(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 660**

(51) Int. CI.:

G06F 21/57 (2013.01)
G06F 21/44 (2013.01)
G06F 21/70 (2013.01)
G06Q 50/06 (2012.01)
H04W 4/20 (2008.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.01.2013 PCT/EP2013/050896**

(87) Fecha y número de publicación internacional: **15.08.2013 WO13117404**

(96) Fecha de presentación y número de la solicitud europea: **18.01.2013 E 13701946 (9)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 2812837**

(54) Título: **Procedimiento para personalizar un medidor inteligente o módulo de seguridad de compuerta de enlace del medidor inteligente**

(30) Prioridad:

07.02.2012 DE 102012201810
02.03.2012 DE 102012203354

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2019

(73) Titular/es:

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

(72) Inventor/es:

DIETRICH, FRANK y
PAESCHKE, MANFRED

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para personalizar un medidor inteligente o módulo de seguridad de compuerta de enlace del medidor inteligente

La invención se refiere a un procedimiento para personalizar un medidor inteligente o módulo de seguridad de compuerta de enlace del medidor inteligente, así como a un producto informático.

Por la expresión "medición inteligente" se entiende generalmente la idea de dotar a los clientes de aparatos electrónicos de detección de consumo de energía para poner a disposición otras funcionalidades además de una detección simple de la cantidad de energía consumida, por ejemplo a través de una red, tanto al cliente como al proveedor de energía.

Es posible a este respecto que el cliente pueda informarse en tiempo real sobre su consumo de energía actual. Por la expresión "consumo de energía" se entiende a este respecto el consumo del cliente con respecto a cualquier tipo de energía que se suministra a los hogares y empresas. Esto comprende además de las formas de energía electricidad, agua y gas también cualquier otra forma de energía, tal como la calefacción urbana.

Para detectar el consumo de energía, se usan por el consumidor respectivo sistemas de medición inteligentes, también llamados medidores inteligentes o "*smart-meter*". Los medidores inteligentes son medidores para la energía consumida. El consumidor puede ser a este respecto una persona física o jurídica, que consume distintas formas de energía medibles tales como la electricidad, gas, agua o calor. El objetivo del uso de medidores inteligentes es la implementación de sistemas de medición inteligentes, lo que posibilitaría, por ejemplo, la percepción de gastos por servicios variables dependiendo de la demanda total y la utilización de la red. De este modo, las redes de suministro de energía pueden ser mejor aprovechadas en general.

Por la directriz técnica del BSI TR-03109 se sabe cómo prever una denominada compuerta de enlace del medidor inteligente, también llamado concentrador, como unidad de comunicación central, que puede comunicarse con medidores inteligentes simples o múltiples. La compuerta de enlace es capaz de comunicarse con aparatos en la denominada "red de área doméstica" y con aparatos en la "red de área amplia". La red de área doméstica comprende a este respecto todos los medidores inteligentes que están acoplados a la compuerta de enlace, así como, por ejemplo, unidades de cálculo privadas de los consumidores. Las unidades de cálculo privadas se pueden usar, por ejemplo, para la información sobre valores de consumo de energía actuales detectados con los medidores inteligentes. La red de área amplia está configurada para posibilitar una comunicación entre la compuerta de enlace y los participantes del mercado autorizados. Por ejemplo, la compuerta de enlace puede recopilar los datos de todos los medidores inteligentes y ponerlos a disposición en un punto de recolección de nivel superior. por ejemplo, un proveedor de energía o un operador de puntos de medición.

BARRIGAL ET AL: "M2M Remote-Subscription Management", CITA DE INTERNET, lunes, 2 de mayo de 2011, páginas 1-6, describe los módulos de identidad de comunicación máquina a máquina (M2M) y su aplicación. En particular, se describen las posibilidades para el mantenimiento remoto de tales módulos.

"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment (Release 9)", 3GPP STANDARD; 3GPP TR 33.812, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA-ANTIPOLIS CEDEX; FRANCE, n.º V9.2.0, 22 de junio de 2010, páginas 1-87, describe aspectos de seguridad y posibilidades para el mantenimiento remoto de dispositivos M2M.

"ETSI TS 102 689 V1.1.1 Machine-to-Machine Communications (M2M); M2M Service requirements", 3 de agosto de 2010, describe requisitos para servicios M2M como directriz técnica del Instituto Europeo de Normas de Telecomunicaciones. "ETSI TS 102 690 V1.1.1 Machine-to-Machine Communications (M2M); Functional architecture", sábado, 1 de octubre de 2011, describe requisitos para una arquitectura M2M como directriz técnica del Instituto Europeo de Normas de Telecomunicaciones. "ETSI TS 102 691 V1.1.1 Machine-to-Machine Communications (M2M); Smart Metering Use Cases", martes, 18 de mayo de 2010, describe casos de aplicación para medidores inteligentes como directriz técnica del Instituto Europeo de Normas de Telecomunicaciones. "ETSI TS 122 022 V10.0.0 Digital cellular telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Personalisation of Mobile Equipment (ME); Mobile functionality specification", miércoles, 11 de mayo de 2011, describe especificaciones funcionales para personalizar aparatos móviles para sistemas GSM y 3G como directriz técnica del Instituto Europeo de Estándares de Telecomunicaciones.

El "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" describe el certificado X.509-v3 y la lista negra de certificado X.509-v2 para su uso en Internet.

El documento US 7 830 021 B1 describe un dispositivo semiconductor a prueba de manipulación, que comprende una superficie con contactos flip-chip eléctricos. Un semiconductor de flip-chip comprende un contacto flip-chip eléctrico. El semiconductor flip-chip tiene una temperatura máxima, a la que puede estar expuesto antes de ser dañado. Las juntas de soldadura flip-chip acoplan y conectan los contactos flip-chip eléctricos del semiconductor flip-chip

eléctricamente con los contactos flip-chip eléctricos de la superficie. Los puntos de soldadura flip-chip están formados a partir de una aleación, que presenta un punto de fusión más alto que la temperatura máxima, de tal modo que la eliminación del semiconductor flip-chip de la superficie por calentamiento destruye la funcionalidad de este semiconductor flip-chip.

El documento US 2007/138657 A1 describe una disposición de procesamiento físicamente segura, que contiene chips montados sobre un sustrato, para incrustar los contactos eléctricos de los chips entre los chips y el sustrato. El sustrato está dotado de contactos de sustrato y pistas conductoras, que están conectados eléctricamente a los contactos del chip y se extienden por el sustrato. Los conductores eléctricos rodean los caminos conductores. Un circuito de monitoreo detecta una interrupción de la continuidad de uno o más de los conductores eléctricos y hace que la disposición deje de funcionar.

Los objetos en los que se basa la invención se solucionan con las características de las reivindicaciones independientes. Las formas de realización preferentes de la invención están indicadas en las reivindicaciones dependientes.

Se indica un procedimiento para personalizar un módulo de seguridad de medidor inteligente o un módulo de seguridad de compuerta de enlace del medidor inteligente mediante un primer sistema informático, pudiendo detectarse mediante el medidor inteligente elementos de datos de medición específicos del consumo de energía, presentando el módulo de seguridad funciones criptográficas para realizar una comunicación cifrada criptográficamente de los elementos de datos de medición recibidos desde el medidor inteligente o la compuerta de enlace del medidor inteligente con un segundo sistema informático de un proveedor de energía y/u operador de puntos de medición, estando asociado al módulo de seguridad un identificador único, comprendiendo el procedimiento las etapas:

- proporcionar el módulo de seguridad,
- almacenamiento del identificador en el módulo de seguridad,
- generación de un par de claves criptográficas asimétricas por el primer sistema informático y almacenamiento del par de claves en el módulo de seguridad,
- firma de la clave pública del par de claves y el identificador para obtener un certificado y almacenar el certificado en el módulo de seguridad, efectuándose la firma mediante el primer sistema informático, estando configurado el módulo de seguridad de tal manera que, después del almacenamiento del par de claves, es posible un acceso de comunicación inicial al medidor inteligente y/o la compuerta de enlace del medidor inteligente exclusivamente para el primer sistema informático, pudiendo habilitarse mediante el acceso de comunicación inicial por el primer sistema informático el módulo de seguridad para la comunicación con el segundo sistema informático,
- instalación del módulo de seguridad en el medidor inteligente o en la compuerta de enlace del medidor inteligente, efectuándose debido a la instalación un proceso de enlace irreversible entre el módulo de seguridad y el medidor inteligente o la compuerta de enlace del medidor inteligente, iniciándose debido a la conexión del módulo de seguridad con el medidor inteligente o con la compuerta de enlace del medidor inteligente un proceso de vinculación
- sobre el medidor inteligente o la compuerta de enlace del medidor inteligente, produciéndose mediante el proceso de vinculación una vinculación lógica inseparable entre el módulo de seguridad y el medidor inteligente o la compuerta de enlace del medidor inteligente, comprendiendo la vinculación lógica inseparable un proceso de copia irreversible del certificado y/o el identificador inequívoco del módulo de seguridad en un área de almacenamiento del medidor inteligente o de la compuerta de enlace del medidor inteligente.

