(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 646 665**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.11.2010 PCT/EP2010/067648**

(87) Fecha y número de publicación internacional: **30.06.2011 WO11076491**

(96) Fecha de presentación y número de la solicitud europea: **17.11.2010 E 10784285 (8)**

(97) Fecha y número de publicación de la concesión europea: **16.08.2017 EP 2499775**

(54) Título: **Equipo y procedimiento para asegurar un acuerdo de al menos una clave criptográfica entre aparatos**

(30) Prioridad:

21.12.2009 DE 102009059893

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.12.2017

(73) Titular/es:

SIEMENS SCHWEIZ AG (100.0%)
Freilagerstrasse 40
8047 Zürich, CH

(72) Inventor/es:

GESSNER, JÜRGEN;
ISLER, BERNHARD y
LIESE, FRANK

(74) Agente/Representante:

LOZANO GANDIA, José

EQUIPO Y PROCEDIMIENTO PARA ASEGURAR UN ACUERDO DE AL MENOS UNA CLAVE CRIPTOGRÁFICA ENTRE APARATOS

DESCRIPCIÓN

Equipo y procedimiento para asegurar un acuerdo de claves criptográficas entre aparatos. La presente invención se refiere a un procedimiento y a un equipo para garantizar una comunicación segura frente a intercepción y segura frente a falseamiento entre aparatos y en particular a un procedimiento y un equipo para asegurar un acuerdo de al menos una clave criptográfica. La presente invención se refiere además a un producto de programa de ordenador que provoca que se ejecute un procedimiento para asegurar un acuerdo de al menos una clave criptográfica, así como a una memoria de datos que memoriza el producto de programa de ordenador.

En la técnica de edificios moderna se montan una pluralidad de aparatos y componentes estructurales no sólo en edificios de fábricas, sino también en edificios de oficinas y privados. Al respecto es posible que al menos algunos aparatos seleccionados de entre los que están montados comuniquen entre sí, intercambiando entonces datos. Un posible escenario de aplicación de aparatos que comunican entre sí es la automatización de edificios. Allí está prevista usualmente una unidad central de control, que activa una pluralidad de aparatos mediante órdenes de control y con ello regula por ejemplo una climatización del edificio completo. Los aparatos que están montados en un edificio pueden configurar, mediante una infraestructura adecuada, una red peer-to-peer (entre iguales) o una red client-server (cliente-servidor).

Además se conocen vehículos que están dotados de unidades de control que mediante una interfaz de aire comunican con aparatos domésticos. Así se sabe que un conductor de un automóvil puede controlar mediante su pantalla del automóvil, a través de una interfaz de telefonía móvil, la evolución del calor de un elemento calentador o el cierre o la apertura de una persiana enrollable. Puesto que en los escenarios de aplicación descritos se comunican entre sí la pluralidad de aparatos que en parte proceden de distintos fabricantes, presentan las redes de comunicación una gran heterogeneidad en cuanto a los fabricantes de componentes de red y además a la utilización de protocolos de red. En este escenario de aplicación es esencial que la comunicación entre los distintos aparatos pueda realizarse con seguridad frente a la intercepción y también frente al falseamiento. Para ello se conocen diversas técnicas de red, así como protocolos de encriptación.

En particular en la automatización de edificios, es decir, en un control automatizado de aparatos que están montados en un edificio, se conoce el protocolo BACnet. BACnet significa aquí “Building Automation and Control Network” (red de automatización y control de edificios). Al respecto se trata de un protocolo de red que se utiliza para la comunicación de aparatos en la técnica de automatización de edificios y en la correspondiente gestión de peligros. BACnet Security se basa en criptografía simétrica, es decir, los aparatos que se comunican deben tener en conjunto un secreto, también llamado clave. Para la distribución de claves está previsto un servidor de claves, que basándose en una “Basis Key" (clave de base) distribuye otras claves con seguridad a los aparatos que se comunican. Esta “Basis Key”, denominada en el estándar de BACnet “Device-Master-Key” (clave maestra del aparato), es individual y diferente para cada aparato. La misma debe introducirse en el “Key Server” o servidor de claves y/o en el aparato que ha de comunicarse de manera adecuada y segura, para hacer posible una distribución segura de otras claves entre el Key-Server y el aparato.

La especificación de la BACnet describe un suministro de los aparatos con una Device-Master-Key, que está impresa sobre una llamada “Tearoff-Label” (etiqueta removible). La etiqueta se retira y se introduce la Device-Master-Key manualmente en el Key-Server. Además apoya la BACnet órdenes para transportar una Device-Master-Key desde el Key-Server a través de la red de aparatos No obstante, estas posibilidades tienen el inconveniente de que son costosas y susceptibles de faltas, puesto que se basan en una introducción manual o son inseguras, ya que se realiza una distribución de claves a través de la red no asegurada.

Los procedimientos criptográficos se utilizan entre otros para encriptar mensajes, firmar documentos y autentificar personas u objetos. Para ello son particularmente adecuados los llamados procedimientos de encriptación asimétricos, que prevén para un abonado tanto una clave privada y mantenida en secreto como también una clave pública.

Al encriptar un mensaje recibe el emisor la clave pública del destinatario deseado y encripta con la misma el mensaje. Sólo el destinatario está a continuación en condiciones de desencriptar el mensaje de nuevo con la clave privada que sólo él conoce.

