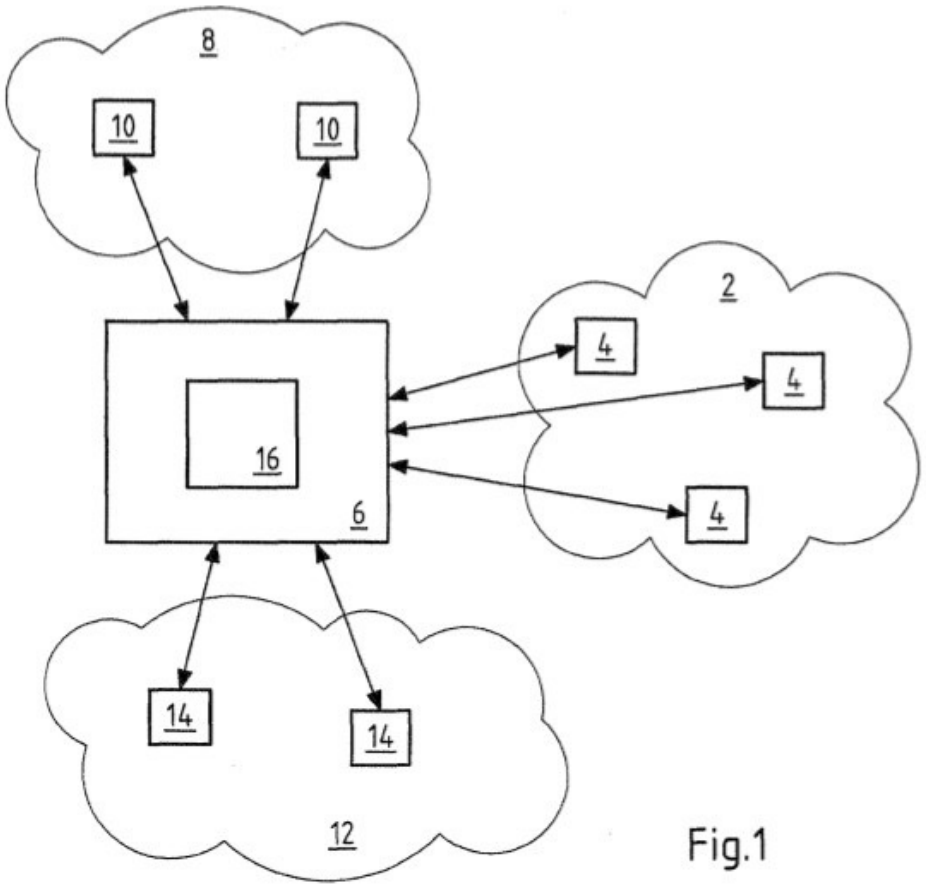

Fig.1

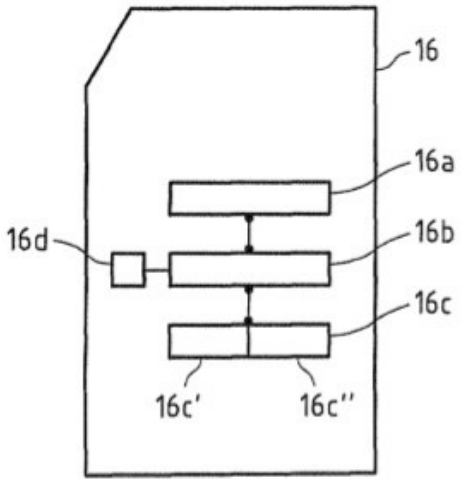

Fig.2

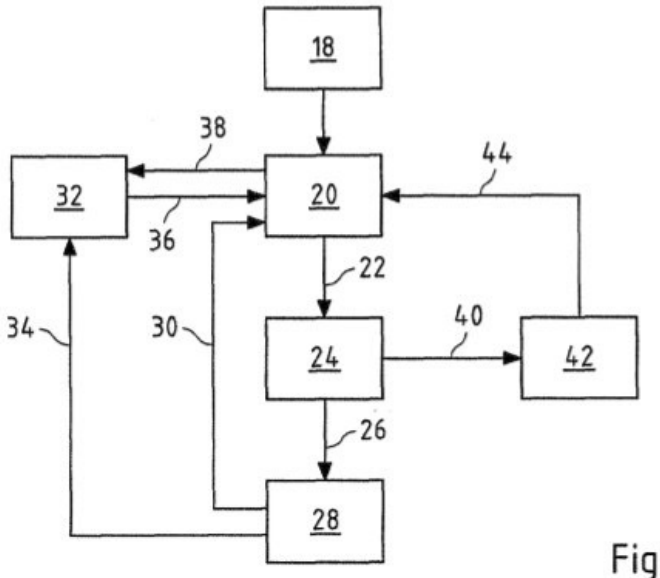
18
38
44
32
20
36
22
34
30
40
24
42
26
28