Las formas de realización de la invención podrían tener la ventaja de que mediante el proceso de inicialización puede proporcionarse de manera segura, inequívoca y comprensible una posibilidad, que posibilita una comunicación segura entre el medidor inteligente y un participante en el mercado autorizado, tal como un proveedor de energía o un operador de puntos de medición. Preferentemente se trata a este respecto en el caso del primer sistema informático de un sistema informático que posibilita un medidor inteligente confiable y un participante en el mercado autorizado, tal como un proveedor de energía o un operador de puntos de medición. Preferentemente se trata a este respecto en el caso del primer sistema informático de un sistema informático de una instancia confiable, que también se denomina "centro de confianza" o "administrador de servicios de confianza" o "TSM".

El módulo de seguridad está configurado en su estado inicializado de tal modo que exclusivamente esta instancia confiable del primer sistema informático es capaz de llevar a cabo una comunicación después de la autenticación exitosa con el módulo de seguridad. De este modo se garantiza que, por ejemplo, una configuración relevante para el pago de la medición inteligente se deja solo hasta tal punto que está clasificada como confiable tanto por los participantes en el mercado autorizados, es decir, por ejemplo, los operadores de partes de medición y los proveedores de energía reales, así como los consumidores finales. Por "configuración relevante para el pago" se entiende a continuación que mediante esta configuración con respecto a un medidor inteligente se establece, por ejemplo, quién tiene derecho a la facturación de las cantidades de energía detectadas por el medidor inteligente. Además, también

puede establecerse de este modo qué personas, como los usuarios finales y los participantes autorizados del mercado, pueden tener acceso a las funciones y a la información disponible en relación con el medidor inteligente y en qué medida. Dado que esta determinación se efectúa por parte de un punto confiable, de este modo se garantiza que se excluya un uso indebido de estas funciones e informaciones por parte de terceros no autorizados. Las informaciones pueden comprender a este respecto, por ejemplo, informaciones de ubicación del medidor inteligente, valores medidos por el medidor inteligente, informaciones de ubicación del área de almacenamiento o cualquier valor contenido en el área de almacenamiento.

En principio es irrelevante por quién se proporciona el módulo de seguridad, es decir, si en este caso se trata de una instancia confiable o no. Además, es en principio irrelevante si el proceso de almacenamiento real se realiza por una instancia confiable o no. El módulo de seguridad no presenta en su estado de entrega en caso de la facilitación del módulo de seguridad en primer lugar ningún material de clave. Una persona no autorizada no podría comenzar, por tanto, con el módulo de seguridad, dado que debido a la falta de certificados no se pueden realizar operaciones criptográficas autorizadas por el primer sistema informático. Únicamente cuando se almacena la clave privada del par de claves criptográficas asimétricas se tiene que asegurar que se efectúa de manera segura contra escuchas ilegales una comunicación necesaria para ello entre el módulo de seguridad y el primer sistema informático.

Incluso después de almacenar estos datos en el módulo de seguridad es esto inútil para personas no autorizadas, porque una comunicación con el módulo de seguridad solo la puede llevar a cabo el primer sistema informático, para, por ejemplo, reproducir o realizar dichas configuraciones.

De acuerdo con la invención, al módulo de seguridad está asociado un identificador único, comprendiendo el procedimiento además la etapa del almacenamiento del identificador en el módulo de seguridad, comprendiendo la firma una firma del identificador. Esto tiene la ventaja de que, por ejemplo, el módulo de seguridad y, con ello, el consumidor final, se puede identificar de manera inequívoca por medio del identificador más adelante durante la operación del módulo de seguridad para la transmisión de datos de consumo de energía a operadores de puntos de medición o proveedores de energía. Si se añade un enlace automático irreversible del módulo de seguridad al medidor inteligente y/o la compuerta de enlace con el uso del identificador, el medidor inteligente y/o la compuerta de enlace también se pueden identificar de manera inequívoca. La "simulación" de otro medidor inteligente o compuerta de enlace se evita con ello de manera confiable.

Por tanto, de acuerdo con otro ejemplo, el identificador de un área de almacenamiento, que está asociado al medidor inteligente directa o indirectamente a través de una compuerta de enlace, está proporcionado por un identificador del módulo de seguridad. De este modo está garantizado que el módulo de seguridad y el área de almacenamiento estén vinculados de manera inseparable. Un direccionamiento inequívoco del módulo de seguridad se corresponde con un direccionamiento inequívoco del área de almacenamiento. Si el área de almacenamiento se encuentra en una compuerta de enlace del medidor inteligente, de este modo está asegurado que posteriormente de manera no autorizada la compuerta de enlace no puede ser reemplazada por otra compuerta de enlace. Por ejemplo, esto podría evitar que a un operador de puntos de medición se pongan a disposición valores desde una compuerta de enlace "pirateada", que solo está conectada esporádicamente con medidores inteligentes correspondientes y, con ello, el primer sistema informático no puede describir exclusivamente a través del módulo de seguridad ningún área de almacenamiento de detección de consumo de energía real y el direccionamiento de esta área de almacenamiento es inequívoco debido al identificador. El uso de otra compuerta de enlace con un área de almacenamiento diferente sería por tanto imposible en principio en este caso, ya que una reproducción de los datos relevantes para la detección de energía por parte del primer sistema informático no tendría lugar nunca.

Según una forma de realización de la invención se trata en el caso del identificador del módulo de seguridad de una clave pública del módulo de seguridad o una dirección IPv6 del módulo de seguridad. El uso de la clave pública del módulo de seguridad como identificador del módulo de seguridad y, con ello, como identificador del área de almacenamiento tiene la ventaja de que se puede proporcionar de este modo un GUID (identificador único global), lo que es inequívoco con una probabilidad casi absoluta. Esto permitiría una fácil gestión de los identificadores asignando una clave pública más larga posible. En caso de que en el caso del identificador del módulo de seguridad se trate de una dirección IPv6, sería posible de una manera sencilla realizar un direccionamiento inequívoco del módulo de seguridad a través de redes existentes.

De acuerdo con una forma de realización adicional de la invención, el certificado incluye la clave pública del módulo de seguridad y el identificador. Esta clave pública está asociada a este respecto a una clave privada, que está almacenada en un área de almacenamiento protegida en el módulo de seguridad. El certificado puede haber sido creado según un estándar de infraestructura de clave pública (PKI), por ejemplo según el estándar X.509.

De acuerdo con la invención, el procedimiento comprende además la etapa de la instalación del módulo de seguridad en el medidor inteligente o la compuerta de enlace del medidor inteligente, efectuándose debido a la instalación un proceso de vinculación irreversible e inseparable entre el módulo de seguridad y el medidor inteligente o la compuerta de enlace del medidor inteligente. Por "inseparable" o "irreversible" se entiende a este respecto un enlace permanente entre el módulo de seguridad y el medidor inteligente o la compuerta de enlace del medidor inteligente, que garantiza una funcionalidad del módulo de seguridad. Una vez que se intenta retirar el módulo de seguridad del medidor inteligente o la compuerta de enlace del medidor inteligente, el módulo de seguridad pasa a un estado inutilizable, es

decir, no funcional. Esto puede estar garantizado mediante una autodestrucción electrónica, autodesactivación o destrucción física o desactivación del módulo de seguridad. En el caso más simple, el módulo de seguridad podría estar integrado en una carcasa del medidor inteligente o la compuerta de enlace del medidor inteligente, de modo que debido a la "ruptura" de esta conexión de conversión se dé como resultado la destrucción del módulo de seguridad.