Al firmar un documento, calcula el firmante de un documento con su clave privada una firma electrónica. Otras personas pueden verificar sin más la firma con ayuda de la clave pública del firmante. No obstante sólo pueden verificarse con la clave pública firmas que están firmadas con la correspondiente clave privada. Mediante esta asociación inequívoca y la hipótesis de que la clave privada se mantiene en secreto por parte del firmante, resulta una asociación inequívoca de la firma al firmante y al documento.

Los procedimientos criptográficos asimétricos se basan, tal como antes se ha indicado, en una clave privada y una clave pública. Al respecto se genera la clave pública a partir de la clave privada mediante un algoritmo predeterminado Es esencial para el procedimiento criptográfico que no pueda forzarse una inversión, es decir, una determinación de la clave privada a partir de la clave pública en un tiempo razonable con las capacidades de cálculo disponibles. Esto último se logra en el caso de que la longitud de la clave privada alcance una longitud mínima. La longitud mínima de la clave depende de los algoritmos utilizados para la encriptación y la determinación de la clave pública.

Las operaciones con las claves públicas o las claves privadas exigen un coste de cálculo. Éste depende de los algoritmos utilizados y también de la longitud de la clave utilizada. Al respecto se comprueba que es ventajoso utilizar procedimientos criptográficos basados en curvas elípticas, ya que las mismas aseguran una elevada seguridad con claves de longitud corta. Hasta ahora no se conocía para procedimientos criptográficos basados en curvas elípticas, contrariamente a en otros procedimientos, ninguna determinación de la clave privada a partir de la clave pública, cuyo coste en cálculo aumente más lentamente que con el aumento exponencial al aumentar la longitud de la clave.

Los acuerdos tradicionales para asegurar un acuerdo de claves son usualmente costosos, susceptibles de faltas e inseguros. En particular en la técnica de edificios o bien automatización de edificios no se conoce ningún procedimiento que haga posible acordar claves criptográficas que sirvan para encriptar una comunicación de manera segura en una red no asegurada.

El documento WO 2005/010214 A2 da a conocer un procedimiento para acordar una clave simétrica para la comunicación entre nodos de sensor inalámbricos de una red, en los que el acuerdo de la clave simétrica entre un nodo de sensor y un centro de claves se asegura con ayuda de claves asimétricas memorizadas en los nodos de sensor.

Es por lo tanto un objetivo de la presente invención proporcionar un procedimiento y un equipo para garantizar una seguridad de la red y en particular para asegurar un acuerdo de al menos una clave criptográfica entre aparatos.

Este objetivo se logra mediante un procedimiento para asegurar un acuerdo de claves criptográficas entre aparatos que presenta las características de la reivindicación 1.

Los aparatos pueden ser elementos estructurales, máquinas, elementos calentadores y/o instalaciones de fabricación. Preferentemente encuentra utilización el procedimiento en un escenario de aplicación de la automatización de edificios. Al respecto conoce el especialista medio otros aparatos que comunican entre sí y acuerdan entonces una clave criptográfica. Es posible que uno de los aparatos proporcione una función central de control. Por ejemplo puede existir uno de los aparatos como una estación central de gestión o bien una estación de gestión de aparatos. En un edificio pueden así estar montados distintos aparatos que comunican entre sí bajo intermediación de una centralita autorizada, por ejemplo un Key Server o servidor de claves, pudiendo ser necesario que esta comunicación esté asegurada.

Los aparatos que están montados en el edificio pueden ser por ejemplo aparatos críticos para la seguridad. Así es posible que estos aparatos sean una instalación para el cierre de puertas y/o un control de las mismas. Para hacer que zonas de acceso protegido dentro del edificio sólo sean accesibles a personal autorizado, se necesitan técnicas de aseguramiento, que hacen posible que pueda asegurarse una comunicación entre los aparatos y en particular un acuerdo de al menos una clave criptográfica entre los aparatos. El aseguramiento se refiere aquí a impedir una intercepción de mensajes que se intercambian entre los aparatos, así como a una garantía de integridad, es decir de la imposibilidad de falseamiento de los mensajes intercambiados entre los aparatos.

Una encriptación de una comunicación puede realizarse mediante una clave criptográfica. Al respecto es usualmente necesario que al menos una clave se distribuya entre aparatos que comunican entre sí. Esta clave, que ha de distribuirse a los correspondientes aparatos, puede ser por ejemplo una clave maestra (master). Para que los aparatos puedan comunicarse de forma encriptada es usualmente necesario tener disponible tanto una clave maestra como también una clave secundaria para un encriptación y/o para una desencriptación del mensaje.

En consecuencia debe acordarse al menos una de estas claves criptográficas entre los aparatos. Para ello puede ser necesario transmitir al menos la clave maestra, también denominada clave principal, a todos los interlocutores de la comunicación, es decir, a los aparatos que se comunican. En una transmisión de la clave maestra a los aparatos puede no obstante producirse una intercepción de esta clave maestra. Para evitar esta intercepción se proporciona en una forma de realización del procedimiento de acuerdo con la invención, para asegurar un acuerdo de al menos una clave criptográfica, una clave privada y una clave pública para cada aparato individual. Con esta clave privada y esta clave pública es posible ahora asegurar un acuerdo de al menos una clave criptográfica, por ejemplo de la clave maestra.