Fig.3

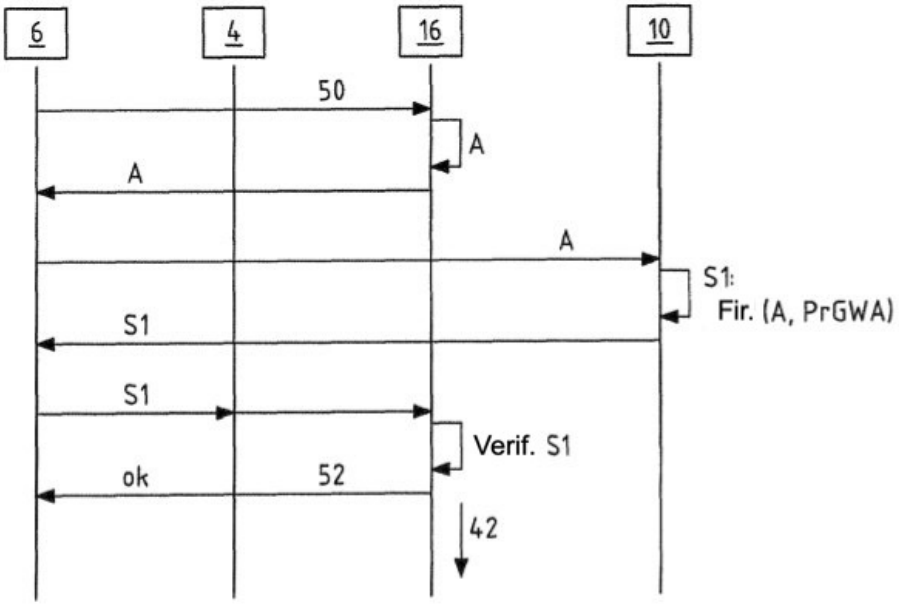
6
4
16
10
50
A
A
A
S1:
Fir. (A, PrGWA)
S1
S1
Verif. S1
ok
52
42

Fig.4

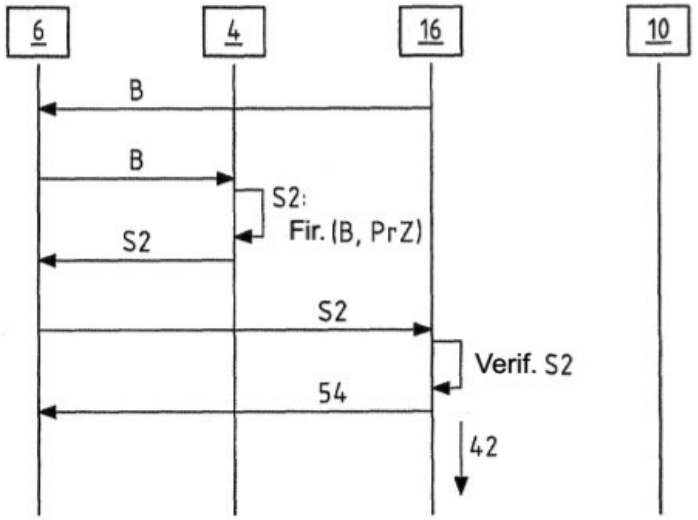
6
4
16
10
B
B
S2:
Fir. (B, PrZ)
S2
S2
Verif. S2
54
42

Fig.5

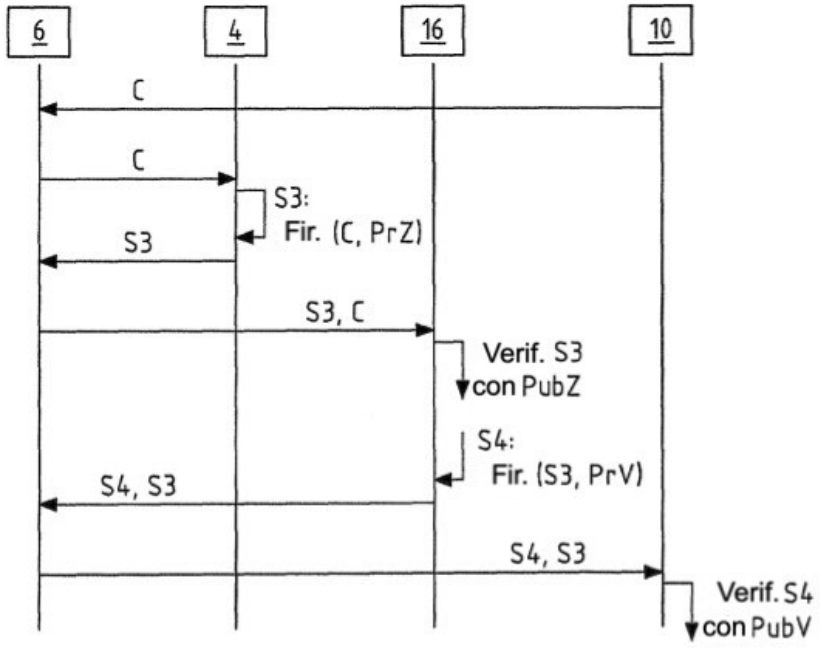
6
4
16
10
C
C
S3:
Fir. (C, PrZ)
S3
S3, C
Verif. S3
con PubZ
S4:
Fir. (S3, PrV)
S4, S3
S4, S3
Verif. S4
con PubV

Fig.6