Debido a la conexión del módulo de seguridad con el medidor inteligente o la compuerta de enlace del medidor inteligente se inicia un proceso de vinculación en el medidor inteligente o la compuerta de enlace del medidor inteligente. en el que el proceso de vinculación establece una vinculación lógica inseparable entre el módulo de seguridad y el medidor inteligente o la compuerta de enlace del medidor inteligente. Esta vinculación lógica inseparable comprende un proceso de copia irreversible del certificado y/o el identificador del módulo de seguridad en un área de almacenamiento asociada al medidor inteligente o a la compuerta de enlace.

De acuerdo con una realización de la invención, el primer sistema informático es parte de un primer equipo de automatización protegido y cerrado,

- efectuándose el almacenamiento del par de claves y/o del certificado y/o del identificador en el módulo de seguridad también en el primer equipo de automatización o
- efectuándose el almacenamiento del par de claves y/o del certificado y/o del identificador en el módulo de seguridad en un segundo equipo de automatización cerrado, transmitiéndose en este caso el par de claves criptográficas asimétricas y/o la firma y/o el identificador desde el primer equipo de automatización al segundo equipo de automatización a través de un enlace de comunicación cifrado.

Preferentemente se trata en el caso del primer equipo de automatización protegido y cerrado de un centro de confianza. El centro de confianza está definido a este respecto como una instancia confiable de la infraestructura de seguridad (PKI), que proporciona servicios de seguridad para usuarios y socios de comunicación. Un centro de confianza puede asumir en principio funciones de una autoridad de certificación o un centro de administración de claves. En el contexto de la presente descripción, no obstante, es decisivo que en el caso del primer equipo de automatización se trate de una colección de componentes, que realizan la generación del par de claves asimétricas y del certificado en un entorno de automatización protegido y espacialmente cerrado. Esto también significa que dentro del primer equipo de automatización los componentes interaccionan de una manera predefinida, se pueden supervisar y controlar de manera centralizada. Lo mismo se aplica a dicho segundo equipo de automatización cerrado. Por lo tanto, ambos equipos de automatización deben considerarse como separados o "separados espacialmente", dado que no hay opción de control central, que podría controlar los respectivos procesos de automatización en los dos equipos de automatización.

Según una forma de realización de la invención se efectúa la instalación del módulo de seguridad en el medidor inteligente o la compuerta de enlace del medidor inteligente dentro del segundo equipo de automatización. Por tanto, la instalación no tiene que efectuarse dentro del primer equipo de automatización o a través del primer equipo de automatización. Con ello, se puede preparar de una manera sencilla una pluralidad de módulos de seguridad mediante el almacenamiento de claves y certificados para vincularse de manera lógica con el hardware "medidor inteligente" o "compuerta de enlace del medidor inteligente" en cualquier momento posterior en cualquier lugar. No obstante, está garantizado que también esté asegurado en este momento posterior que una activación de una comunicación con el segundo sistema informático pueda efectuarse exclusivamente por el primer sistema informático.

Según una forma de realización de la invención, el módulo de seguridad se proporciona en forma de una tarjeta chip. Por tanto, el módulo de seguridad está preconfigurado en forma de tarjeta chip por el operador del primer sistema informático, almacenándose las respectivas informaciones en la tarjeta chip que hacen posible posibilitar una autenticación del primer sistema informático con respecto al módulo de seguridad para la ejecución posterior de un proceso de inicialización o proceso de activación.

Según una forma de realización de la invención, el módulo de seguridad proporcionado no está personalizado, efectuándose solo debido al almacenamiento del par de claves y/o del certificado en el módulo de seguridad una personalización del módulo de seguridad. El término "personalización" describe a este respecto la determinación inequívoca de características que hacen que el módulo de seguridad sea único y lo distinga de manera inequívoca de otros módulos de seguridad.

Según otra forma de realización de la invención, el procedimiento comprende además la etapa del almacenamiento de informaciones de contacto del primer sistema informático en el módulo de seguridad, efectuándose mediante las informaciones de contacto la determinación de la restricción del acceso de comunicación inicial exclusivamente al primer sistema informático. Por tanto, durante el proceso de almacenamiento, también se determina de manera inequívoca al mismo tiempo que el primer sistema informático está desbloqueado exclusivamente para el establecimiento inicial de contacto con el módulo de seguridad. Todos los demás sistemas informáticos están excluidos de dicho acceso inicial. Por ejemplo, en el módulo de seguridad podría estar almacenada como información un identificador inequívoco del primer sistema informático, como su nombre o su clave pública. El primer sistema informático puede autenticarse como "genuino" mediante, por ejemplo, su propio certificado en relación con el módulo de seguridad.

En otro aspecto, la invención se refiere a un producto de programa informático con instrucciones ejecutables de procesador para llevar a cabo las etapas de procedimiento descritas anteriormente.

A continuación se explican en más detalle formas de realización preferentes de la invención mediante los dibujos. Muestran:

la Figura 1 un diagrama de bloques de un sistema para implementar el procedimiento descrito anteriormente,

la Figura 2 un diagrama de bloques de un sistema para la comunicación de datos de medición desde medidores inteligentes,

la Figura 3 un diagrama de flujo de un procedimiento para inicializar un área de almacenamiento,

la Figura 4 un diagrama de flujo de un procedimiento para proporcionar un módulo de seguridad.

A continuación los elementos similares se denotarán con los mismos números de referencia.

La Figura 1 muestra un diagrama de bloques de una disposición de distintos equipos de automatización para personalizar módulos de seguridad. A continuación, solo se considera la variante del lado izquierdo de la Figura 1, en el que el módulo de seguridad 100 se personaliza completamente por el equipo de automatización 600.

El equipo de automatización 600 presenta una computadora 602, que posee módulos para la generación de claves 604 y firma 606. Por medio del módulo para la generación de claves 604, la computadora 602 puede generar pares de claves criptográficas asimétricas. Mediante el módulo 606 para la firma, la computadora 600 puede firmar la clave pública generada con el módulo 604, para generar con ello un certificado 104. Para ello, el módulo 606 puede cifrar la clave pública generada con una clave privada del equipo de automatización 600.

Después de la generación de los pares de claves, en particular la clave privada 106 se puede almacenar en una memoria 102 del módulo de seguridad 100, teniendo que asegurarse que a continuación ya no es posible un proceso de lectura de la clave privada 106 desde fuera del módulo de seguridad 100. Para ello, por ejemplo, en una etapa separada inmediatamente después del almacenamiento de la clave privada 106, el módulo de seguridad 100 "se completó".

El certificado 104 se almacena preferentemente en un servidor de directorio público 610 a través de la red 608. No obstante, también es posible almacenar el certificado directamente en la memoria 102.

Después de la personalización del módulo de seguridad 100, esto se puede instalar en una etapa de trabajo separada con un medidor inteligente o una compuerta de enlace del medidor inteligente 138. Esto no tiene que efectuarse dentro del equipo de automatización 600, sino que puede realizarse por ejemplo en el equipo de automatización 611. Mediante la instalación del módulo de seguridad 100 en la compuerta de enlace 138 se origina un proceso de enlace lógico irreversible y dado el caso también físico entre la compuerta de enlace y el módulo de seguridad. Esto se explicará en detalle a continuación.

Como alternativa al modo de proceder de personalización descrito hasta ahora, también es posible realizar en lugar de la personalización "*in situ*" en el equipo de automatización 600, la personalización a través de la red 608 en el equipo de automatización 611. Para ello está representado el módulo de seguridad 100 en líneas discontinuas en la Figura 1 en el lado derecho. En este caso todavía se efectúa igual que antes la generación del par de claves criptográficas asimétricas por la computadora 602. No obstante, se efectúa entonces una transmisión de la clave privada 106 al equipo de automatización 611 y, con ello, a la memoria 102 del módulo de seguridad 100 a través de una conexión de comunicación protegida criptográficamente usando la red 608.

Los dos equipos de automatización 600 y 611 están separados espacial y logísticamente entre sí. En el caso de ambos se trata de "instalaciones de automatización", dándose no obstante un control espacialmente completamente separado de los respectivos procesos de automatización.

Por ejemplo, el equipo de automatización 610 podría presentar una cadena de montaje con tarjetas chip suministradas, que suministra con el uso de un control central dentro del equipo de automatización 610 con un ciclo determinado las tarjetas chip individuales a un aparato de lectura/escritura de tarjetas chip. Las tarjetas chip son en este caso los elementos de seguridad. El aparato de lectura/escritura de la tarjeta chip lleva a cabo entonces las operaciones de escritura descritas anteriormente de la clave privada 106 y dado el caso del certificado 104 en la tarjeta chip. Finalmente, las tarjetas inteligentes personalizadas aún podrían empaquetarse y proporcionarse automáticamente para el envío.