La aportación de la clave privada y de la clave pública puede realizarse por ejemplo mediante métodos tradicionales. Para ello conoce el especialista distintas formas de proceder en el sector técnico de la

criptografía. Según una forma de realización del procedimiento para asegurar un acuerdo de al menos una clave criptográfica, puede realizarse una generación o una creación de la clave privada y de la clave pública para cada aparato individual. Es decir, que cada uno de los aparatos que están montados en el edificio recibe como asignada exactamente una clave privada y exactamente una clave pública. Al respecto puede ser ventajoso que un aparato central de control dentro del edificio, por ejemplo la estación de gestión de aparatos, conozca todos los pares de claves. Además puede ser necesario que todos los aparatos conozcan la clave privada propia y también la clave pública propia. Si ha de realizarse un acuerdo de al menos una clave criptográfica en un escenario cliente-servidor, entonces puede conocer la estación de gestión de aparatos cada uno de los pares de claves, que presentan una clave privada y una clave pública, para cada uno de los aparatos. Así es posible que los aparatos no comuniquen directamente entre sí, es decir, no realicen directamente uno con otro un acuerdo de al menos una clave criptográfica, sino que los mismos se comuniquen con una instancia central, que es la estación de gestión de aparatos.

Cuando se ha creado para cada uno de los aparatos una clave privada y una clave pública, puede comunicarse este par de claves al correspondiente aparato. Para ello puede estar prevista una memorización de la clave privada y de la clave pública en cada aparato individual. Para ello es posible que cada aparato presente una memoria de datos para memorizar la clave privada y la clave pública.

Puesto que ahora para cada uno de los aparatos está generada y memorizada una clave privada, así como una clave pública, puede realizarse un acuerdo de la clave criptográfica, de las que al menos hay una, entre los aparatos en función de la clave privada memorizada y de la clave pública memorizada. Esto puede realizarse por ejemplo mediante el protocolo de red BACnet, utilizándose de acuerdo con la invención la clave privada memorizada y la clave pública memorizada para encriptar la comunicación. Si se realiza el acuerdo de al menos una clave criptográfica según el protocolo de red BACnet, entonces se asegura un intercambio de mensajes según este protocolo de red BACnet mediante la clave privada y mediante la clave pública.

El acuerdo de claves criptográficas puede incluir por ejemplo una generación de una clave maestra para cada uno de los aparatos. Entonces puede ser conocida la clave maestra por cada aparato, es decir, el aparato conoce no sólo la clave maestra propia sino también la clave maestra correspondiente a los otros aparatos. Además puede realizarse una generación de una clave secundaria para cada uno de los aparatos, siendo conocida la clave secundaria generada sólo al propio aparato. Además puede realizarse un encriptación de la correspondiente clave secundaria en función de la clave maestra mediante cada aparato individual. Las claves secundarias así encriptadas pueden distribuirse ahora a cada uno de los aparatos.

Si ha de realizarse un acuerdo de al menos una clave criptográfica mediante un equipo central de control, por ejemplo la estación de gestión de aparatos, entonces es ventajoso que la estación de gestión de aparatos sólo disponga de claves maestras por pares, es decir, una clave maestra para exactamente un aparato, así como una clave maestra para la estación de gestión de aparatos. En otra clave maestra por pares dispone la estación de gestión de aparatos de una clave maestra para el siguiente aparato junto con una siguiente clave maestra para la estación de gestión de aparatos. Al respecto es posible también que la estación de gestión de aparatos presente exactamente una clave maestra. Para visualizar la clave maestra por pares, remitimos a la siguiente tabla:

estación de gestión de aparatos	aparato	valor de la clave
GVS-ID1	G1-ID1	valor de clave 1
GVS-ID2	G2-ID2	valor de clave 2
GVS-ID3	G3-ID3	valor de clave 3
…	…	…
GVS-IDn	GN-IDn	valor de clave n

En la tabla que acabamos de mostrar se inscriben para usualmente una estación de gestión de aparatos GVS pares de claves incluyendo su valor. El parámetro n se refiere entonces a la cantidad de aparatos. Es posible que una estación de gestión de aparatos comunique mediante distintas claves maestras GVS-ID1, GVS-ID2, GVS-ID3,…, GVS-IDn con los aparatos terminales o que la estación de gestión de aparatos comunique mediante los mismos valores de clave con los aparatos, es decir, que por lo tanto GVS-ID1, GVS-ID2, GVS-ID3,…, GVS-IDn presenten el mismo valor de identificación.

Es especialmente ventajoso en el procedimiento descrito para asegurar un acuerdo de al menos una clave criptográfica según una forma de realización de la presente invención, que tanto la clave pública como también la clave privada puedan ser generadas ya antes de operar los aparatos y puedan memorizarse en el correspondiente aparato. Esto es ventajoso en particular porque el acuerdo así como la introducción de una clave privada y de una clave pública pueden faltar en un aparato durante el tiempo de funcionamiento. En consecuencia es posible según una forma de realización de la presente invención

memorizar ya durante la fabricación de los aparatos, es decir, offline la clave privada y la clave pública en un entorno asegurado en los correspondientes aparatos. Así se evita el acuerdo especialmente susceptible de faltas e inseguro de la clave privada y de la clave pública en el tiempo de funcionamiento.

Cualquier comunicación adicional entre los aparatos puede ahora asegurarse mediante la clave privada memorizada y la clave pública memorizada. Para ello puede realizarse un encriptación de aquellos mensajes que sirven para el acuerdo de al menos una clave criptográfica.

En una forma de realización del procedimiento de acuerdo con la presente invención, se realiza una encriptación de una comunicación entre los aparatos mediante la clave criptográfica acordada.

Esto tiene la ventaja de que la comunicación entre los aparatos puede asegurarse mediante una clave criptográfica generada de manera segura.

En otra forma de realización del procedimiento de acuerdo con la presente invención, se realiza la memorización de la clave privada y de la clave pública durante una fabricación y/o antes de una puesta en servicio del correspondiente aparato.