Aparte de esto, el equipo de automatización 611 ofrece la posibilidad de desempaquetar con el uso de una unidad de control central, que funciona exclusivamente para el equipo de automatización 611, las tarjetas chip después de la recepción del envío e instalarlas en compuertas de enlace 138 correspondientes.

En el caso de los módulos de seguridad 100 descritos en el equipo de automatización 611, se reduce el ámbito de actividad del equipo de automatización 610 en la generación de claves y la transferencia de claves al equipo de

automatización 611. El equipo de automatización 611, al contrario, asume las funciones descritas anteriormente de la descripción de las tarjetas chip con estas claves.

La Figura 2 muestra un diagrama de bloques de un sistema general para inicializar un área de almacenamiento utilizando los módulos de seguridad 100 descritos con respecto a la Figura 1. Junto con las etapas de procedimiento mostradas en la Figura 3 para inicializar un área de almacenamiento se muestra a continuación sin la restricción de la generalidad cómo un área de almacenamiento 136 de una compuerta de enlace 138, que está asociada a una pluralidad de medidores inteligentes 142, 144, 146, 148, se puede inicializar.

Los medidores inteligentes 142-148 sirven a este respecto para detectar distintos valores de consumo de energía con respecto a, por ejemplo, el gas (medidor inteligente 142), agua (medidor inteligente 144), electricidad (medidor inteligente 146) y otras formas de energía no especificadas en más detalle (medidor inteligente 148). Los medidores inteligentes están conectados a este respecto a través de conexiones de comunicación correspondientes 192 con la interfaz 118 de la compuerta de enlace 138.

Se parte de que un módulo de seguridad 100 está conectado de manera fija e inseparable con la compuerta de enlace 138, de modo que en conjunto mediante la combinación de la compuerta de enlace 138 y el módulo de seguridad 100 se proporciona una unidad 140 inseparable. La compuerta de enlace 138 y el módulo de seguridad 100 se comunican entre sí a través de respectivas interfaces 118 y 116. A través de la interfaz 116 tiene lugar además una comunicación con participantes del mercado autorizados y terceros o instancias que no se encuentran dentro de la red formada por la unidad 140 y los medidores inteligentes 142-148. La comunicación entre la interfaz 116 del módulo de seguridad 100 y otros participantes de la comunicación se efectúa a este respecto a través de una conexión de comunicación 190. En este caso puede tratarse, por ejemplo, de una conexión de línea eléctrica o una conexión de comunicación a través de una red de telecomunicaciones móvil o Internet.

El módulo de seguridad 100 tiene la memoria 102 electrónica con área de almacenamiento 106 y 108 protegida. El área de almacenamiento 106 protegida sirve para almacenar una clave privada del módulo de seguridad 100 y el área de almacenamiento 108 sirve para almacenar un identificador del módulo de seguridad "GUID" (identificador único global). En el caso del GUID puede tratarse, por ejemplo, de una dirección IPv6 del módulo de seguridad 100. El GUID puede ser generado, por ejemplo, por el equipo de automatización 610 descrito en la Figura 1 y ser almacenado en el marco del procedimiento descrito anteriormente para almacenar la clave privada 106 en el módulo de seguridad. El proceso de almacenamiento real puede estar efectuado a este respecto o bien por parte del equipo de automatización 610 o bien por parte del equipo de automatización 611.

La memoria 102 electrónica puede presentar, además, el área de almacenamiento 104 para almacenar un certificado. El certificado contiene una clave pública, que está asociada a la clave privada almacenada en el área de almacenamiento 106 protegida. El certificado puede haber sido creado según un estándar de infraestructura de clave pública (PKI), por ejemplo según el estándar X.509.

El certificado no tiene que estar almacenado necesariamente con la memoria 102 electrónica del módulo de seguridad 100. Como alternativa o de manera adicional, el certificado también puede estar almacenado en un servidor de directorio público, véase la Figura 1.

El módulo de seguridad 100 tiene un procesador 110 para ejecutar instrucciones de programa 112 y 114. Mediante la ejecución de las instrucciones de programa 112 "protocolo criptográfico", por ejemplo, se hace posible una autenticación de una instancia confiable 150 o de un proveedor de energía 166 con respecto al módulo de seguridad 100. En el caso del protocolo criptográfico puede tratarse, por ejemplo, de un protocolo de desafío-respuesta basado en una clave simétrica o un par de claves asimétricas.

También es posible, por supuesto, una autenticación mutua del módulo de seguridad y la instancia confiable o el proveedor de energía.

Las instrucciones de programa 114 sirven para el cifrado de extremo a extremo de los datos que van a transmitirse entre el módulo de seguridad 100 y la instancia confiable 150 o el proveedor de energía 166. Para el cifrado de extremo a extremo se puede usar una clave simétrica, que, por ejemplo, se acordó con motivo de la ejecución del protocolo criptográfico entre el módulo de seguridad 100 y los otros participantes 150 o 166.

De manera similar al módulo de seguridad 100, la instancia confiable 150 también presenta una memoria 152 electrónica y un área de almacenamiento 156 protegida para almacenar una clave privada de la instancia confiable. En la memoria 152 también puede estar contenido un certificado 154 de la instancia confiable. No obstante, este certificado también se puede almacenar en un servidor de certificados central.

Un procesador 158 de la instancia confiable 150 presenta a su vez las instrucciones de programa 112 y 114 descritas anteriormente con respecto al módulo de seguridad 100 para implementar un protocolo criptográfico y llevar a cabo un cifrado de extremo a extremo. El protocolo criptográfico y el cifrado de extremo a extremo pueden usarse para la comunicación a través de la interfaz 164 con el proveedor de energía 166 o con el módulo de seguridad 100. El certificado 154 contiene a su vez una clave pública, que está asociada a la clave privada almacenada en el área de almacenamiento 156 protegida.

En el caso del "proveedor de energía" 166 se trata de un sistema informático del proveedor de energía, que a su vez presenta una memoria 168 electrónica y un procesador 178. Además, a este sistema informático se le asocia una interfaz 186, a través de la cual se posibilita una comunicación con la instancia confiable 150 o el módulo de seguridad.

La memoria 168 electrónica del proveedor de energía 166 presenta un área de almacenamiento 172 protegida con una clave privada, estando asociada a la clave privada una clave pública, que está contenida en un certificado 170 también en la memoria electrónica 168. Además, en la memoria 168 está prevista un área de almacenamiento para una o más aplicaciones, posibilitando estas aplicaciones por ejemplo una configuración relevante para el pago de la compuerta de enlace 138. También en la memoria 168 electrónica pueden estar almacenados datos de medición 176, los cuales se recibieron anteriormente por la compuerta de enlace 138.

El procesador 178 incluye instrucciones de programa 180 para detectar los datos de consumo proporcionados por la compuerta de enlace 138 y, opcionalmente, para ejecutar las etapas de procedimiento para la facturación por consumo en función de los datos de medición determinados (instrucciones de programa 182). También pueden estar previstas las instrucciones de programa para ejecutar etapas de un protocolo criptográfico 112, así como instrucciones de programa no mostradas para llevar a cabo un cifrado de extremo a extremo, posibilitándose mediante estas instrucciones de programa una comunicación segura con la instancia confiable 150 o el módulo de seguridad 100.

Si ahora se asocia un nuevo cliente al proveedor de energía 166, podría tener lugar, por ejemplo, después de una primera instalación del medidor inteligente 142-148 y la provisión de la compuerta de enlace 138 con módulo de seguridad 102, un proceso de inicialización del módulo de seguridad. Este proceso de inicialización podría ser desencadenado de tal modo que el nuevo cliente (un consumidor final) o una instancia técnica determinada que haya instalado el medidor inteligente proporciona al proveedor de energía 166 un mensaje correspondiente. Este mensaje debería comprender preferiblemente el GUID 108 del módulo de seguridad 100, dado que de este modo es posible una identificación inequívoca del módulo de seguridad 100 con respecto al proveedor de energía 166.

Después de que el proveedor de energía 166 haya recibido este mensaje a través de su interfaz 186, por ejemplo a través de una interfaz web de un sitio web correspondiente, el proveedor de energía 166 establece un canal de comunicación con respecto a la instancia confiable 150. Esta etapa se denomina en la Figura 3 con la referencia 200. La instancia confiable puede ser en este caso, por ejemplo, un denominado "*Trusted Service Manager* TSM", es decir, una instancia oficialmente certificada, que certifica la identidad respectiva del interlocutor en procesos de comunicación electrónicos.

Se parte a continuación de que el equipo de automatización 600 o su computadora 602 es en principio idéntico a la instancia confiable 150.

Tras el establecimiento del canal de comunicación en la etapa 200 se efectúa una autenticación del proveedor de energía 166 en la etapa 202. Para ello se comprueba el certificado 170 del proveedor de energía por la instancia confiable 150. Por ejemplo, la instancia confiable 150 puede llevar a cabo en caso de comprobación de certificado positiva un procedimiento de desafío-respuesta, en el que se genera un número aleatorio, que se cifra con una clave pública del proveedor de energía 166 contenida en el certificado 170 y se transmite al proveedor de energía 166. El proveedor de energía 166 puede descifrar después con su clave privada 172 el número aleatorio y enviarlo de vuelta en texto sin formato. Si el número aleatorio recibido ahora por la instancia confiable 150 coincide con el número aleatorio descrito anteriormente, la autenticidad del proveedor de energía 166 está realmente asegurada.

Tras llevar a cabo la etapa 202 y el procedimiento opcional de desafío-respuesta, se puede establecer después en la etapa 204 un canal con cifrado de extremo a extremo a través de la conexión de comunicación 188 entre suministro de energía 166 y la instancia confiable 150. En este caso, se pueden usar las instrucciones de programa 114 del procesador 158 de la instancia confiable.

Después de establecer el canal en la etapa 204, la instancia confiable 150 recibe en la etapa 206 una solicitud para la instalación de una aplicación de detección de energía 174 del proveedor de energía 166 y la memoria 136 de la compuerta de enlace 138. Para especificar de manera inequívoca la memoria 136 o la compuerta de enlace 138, con la solicitud de inicializar la memoria 136 también el GUID 128 de la compuerta de enlace 138, que está contenido en la memoria 136, se transmite a la instancia confiable. Preferentemente, el GUID 128 de la memoria 136 es idéntico al GUID 108 de la memoria 102 del módulo de seguridad 100.

Con la recepción del GUID en la etapa 206, la instancia confiable 150 es capaz de direccionar de manera inequívoca la compuerta de enlace 138 deseada para la instalación de la aplicación 174. Para ello, en la siguiente etapa 208, la instancia confiable 150 establece a través de la conexión de comunicación 190 un canal de comunicación al módulo de seguridad 100. La instancia confiable 150 se autentica con respecto al módulo de seguridad 100, comprendiendo la autenticación, además de una comprobación del certificado 154 por el módulo de seguridad, por ejemplo, a su vez un procedimiento de desafío-respuesta por parte del módulo de seguridad 100. Para ello, el módulo de seguridad 100 podría generar a su vez un número aleatorio, cifrar con la clave pública de la instancia confiable 150 y enviarla a la instancia confiable 150. La instancia confiable 150 descifraría el número aleatorio cifrado con su clave privada 156 y enviaría el número aleatorio descifrado de vuelta al módulo de seguridad 100 en texto sin formato. Si el módulo de seguridad determina que el número aleatorio descifrado así recibido coincide con el número aleatorio originalmente

cifrado por su parte, se le da una autenticación de la instancia confiable.

El procedimiento continúa entonces en la etapa 212, a saber, el establecimiento de un canal de comunicación con cifrado de extremo a extremo entre la instancia confiable 150 y el módulo de seguridad 100. Esto se puede efectuar a su vez usando las instrucciones de programa 114 del procesador 110 del módulo de seguridad 100.

En la etapa 214, el módulo de seguridad 100 recibe la aplicación de detección de energía 174 desde la instancia confiable.

En este punto cabe señalarse que puede ser ventajoso, por ejemplo, que la instancia confiable mantenga disponibles las aplicaciones de detección de energía enviadas con mayor frecuencia en una memoria local de la instancia confiable, de modo que no es necesario en el caso de apertura de nuevos clientes transmitir constantemente las aplicaciones 174 desde el proveedor de energía 166 a la instancia confiable 150.

Tras la recepción de la aplicación de detección de energía en la etapa 214, el módulo de seguridad 100 almacena la aplicación en la memoria 136 de la compuerta de enlace 138. En el caso de la aplicación 174 se trata, por ejemplo, de una aplicación para detectar el consumo de energía en términos de agua y electricidad, por lo que la aplicación se almacena como la aplicación 132 en la memoria 136. Esta aplicación es capaz de procesar datos de consumo de energía del medidor inteligente 144. De manera análoga a ello, la memoria 136 puede comprender aplicaciones correspondientes para la detección de gas (134) y otras aplicaciones 130 para la detección de otras formas de energía. El almacenamiento de la aplicación de detección de energía por el módulo de seguridad 100 en la compuerta de enlace 138 se indica en la Figura 2 mediante la etapa 216.

Adicionalmente a la recepción de la aplicación de detección de energía en la etapa 214 por el módulo de seguridad 100, también es posible que se reciban por la instancia confiable 150 autorizaciones específicas del proveedor de energía o especificaciones exactas de elementos de datos de red, que también se almacenan en un área 125 más amplia de la memoria 136. Estas autorizaciones o especificaciones de elementos de datos de medición hacen posible establecer por adelantado qué informaciones puede obtener en absoluto el proveedor de energía 166 desde la compuerta de enlace 138. Para ello es por ejemplo posible que de antemano se definan por la instancia confiable 150 autorizaciones específicas para cada proveedor de energía, que se aplican globalmente a todos los proveedores de energía 166 y que en principio se transmiten al módulo de seguridad y, con ello, a la compuerta de enlace 138 con la transmisión de aplicaciones de detección de energía.

También es posible que se obtengan datos de configuración de la instancia confiable 150. Estos datos de configuración pueden estar relacionados a este respecto con la configuración técnica del medidor inteligente y/o la compuerta de enlace.

Por medio de las instrucciones de programa para la detección de datos 122 del procesador 126, la compuerta de enlace 138 ahora es capaz de detectar datos de medición relacionados con un consumo de energía, por ejemplo, desde el medidor inteligente 144 y el medidor inteligente 146. Los datos de medición correspondientes se almacenan en el área de almacenamiento 124 de la memoria 136. Básicamente, los datos de medición 124 se componen de distintos elementos de datos de medición, que pueden comprender por ejemplo: momento de la detección de los datos de medición, puntos de datos de medición individuales en el momento respectivo, información sobre la realización de los datos de medición (por ejemplo, intensidad de la electricidad, voltaje, presión del agua, temperatura del agua, presión de gas). Los datos de medición 124 pueden someterse a una evaluación adicional a través de las aplicaciones 130, 132 y 134, de lo que resultan datos de medición evaluados, que también se puede almacenar como "elementos de datos de medición" en el área de almacenamiento 124. Por ejemplo, en el caso de los datos de medición evaluados puede tratarse de valores de consumo de energía acumulados.

Las autorizaciones 125 descritas anteriormente o las especificaciones de los elementos de datos de medición posibilitan establecer desde el principio a cuál de estos elementos de datos de medición 124 del proveedor de energía 126 puede consultar en absoluto. Además, esto posibilita establecer desde el principio cómo de detallada está permitida tal consulta. Una consulta detallada y oportuna de los datos de medición 124 podría ser indeseable a este respecto, dado que mediante intervalos de tiempo cortos de mediciones pueden obtenerse conocimientos del uso de aparatos electrónicos y de este modo elaborarse perfiles de usuario, sobre los que un cliente final, no obstante, podría no tener interés dado el caso.

Como ya se mencionó, preferentemente el módulo de seguridad 100 y la compuerta de acceso 138 están conectados entre sí de manera inseparable. Por ejemplo, estos forman una unidad estructural 140, como se muestra en la Figura 2. Para generar esta unidad 140, podrían llevarse a cabo las etapas de procedimiento explicadas en el diagrama de flujo de la Figura 4.