Esto tiene la ventaja de que la memorización de la clave privada y de la clave pública puede realizarla un fabricante de aparatos en un entorno seguro, es decir, sin un acuerdo de la clave privada y de la clave pública durante el funcionamiento de los aparatos.

En otra forma de realización del procedimiento de acuerdo con la presente invención, se realiza el acuerdo sobre la clave criptográfica tras una puesta en servicio de los aparatos.

Esto tiene la ventaja de que el acuerdo de la clave criptográfica puede realizarse dinámicamente durante el tiempo de funcionamiento de los aparatos, pero una vez que la clave privada y la clave pública ya están memorizadas en el aparato.

En otra forma de realización del procedimiento según la presente invención, se realiza el acuerdo de la clave criptográfica según un protocolo de red.

Esto tiene la ventaja de que al acordar las claves criptográficas las infraestructuras de red ya existentes pueden operar mediante protocolos de red ya existentes.

En otra forma de realización del procedimiento según la presente invención, implementa el protocolo de red al menos un método criptográfico.

Esto tiene la ventaja de que el protocolo de red prevé medidas de aseguramiento adicionales.

En otra forma de realización del procedimiento según la presente invención, se realiza la negociación, al menos parcialmente, mediante un protocolo de red de la Building Automation and Control Network (red de automatización y control de edificios).

Esto tiene la ventaja de que el procedimiento descrito para asegurar un acuerdo de claves criptográficas puede encontrar aplicación en particular en escenarios de aplicación de la automatización de edificios.

En otra forma de realización del procedimiento según la presente invención incluye el acuerdo al menos un intercambio de mensajes directo o indirecto entre los aparatos.

Esto tiene la ventaja de que por ejemplo en un acuerdo de claves criptográficas los aparatos pueden comunicar directamente entre sí, por ejemplo en una red peer-to-peer o indirectamente, por ejemplo en una red cliente-servidor.

En otra forma de realización del procedimiento según la presente invención, se realiza el intercambio de mensajes mediante al menos una red inalámbrica o de línea física.

Esto tiene la ventaja de que el intercambio de mensajes dentro de un edificio puede realizarse inalámbricamente, por ejemplo a través de paredes del edificio, o por línea física, por ejemplo mediante enlaces de datos de banda ancha ligados a cable.

En otra forma de realización del procedimiento según la presente invención, se confecciona al menos un certificado de seguridad relativo a una prueba de autenticidad para al menos uno de los aparatos.

Esto tiene la ventaja de que está previsto un mecanismo de seguridad adicional, mediante el cual puede autentificarse cada aparato individual.

En otra forma de realización del procedimiento según la presente invención, se confecciona el certificado de seguridad en función de al menos una de las claves públicas.

Esto tiene la ventaja de que el certificado de seguridad puede confeccionarse en función de una clave pública creada de manera segura.

En otra forma de realización del procedimiento según la presente invención, presenta al menos una de las claves públicas, de las claves privadas y/o de las claves criptográficas, una marca de tiempo, una indicación relativa a un derecho de acceso, una cadena de caracteres alfanumérica, un valor numérico y/o datos de claves.

Esto tiene la ventaja de que al menos una de las claves puede dotarse de una validez de duración relativa a una determinada identidad de aparato, así como especificación de derechos.

En otra forma de realización del procedimiento según la presente invención, se realiza la aportación de la clave privada y de la clave pública mediante un servidor de claves.

Esto tiene la ventaja de que infraestructuras y puestos de emisión de claves ya existentes pueden encontrar aplicación en el presente procedimiento.

El objetivo se logra además mediante un equipo para asegurar un acuerdo de claves criptográficas para cada uno de los aparatos de acuerdo con la reivindicación 14. La invención se refiere además a un producto de programa de ordenador que origina la realización de los procedimientos descritos, así como a una memoria de datos, que memoriza el producto de programa de ordenador.

Así se proporcionan un procedimiento y un equipo para asegurar un acuerdo de claves criptográficas para cada uno de los aparatos, las cuales permiten con poco coste de cálculo y sin la necesidad de un intercambio de mensajes para acordar la clave privada y la clave pública, asegurar un acuerdo de claves criptográficas.

En una forma de realización del procedimiento tiene lugar de acuerdo con la invención la aportación de una clave privada y de una clave pública separadamente de un acuerdo de las claves criptográficas, con lo que la aportación de la clave privada y de la clave pública puede realizarse durante el tiempo de fabricación de los aparatos y el acuerdo de las clave criptográficas puede realizarse durante el tiempo de funcionamiento de los aparatos. Puesto que la aportación de la clave privada y de la clave pública puede realizarse durante el tiempo de fabricación de los aparatos, pueden crearse ambas claves, es decir, la clave privada y la clave pública, en una zona asegurada, como por ejemplo una planta de fabricación de aparatos y memorizarse de forma segura directamente en el correspondiente aparato.

Otras variantes ventajosas de la invención son objeto de las reivindicaciones secundarias, así como de los ejemplos de realización descritos en lo que sigue. A continuación se describirá la invención más en detalle en base a implementaciones a modo de ejemplo con referencia a las figuras adjuntas.

Al respecto muestra:

figura1 una ilustración de un ejemplo de aplicación de un procedimiento para asegurar un acuerdo de al menos una clave criptográfica entre aparatos según una forma de realización de la presente invención;

figura 2 un diagrama secuencial de un procedimiento para asegurar un acuerdo de al menos una clave criptográfica entre aparatos según una forma de realización de la presente invención;

figura 3 un diagrama secuencial detallado de un procedimiento para asegurar un acuerdo de al menos una clave criptográfica entre aparatos según una forma de realización de la presente invención;

figura 4 un diagrama de bloques de un equipo para asegurar un acuerdo de al menos una clave criptográfica entre aparatos según una forma de realización de la presente invención y

figura 5 un diagrama de bloques detallado de un equipo para asegurar un acuerdo de al menos una clave criptográfica entre aparatos según una forma de realización de la presente invención.

En las figuras se han dotado los mismos elementos o elementos que tienen las mismas funciones de las mismas referencias, siempre que no se indique otra cosa.

La figura 1 muestra una ilustración de un procedimiento para asegurar un acuerdo de al menos una clave criptográfica según una forma de realización de la presente invención.

Al respecto se fabrica un aparato en una fábrica F. El aparato es en el presente ejemplo de realización un aparato doméstico y debe alojarse en un edificio G tras el suministro A. El aparato es por ejemplo un elemento calentador, que mediante una automatización de edificios, es decir, un control autónomo de aparatos dentro de un edificio, se controla en cuanto a su potencia de calentamiento. Puesto que en el edificio G no está montado sólo un único elemento calentador, sino una pluralidad de elementos calentadores, es necesario para regular la temperatura en el edificio G que los distintos elementos calentadores se comuniquen entre sí y entonces por ejemplo intercambien datos de medida en relación con el calor generado.

La comunicación entre los aparatos debe asegurarse en el presente ejemplo de realización mediante una clave criptográfica, que los aparatos acuerdan durante el funcionamiento. Para ello es necesario que se asegure ya el acuerdo de la clave criptográfica, de las que menos hay una. Si no se asegurase el acuerdo de la clave criptográfica, de las que al menos hay una, entonces existiría el riesgo de que terceros no autorizados pudieran espiar la clave criptográfica, interceptando el intercambio de mensajes entre los aparatos.

Para el asegurar el acuerdo de la clave criptográfica, de las que al menos hay una, se realiza el proceso en la presente forma de realización del procedimiento para asegurar un acuerdo de al menos una clave criptográfica mediante una clave privada y una clave pública para cada aparato individual. Es decir, que para cada aparato individual se proporcionan una clave privada y una clave pública.

Si existen por lo tanto n aparatos, entonces es posible en una forma de realización proporcionar n claves privadas así como n claves públicas. En consecuencia está asociada a cada aparato individual exactamente una determinada clave privada y clave pública proporcionadas. Precisamente esta clave privada y precisamente esta clave pública se memoriza en cada aparato individual.

La aportación de la clave privada y de la clave pública es especialmente crítica para la seguridad, ya que mediante la clave privada y la clave pública queda asegurado el acuerdo de la clave criptográfica, de las que al menos hay una. En la presente forma de realización del procedimiento para asegurar el acuerdo según la presente invención, se realizan la aportación y/o la memorización de la clave privada y de la clave pública en la fábrica F. La fábrica F es una instancia digna de confianza en cuanto a la aportación y a la memorización de la clave privada y de la clave pública. Así es posible proporcionar y memorizar precisamente estas claves bajo condiciones especialmente seguras dentro de la fábrica F. Con ello es posible proporcionar la clave privada y la clave pública en cualquier etapa de fabricación de los aparatos que están previstos para montarlos en el edificio G. Al respecto es especialmente ventajoso que la clave privada y la clave pública no tengan que ser acordadas durante el funcionamiento de los aparatos, es decir, durante la operación de los aparatos. En consecuencia la clave privada y la clave pública están memorizadas en cada aparato individual antes del suministro A al edificio G.

Así puede asegurarse tras el suministro A de los aparatos un acuerdo de la clave criptográfica, de las que al menos hay una, entre los aparatos suministrados mediante la clave privada y la clave pública proporcionadas bajo condiciones seguras.

La figura 2 muestra un procedimiento para asegurar el acuerdo de al menos una clave criptográfica entre aparatos. El procedimiento presenta las siguientes etapas:

Memorización 100 de una clave privada y de una clave pública en cada aparato individual, proporcionándose la clave privada y la clave pública para el correspondiente aparato.

Acuerdo 101 de la clave criptográfica, de las que al menos hay una, entre los aparatos en función de la clave privada memorizada y de la clave pública memorizada.

Las etapas del procedimiento descritas pueden presentar etapas subordinadas adicionales, así como estar realizadas iterativamente y/o en otra secuencia.

La figura 3 muestra un diagrama secuencial detallado de un procedimiento para asegurar un acuerdo de al menos una clave criptográfica entre aparatos según una forma de realización de la presente invención.

En una primera etapa del procedimiento 200 se proporciona una clave privada para exactamente un único aparato. En una etapa del procedimiento 201 análoga se proporciona una clave pública para exactamente un aparato. Usualmente se ejecutan las etapas del procedimiento 200 y 201 repetidamente hasta que para cada aparato individual existen una clave privada y una clave pública. La aportación de las claves en la etapa del procedimiento 200, así como en la etapa del procedimiento 201, puede realizarse por ejemplo generando números aleatorios, palabras de paso, números de identificación, identidades de aparatos y/u otros procedimientos de aportación de claves adecuados.