En la etapa 400 se proporciona en primer lugar el módulo de seguridad 100. A continuación se efectúa en la etapa 402 el almacenamiento de material de clave y/o de certificados en el módulo de seguridad. Por ejemplo para ello podría presentar el módulo de seguridad una unidad criptográfica correspondiente, por medio de la cual se genera automáticamente la clave privada 106. Como alternativa también es posible que la instancia confiable genere la clave privada y la almacene en el módulo de seguridad en un área de almacenamiento que no sea accesible desde el exterior. La clave pública que pertenece a la clave privada se adjunta al certificado, que luego se firma por la instancia

confiable y se almacena en la memoria 102 del módulo de seguridad o en un servidor de directorio público. Además, pueden almacenarse en la etapa 402 aún informaciones de contacto de la instancia confiable en el módulo de seguridad, efectuándose mediante las informaciones de contacto la determinación de la restricción del acceso de comunicación inicial exclusivamente a la instancia confiable. Es decir, exclusivamente la instancia confiable es capaz en una etapa de inicialización después de almacenar el material de clave en la etapa 402 de acceder con éxito al módulo de seguridad.

Después se inserta el módulo de seguridad en la compuerta de enlace en la etapa 404, por ejemplo en forma de una tarjeta chip, y se realiza una conexión inseparable entre el módulo de seguridad y la compuerta de enlace. Por ejemplo, el módulo de seguridad y la compuerta de enlace podrían estar acoplados electrónicamente entre sí de tal modo que una eliminación del módulo de seguridad de la compuerta de enlace conduciría a la destrucción automática del módulo de seguridad.

Después de la inserción del módulo de seguridad en la compuerta de enlace 404, en la etapa 406 se efectúa una vinculación lógica automática del módulo de seguridad 100 y la compuerta de enlace 138. Por ejemplo, esto podría efectuarse de tal modo que se escribe el GUID 108 del módulo de seguridad de manera irreversible en la memoria 136 de la compuerta de enlace 138 como GUID 128. En este caso, por parte por ejemplo del módulo de seguridad 100 debería asegurarse, por ejemplo, que solo tenga lugar una comunicación con la compuerta de enlace 138 para proporcionar elementos de datos de medición y a través del proveedor de energía 166, cuando se da una identidad de los GUID 108 y 128.

Ahora es posible, por ejemplo, después de la autenticación exitosa de la instancia confiable con respecto al módulo de seguridad, recibir datos de la instancia confiable a través del módulo de seguridad mediante una transmisión segura. Estos datos se pueden usar para inicializar un área de almacenamiento asociada a la compuerta de enlace mencionada anteriormente y para almacenar los datos en el área de almacenamiento. Solo basándose en los datos almacenados es posible ahora una comunicación de cualquier otro sistema informático de un proveedor de energía y/u operador de puntos de medición y el módulo de seguridad sin pasar por la instancia confiable. Los datos almacenados especifican a este respecto este otro sistema informático. Mediante los datos almacenados en el área de almacenamiento se desbloquea, por tanto, la comunicación con el otro sistema informático.

Lista de referencias

100 Módulo de seguridad

102 Memoria

104 Certificado

106 Clave privada

108 GUID

110 Procesador

112 Protocolo criptográfico

114 Cifrado de extremo a extremo

116 Interfaz

118 Interfaz

120 Transmisión de datos

122 Detección de datos

124 Datos de medición

125 Autorización

126 Procesador

128 GUID

130 Aplicación

132 Aplicación

134 Aplicación

136 Memoria
138 Memoria
140 Unidad
142 Medidor inteligente
144 Medidor inteligente
146 Medidor inteligente
148 Medidor inteligente
150 Instancia de fiabilidad
152 Memoria
154 Certificado
156 Clave privada
158 Procesador
164 Interfaz
166 Proveedor de energía
168 Memoria
170 Certificado
172 Clave privada
174 Aplicación
176 Datos de medición
178 Procesador
180 Detección de datos
182 Facturación por consumo
186 Interfaz
188 Conexión de comunicación
190 Conexión de comunicación
192 Conexión de comunicación
600 Equipo de automatización
602 Computadora
604 Módulo para la generación de claves
606 Modulo para la firma
608 Red
610 Servidor de directorio
611 Equipo de automatización

REIVINDICACIONES

1. Procedimiento para personalizar un medidor inteligente o un módulo de seguridad de compuerta de enlace del medidor inteligente (100) mediante un primer sistema informático (150), pudiendo detectarse mediante el medidor inteligente (142; 144; 146; 148) elementos de datos de medición específicos del consumo de energía, presentando el módulo de seguridad (100) funciones criptográficas para llevar a cabo una comunicación cifrada criptográficamente de los elementos de datos de medición recibidos por el medidor inteligente (142; 144; 146; 148) o la compuerta de enlace del medidor inteligente (138) con un segundo sistema informático (166) de un proveedor de energía y/u operador del punto de medición, estando asociado al módulo de seguridad (100) un identificador (128) inequívoco, comprendiendo el procedimiento las etapas:

- facilitación del módulo de seguridad (100),
- almacenamiento del identificador (128) en el módulo de seguridad (100),
- generación de un par de claves criptográficas asimétricas por el primer sistema informático y almacenamiento del par de claves en el módulo de seguridad (100),
- firma de la clave pública del par de claves y el identificador (128) para obtener un certificado y almacenamiento del certificado en el módulo de seguridad (100), efectuándose la firma mediante el primer sistema informático (150), estando configurado el módulo de seguridad (100) de tal manera que después del almacenamiento del par de claves es posible un acceso de comunicación inicial al medidor inteligente (142; 144; 146; 148) y/o la compuerta de enlace del medidor inteligente (138) exclusivamente para el primer sistema informático (150), pudiendo desbloquearse mediante el acceso de comunicación inicial por el primer sistema informático (150) el módulo de seguridad (100) para la comunicación con el segundo sistema informático (166),
- instalación del módulo de seguridad (100) en el medidor inteligente (142; 144; 146; 148) o la compuerta de enlace del medidor inteligente (138), efectuándose debido a la instalación un proceso de enlace irreversible entre el módulo de seguridad (100) y el medidor inteligente (142; 144; 146; 148) o la compuerta de enlace del medidor inteligente (138), iniciándose debido a la conexión del módulo de seguridad (100) con el medidor inteligente (142; 144; 146; 148) o la compuerta de enlace del medidor inteligente (138) un proceso de vinculación sobre el medidor inteligente (142; 144; 146; 148) o la compuerta de enlace del medidor inteligente (138), estableciéndose mediante el proceso de vinculación una vinculación lógica inseparable entre el módulo de seguridad (100) y el medidor inteligente (142; 144; 146; 148) o la compuerta de enlace del medidor inteligente (138), comprendiendo la vinculación lógica inseparable un proceso de copia irreversible del certificado y/o el identificador (128) inequívoco del módulo de seguridad (100) en un área de almacenamiento del medidor inteligente (142; 144; 146; 148) o de la compuerta de enlace del medidor inteligente (138).

2. Procedimiento según la reivindicación 1, conteniendo el certificado la clave pública del módulo de seguridad (100) y el identificador (128) inequívoco.

3. Procedimiento según la reivindicación 1 o 2, tratándose en el caso del identificador (128) del módulo de seguridad (100) de una clave pública del módulo de seguridad (100) o una dirección IPv6 del módulo de seguridad (100).

4. Procedimiento según una de las reivindicaciones anteriores, siendo el primer sistema informático parte de un primer equipo de automatización (600) protegido y cerrado,

- efectuándose el almacenamiento del par de claves y/o del certificado y/o del identificador (128) sobre el módulo de seguridad (100) también en el primer equipo de automatización (600) o
- efectuándose el almacenamiento del par de claves y/o del certificado y/o del identificador (128) sobre el módulo de seguridad (100) en un segundo equipo de automatización (611) cerrado, transmitiéndose en este caso el par de claves criptográficas asimétricas y/o la firma y/o el identificador (128) desde el primer equipo de automatización (600) al segundo equipo de automatización (611) a través de una conexión de comunicación cifrada.

5. Procedimiento según la reivindicación 4, tratándose en el caso del primer equipo de automatización (600) protegido y cerrado de un centro de confianza.

6. Procedimiento según una de las reivindicaciones anteriores, efectuándose la instalación del módulo de seguridad (100) en el medidor inteligente (142; 144; 146; 148) o la compuerta de enlace de medidor inteligente (138) dentro del segundo equipo de automatización (611).

7. Procedimiento según una de las reivindicaciones anteriores, estando el módulo de seguridad (100) proporcionado sin personalizar, efectuándose solo debido al almacenamiento del par de claves y/o del certificado en el módulo de seguridad (100) una personalización del módulo de seguridad (100).

8. Procedimiento según una de las reivindicaciones anteriores, proporcionándose el módulo de seguridad (100) en forma de una tarjeta chip.

9. Procedimiento según una de las reivindicaciones anteriores, además con la etapa del almacenamiento de información de contacto del primer sistema informático (150) en el módulo de seguridad, efectuándose mediante las informaciones de contacto la determinación de la restricción del acceso de comunicación inicial exclusivamente al primer sistema informático.

10. Producto de programa informático con instrucciones ejecutables por un procesador para llevar a cabo las etapas de procedimiento de acuerdo con una de las reivindicaciones anteriores.

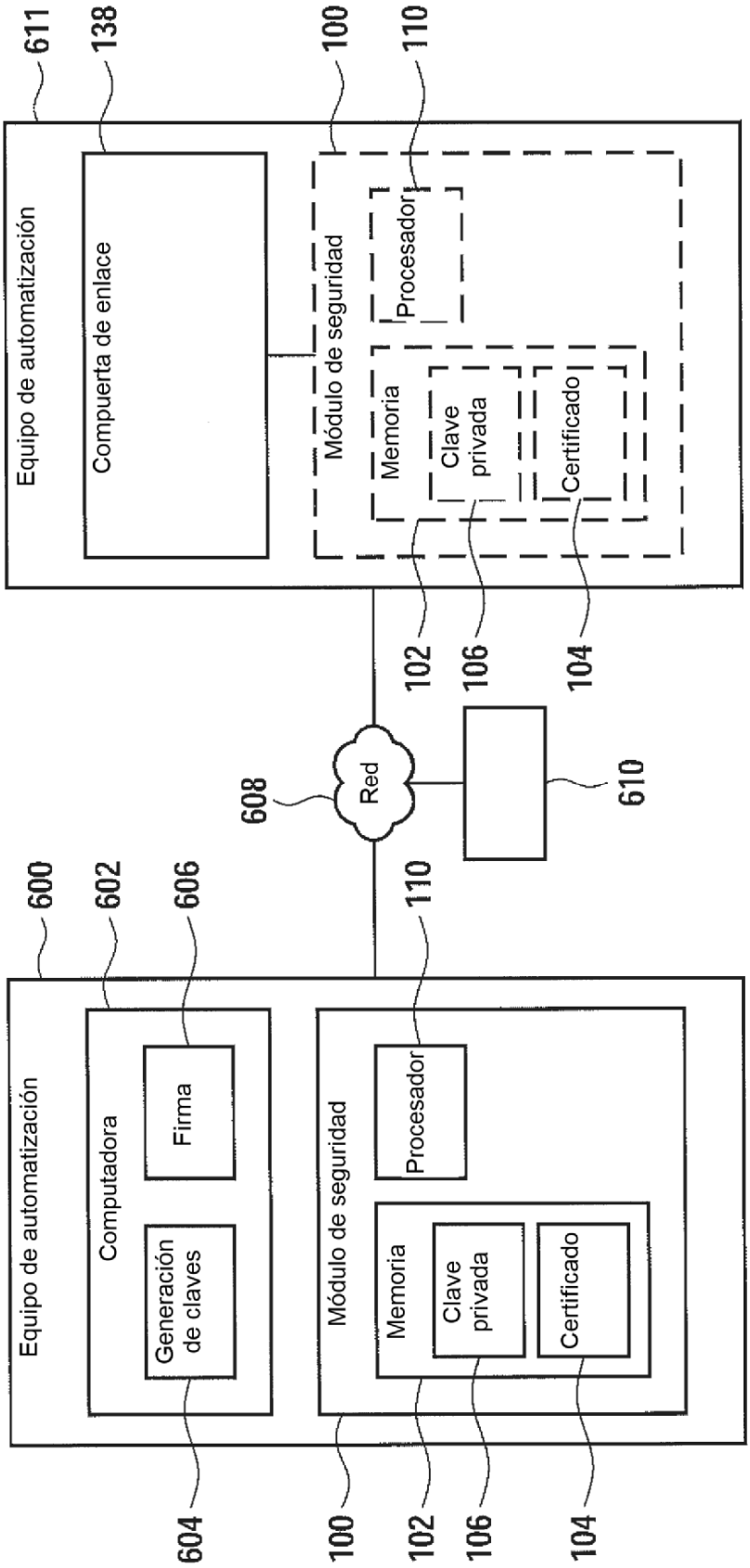
611
138
100
110
Equipo de automatización
Compuerta de enlace
Módulo de seguridad
Procesador
Memoria
Clave privada
Certificado
102
106
104
608
Red
610
600
602
606
110
Equipo de automatización
Computadora
Firma
Generación de claves
Módulo de seguridad
Procesador
Memoria
Clave privada
Certificado
604
100
102
106
104

Fig. 1

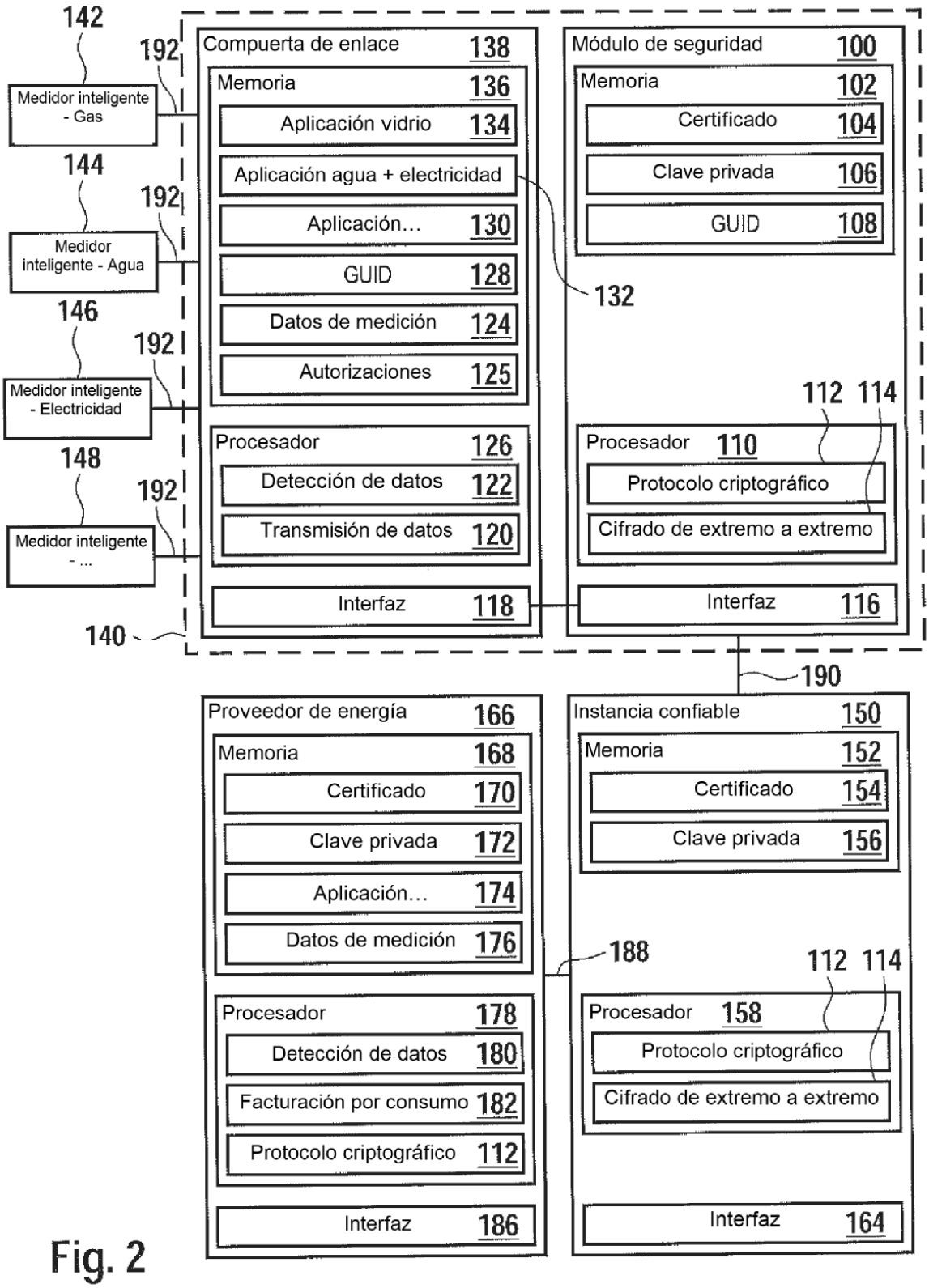
142
192
Medidor inteligente - Gas
144
192
Medidor inteligente - Agua
146
192
Medidor inteligente - Electricidad
148
192
Medidor inteligente - ...
140
Compuerta de enlace 138
Memoria 136
Aplicación vidrio 134
Aplicación agua + electricidad
Aplicación... 130
GUID 128
Datos de medición 124
Autorizaciones 125
Procesador 126
Detección de datos 122
Transmisión de datos 120
Interfaz 118
Módulo de seguridad 100
Memoria 102
Certificado 104
Clave privada 106
GUID 108
132
112 114
Procesador 110
Protocolo criptográfico
Cifrado de extremo a extremo
Interfaz 116
190
Proveedor de energía 166
Memoria 168
Certificado 170
Clave privada 172
Aplicación... 174
Datos de medición 176
188
Procesador 178
Detección de datos 180
Facturación por consumo 182
Protocolo criptográfico 112
Interfaz 186
Instancia confiable 150
Memoria 152
Certificado 154
Clave privada 156
112 114
Procesador 158
Protocolo criptográfico
Cifrado de extremo a extremo
Interfaz 164