En una etapa del procedimiento 202 subsiguiente, sigue la memorización de la clave privada, así como la memorización de la clave pública en la etapa del procedimiento 203. Análogamente a la aportación de la clave privada y de la clave pública en las etapas del procedimiento 200 y 201, pueden ejecutarse las etapas del procedimiento 202 y 203 repetidamente. En consecuencia, se memoriza en cada aparato individual en la etapa del procedimiento 202 la correspondiente clave privada y en la etapa del procedimiento 203 en cada aparato la correspondiente clave pública.

En una etapa del procedimiento 204 opcional que sigue a continuación, se realiza el suministro y/o el montaje del aparato, memorizándose la clave privada y la clave pública. Usualmente se montan entonces una pluralidad de aparatos.

En una etapa del procedimiento preparatoria 205 adicional, se realiza el establecimiento de la red mediante la cual pueden comunicarse entre sí los aparatos, El establecimiento de una red incluye tanto la aportación del hardware físico como también la aportación de órdenes de control y/o protocolos de red. Por ejemplo puede establecerse en la etapa del procedimiento 205 una red peer-to-peer o una red cliente-servidor.

En una etapa del procedimiento siguiente 206 opcional es posible intercambiar informaciones públicas, por ejemplo una clave pública, entre los aparatos. El intercambio de las claves públicas en la etapa del procedimiento 206 puede servir por ejemplo para identificar interlocutores de comunicación, es decir, otros aparatos. La clave pública puede presentar por ejemplo un número de serie y/o una dirección de red de un aparato.

Ahora puede realizarse un acuerdo de la clave criptográfica, de las que al menos hay una, entre los aparatos en una etapa del procedimiento 207. El acuerdo se realiza entonces en función de una encriptación de los mensajes con la clave privada y/o con la clave pública proporcionada en las etapas del procedimiento 200 y 201. Si ya se ha acordado la clave criptográfica entre los aparatos, entonces se realiza en la etapa del procedimiento 208 una comunicación de los aparatos 208. Al respecto es ventajoso encriptar y/o asegurar la comunicación con la clave criptográfica acordada.

Las etapas del procedimiento descritas pueden presentar etapas secundarias, así como realizarse iterativamente y/o en otra secuencia.

En otra forma de realización del procedimiento para asegurar un acuerdo de al menos una clave criptográfica, se utiliza el protocolo de red BACnet. El BACnet sirve entonces como protocolo de transporte para los mensajes criptográficos y para la utilización de criptografía asimétrica. Se puede utilizar entonces el protocolo a asegurar igualmente como protocolo para un acuerdo seguro de claves. Para ello puede memorizarse durante la fabricación de los aparatos un certificado de aparato con la clave pública, así como la correspondiente clave privada y un certificado de raíz. Al respecto está previsto un servidor de claves, que comunica con los aparatos, también llamados devices. Por cada aparato se realiza primeramente una autentificación mutua de aparato (device) y servidor de claves (Key-Server). Tras realizarse la autentificación con éxito, se acuerda a continuación entre aparatos y Key-Server una clave, que se utiliza como clave maestra de los aparatos (Device-Master-Key). Este acuerdo puede realizarse en texto explícito, ya que la propia clave no se transmite.

Como protocolo de autentificación y acuerdo de claves pueden utilizarse protocolos estándar, que cumplen la correspondiente exigencia, como por ejemplo TLS, Diffie-Hellman. Como mecanismo de encriptación pueden utilizarse curvas elípticas. Pero también pueden utilizarse otros protocolos criptográficos. Como protocolo de transporte para la autentificación y los mensajes de acuerdo de claves, puede utilizarse por ejemplo BACnet. Para ello pueden definirse características de objeto BACnet propietarias, que se describen con el servidor BACnet estándar.

Es especialmente ventajosa al respecto la combinación de criptografía asimétrica, cuyos parámetros pueden ya memorizarse durante la fabricación en los aparatos y además la utilización de BACnet como protocolo de transporte para la autentificación y acuerdo de claves.

Así se realiza un acuerdo de claves seguro a través de redes BACnet no aseguradas. En el acuerdo de claves con métodos asimétricos no tienen que estar asegurados los mensajes individuales transmitidos. No obstante, sólo conocen la clave acordada los aparatos participantes. Con ello no se necesita un cableado especial para la transmisión o interfaces de red adicionales para la conexión asegurada con el servidor de claves.

Además no se necesita ningún protocolo adicional para transportar mensajes para la autentificación y acuerdo de claves, ya que se utiliza BACnet. Además es posible una autentificación inequívoca de los aparatos. La utilización de certificados permite una autentificación inequívoca de los aparatos durante el acuerdo de claves, si ello es necesario. Además no existe ningún coste de configuración para distribuir las Device-Master-Keys en la instalación. Debido a la memorización de los datos necesarios durante la fabricación, no es necesario durante el tiempo de instalación ningún coste adicional para distribuir las Device-Master-Key. En caso necesario puede realizarse un nuevo acuerdo de la Device-Master-Key sin acceso físico a los aparatos. Los aparatos de la automatización de edificios pueden estar montados en lugares muy inaccesibles. Si se necesita por cualquier razón una nueva Device-Master-Key, puede acordarse de nuevo la misma a través de la red fácilmente y de manera segura basándose en los datos asimétricos existentes.

Además la Device-Master-Key sólo es conocida en el aparato y en el servidor de claves. Debido a ello resulta una seguridad adicional. Además no es necesaria ninguna interfaz adicional para leer o para introducir las claves. Los aparatos no tienen que presentar necesariamente una interfaz de usuario que permita la introducción o la lectura de una clave. Si se introducen los datos necesarios para el acuerdo de la clave durante la fabricación, no se necesita para ello una interfaz de usuario.