Fig. 2

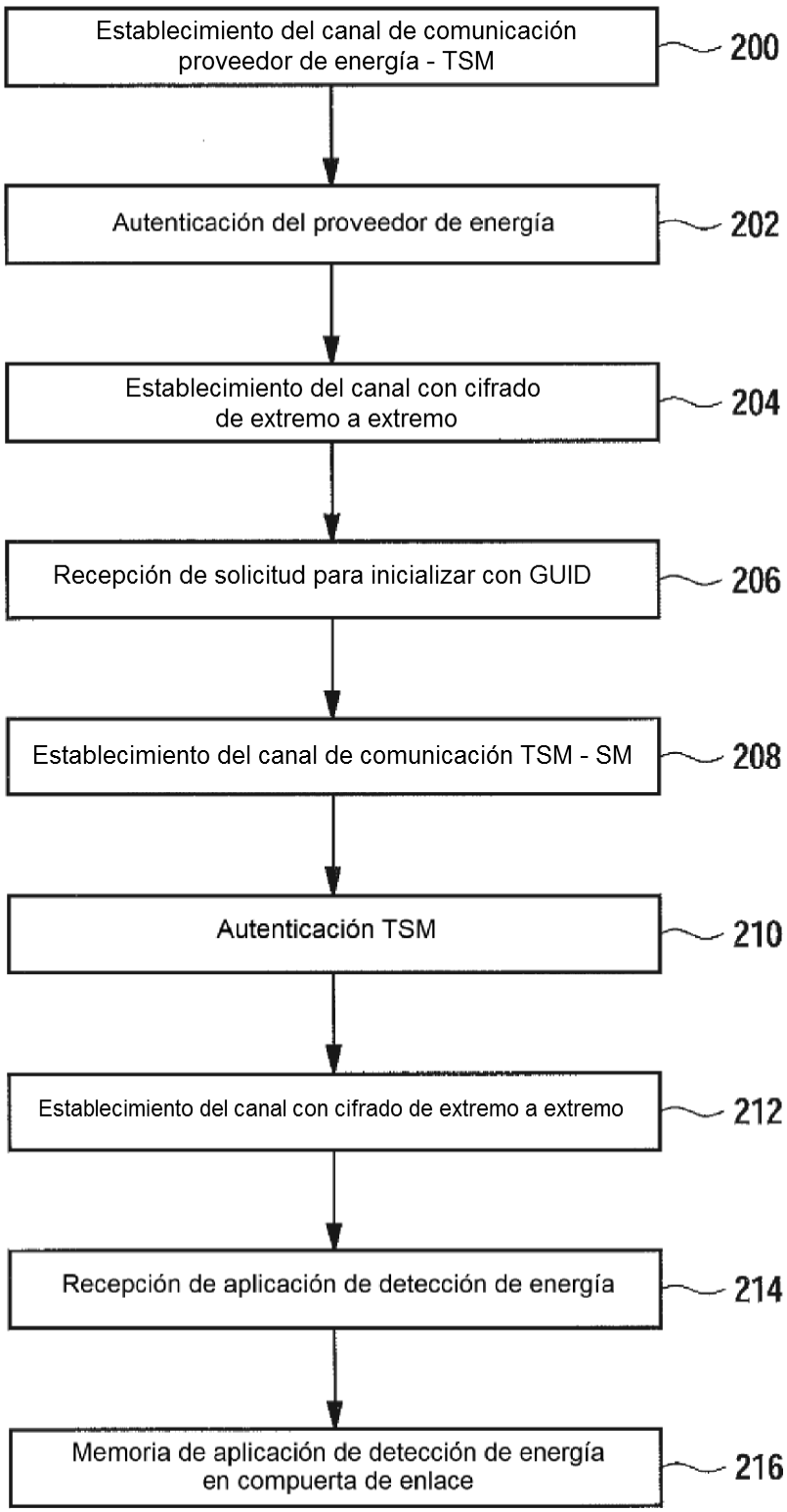
Establecimiento del canal de comunicación proveedor de energía - TSM
200
Autenticación del proveedor de energía
202
Establecimiento del canal con cifrado de extremo a extremo
204
Recepción de solicitud para inicializar con GUID
206
Establecimiento del canal de comunicación TSM - SM
208
Autenticación TSM
210
Establecimiento del canal con cifrado de extremo a extremo
212
Recepción de aplicación de detección de energía
214
Memoria de aplicación de detección de energía en compuerta de enlace
216

Fig. 3

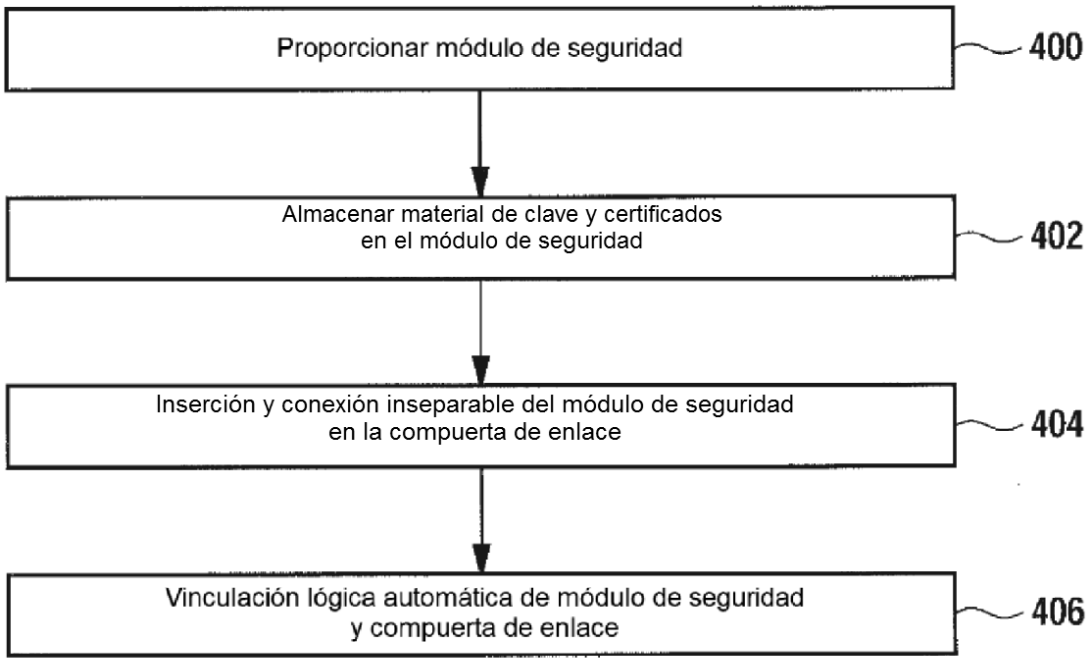
Proporcionar módulo de seguridad
400
Almacenar material de clave y certificados en el módulo de seguridad
402
Inserción y conexión inseparable del módulo de seguridad en la compuerta de enlace
404
Vinculación lógica automática de módulo de seguridad y compuerta de enlace
406

Fig. 4