La figura 4 muestra un equipo 1 para asegurar un acuerdo de al menos una clave criptográfica KS entre aparatos Gn según una forma de realización de la presente invención. El equipo 1 presenta:

Un primer equipo de cálculo 2 para memorizar una clave privada PS y una clave pública OS en respectivas memorias de datos en cada aparato individual, aportándose la clave privada PS y la clave pública OS para el correspondiente aparato Gn y
un segundo equipo de cálculo 3 para acordar una clave criptográfica KS, de las que al menos hay una, entre los aparatos Gn en función de la clave privada PS memorizada y de la clave pública OS memorizada.

La figura 5 muestra un equipo 1 de acuerdo con otra forma de realización de la presente invención y se diferencia del equipo 1 mostrado en la figura 4 como sigue:

En el presente ejemplo de realización comunica el primer equipo de cálculo 2 con una memoria de datos DB1 alejada. Aquí puede por ejemplo leerse la clave privada PS a partir de la memoria de datos DB1 alejada. Además comunica el primer equipo de cálculo 2 en la otra memoria de datos DB2 y lee entonces la clave pública OS. La memoria de datos DB1 y la memoria de datos DB2 pueden ser operadas por una instancia de aportación de claves. Las memorias de datos DB1 y DB2 pueden ser respectivos bancos de datos de un Key-Server, también llamado servidor de claves. El primer equipo de cálculo 2 puede estar integrado por ejemplo en un chip RFID. Así memoriza el primer equipo de cálculo 2 la clave privada PS y la clave pública OS sobre un chip RFID. Este chip RFID puede montarse en un aparato.

El segundo equipo de cálculo puede ser por ejemplo un microprocesador, que está integrado en uno de los aparatos Gn. Al respecto es posible que el aparato Gn sea adecuado para leer la clave privada PS y la clave pública OS del chip RFID. El aparato Gn puede también presentar una memoria de datos DB3 separada. La memoria de datos DB3 puede estar incluida por ejemplo en el chip RFID. En consecuencia, lee el primer equipo de cálculo 2 la clave privada PS y la clave pública OS a partir de una primera memoria de datos DB1 y una segunda memoria de datos DB2 y memoriza las mismas en la memoria de datos DB3.

En otra forma de realización del equipo 1 para asegurar un acuerdo de al menos una clave criptográfica KS, está incluido el primer equipo de cálculo 2, el segundo equipo de cálculo 3, así como la memoria de datos DB3 en el aparato Gn. En consecuencia en este ejemplo de realización el aparato Gn es adecuado para acordar con otros aparatos Gn la clave criptográfica KS en función de la clave privada PS proporcionada y de la clave pública OS proporcionada.

REIVINDICACIONES

1. Procedimiento para asegurar un acuerdo de claves criptográficas (KS) para cada uno de unos aparatos (Gn) con las siguientes etapas:
   - Memorización (100) de una clave privada (PS) y de una clave pública (OS) en cada aparato individual (Gn), proporcionándose la clave privada (PS) y la clave pública (OS) para el correspondiente aparato;
   - memorización de cada uno de los pares de claves, que presenta una clave privada (PS) y una clave pública (OS) para cada uno de los aparatos (Gn), en una estación de gestión de aparatos y
   - generación (101) de la clave criptográfica (KS) para cada uno de los aparatos (Gn) en función de la clave privada (PS) memorizada y de la clave pública (OS) memorizada mediante la estación de gestión de aparatos.

2. Procedimiento de acuerdo con la reivindicación 1, en el que se realiza una encriptación de una comunicación entre los aparatos (Gn) mediante la clave criptográfica (KS) acordada.

3. Procedimiento de acuerdo con la reivindicación 1 ó 2, en el que se realiza la memorización de la clave privada (PS) y de la clave pública (OS) durante una fabricación y/o antes de una puesta en servicio del correspondiente aparato (Gn).

4. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, en el que se realiza la generación (101) de la clave criptográfica (KS) tras una puesta en servicio de los aparatos (Gn).

5. Procedimiento de acuerdo con una de las reivindicaciones 1 a 4, en el que se realiza la generación (101) de la clave criptográfica (KS) según un protocolo de red.

6. Procedimiento de acuerdo con la reivindicación 5, en el que el protocolo de red implementa al menos un método criptográfico.

7. Procedimiento de acuerdo con una de las reivindicaciones 1 a 6, en el que la generación (101) se realiza, al menos parcialmente, mediante un protocolo de red de la Building Automation and Control Network (red de automatización y control de edificios).

8. Procedimiento de acuerdo con una de las reivindicaciones 1 a 7, en el que la generación (101) incluye al menos un intercambio de mensajes directo o indirecto entre los aparatos (Gn).

9. Procedimiento de acuerdo con la reivindicación 8, en el que el intercambio de mensajes se realiza mediante al menos una red inalámbrica o de línea física.

10 Procedimiento de acuerdo con una de las reivindicaciones 1 a 9, en el que se confecciona al menos un certificado de seguridad relativo a una prueba de autenticidad para al menos uno de los aparatos (Gn).

11. Procedimiento de acuerdo con la reivindicación 10, en el que se confecciona el certificado de seguridad en función de al menos una de las claves públicas (OS).

12. Procedimiento de acuerdo con una de las reivindicaciones 1 a 11, en el que al menos una de las claves públicas (OS), de las claves privadas (PS) y/o las claves criptográficas (KS) presentan una marca de tiempo, una indicación relativa a un derecho de acceso, una cadena de caracteres alfanumérica, un valor numérico y/o datos de claves.

13. Procedimiento de acuerdo con una de las reivindicaciones 1 a 12, en el que se realiza la aportación de la clave privada (PS) y de la clave pública (OS) mediante un servidor de claves.

14. Equipo (1) para asegurar un acuerdo de claves criptográficas (KS) para cada uno de unos aparatos (Gn), en particular para realizar un procedimiento de acuerdo con las reivindicaciones 1 a 13, con:

   - un primer equipo de cálculo (2) para memorizar una clave privada (PS) y una clave pública (OS) en respectivas memorias de datos (DB3) en cada aparato individual (Gn), aportándose la clave privada (PS) y la clave pública (OS) para el correspondiente aparato (Gn) y en el que cada uno de los pares de claves, que presenta una clave privada (PS) y una clave pública (OS), está memorizado para cada uno de los aparatos (Gn) en una estación de gestión de aparatos y

- un segundo equipo de cálculo (3) para generar la clave criptográfica (KS) para cada uno de los aparatos (Gn) en función de la clave privada (PS) memorizada y de la clave pública (OS) memorizada, mediante la estación de gestión de aparatos.

15. Producto de programa de ordenador, que provoca la realización de un procedimiento de acuerdo con una de las reivindicaciones 1 a 13.

16. Memoria de datos, que memoriza el producto de programa de ordenador de acuerdo con la reivindicación 15.

FIG 1

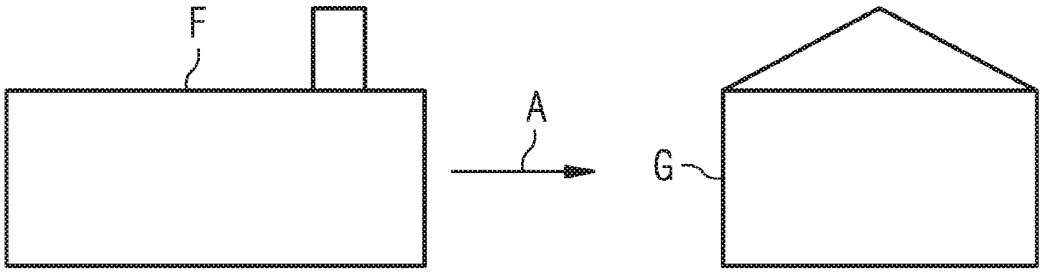

FIG 2

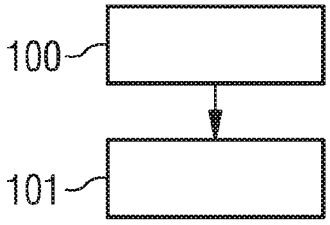

FIG 3

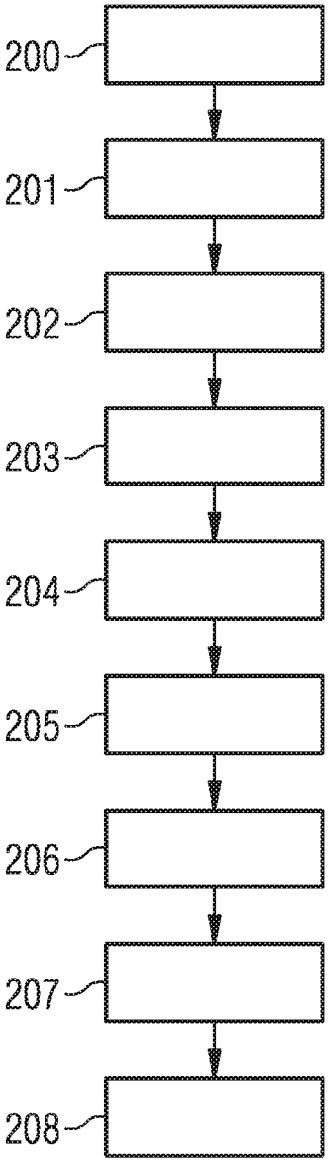

FIG 4

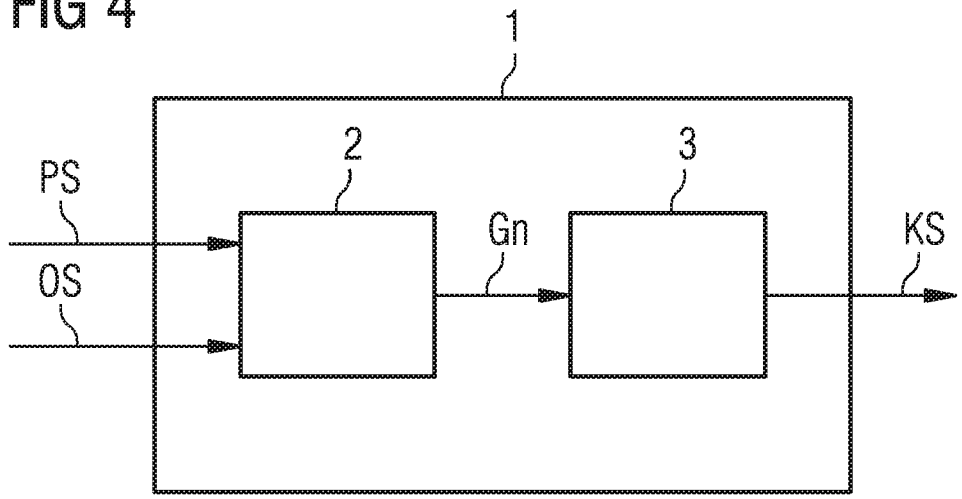

FIG 5