(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 635 556**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 12/28 (2006.01)
H04L 12/46 (2006.01)
H04L 29/06 (2006.01)
G06F 21/33 (2013.01)
G07C 9/00 (2006.01)
G06F 21/44 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.04.2013 PCT/FI2013/050362**

(87) Fecha y número de publicación internacional: **10.10.2013 WO13150186**

(96) Fecha de presentación y número de la solicitud europea: **03.04.2013 E 13772027 (2)**

(97) Fecha y número de publicación de la concesión europea: **31.05.2017 EP 2834938**

(54) Título: **Método seguro para la concesión remota de derechos de funcionamiento**

(30) Prioridad:

05.04.2012 FI 20120110

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.10.2017

(73) Titular/es:

TOSIBOX OY (100.0%)
Teknologiantie 12 A
90590 Oulu, FI

(72) Inventor/es:

YLIMARTIMO, VEIKKO;
KORKALO, MIKKO y
JUOPPERI, JUHO

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Método seguro para la concesión remota de derechos de funcionamiento.

La invención se refiere a un procedimiento seguro de asignación de derechos de funcionamiento para su utilización en un método de control remoto y un sistema de control remoto de accionadores en una propiedad.

Técnica anterior

Cada vez se están instalando más dispositivos y sistemas controlables remotamente en propiedades y viviendas. La finalidad de los sistemas es proteger y/o mantener unas condiciones tales en las propiedades que vivir en ellas resulte tanto seguro como agradable.

En el mercado, hay disponibles una disposición de control remoto para dispositivos técnicos en una propiedad y un método de control remoto que hace uso de esta disposición de control remoto, donde la conexión de Internet, ya existente en las propiedades y las viviendas, se utiliza como tal en el uso remoto de los servicios y la vigilancia de los edificios. En dicha disposición de control remoto se utiliza un par de dispositivos de uso remoto. El usuario lleva un dispositivo de clave portátil, y, en la propiedad, se ha instalado un dispositivo de bloqueo, por medio de los cuales la conexión de destino de la propiedad se modifica de manera que resulte adecuada como tal para un uso remoto. No se modifican las funciones ya existentes de la conexión de red de datos en el destino y la intranet en el destino.

En dicha disposición de control remoto, un dispositivo de bloqueo instalado de una manera fija en una propiedad y un dispositivo de clave llevado por una persona que realiza la monitorización de la propiedad, pueden establecer una red privada virtual (VPN) bidireccional y segura a través de Internet, sobre la base de información de contacto obtenida a partir de un servidor de red de control remoto perteneciente a la disposición de control remoto. El dispositivo de bloqueo en la propiedad – dispositivo de bloqueo al cual están conectados los dispositivos a controlar o monitorizar de manera remota en la propiedad -, se conecta a un dispositivo de interfaz de red de datos/terminal de red en la propiedad, por ejemplo, a un módem.

El par de dispositivos de control remoto de la disposición constituye un par de dispositivos o un grupo de dispositivos predeterminado único, los cuales se identifican mutuamente en la red. Debido al método de identificación, el dispositivo de clave que lleva consigo el usuario o un programa de ordenador instalado en algún dispositivo de procesamiento de datos – implementando dicho programa de ordenador las funciones del dispositivo de clave -, establece una conexión de red únicamente con su propio dispositivo de bloqueo único, y no puede establecerse una conexión correspondiente con ningún otro dispositivo de red. De este modo, el dispositivo de clave sirve como clave de seguridad fuerte para las “puertas de red” de la propiedad.

El par de dispositivos de red de control remoto usado en la disposición de control remoto se puede establecer o bien en relación con la fabricación o bien en relación con la puesta en marcha que tenga lugar posteriormente. En ambos casos, el par de dispositivos se forma conectando el dispositivo de bloqueo y el dispositivo de clave entre sí, por ejemplo, por el puerto USB del dispositivo de clave, con lo cual uno o ambos dispositivos reciben el código de identificación, certificado de dispositivo, del otro.

Las direcciones IP actuales del dispositivo de bloqueo y del dispositivo de clave se mantienen en el servidor de red de control remoto perteneciente a la disposición, usándose dichas direcciones IP para establecer una conexión entre dichos dispositivos. Gracias a los métodos utilizados de establecimiento de la conexión, ambos dispositivos mencionados se pueden conectar a alguna red privada, no pública, y pueden seguir estableciendo entre ellos una conexión segura de transferencia de datos a través de Internet. Para establecer la conexión de transferencia de datos a través de Internet entre el dispositivo de clave móvil y el dispositivo de bloqueo instalado fijo es suficiente con que dichos dispositivos, en algún punto de la conexión establecida, obtengan también una dirección IP pública, aun cuando simultáneamente el dispositivo de bloqueo y el dispositivo de clave solo tienen direcciones IP no públicas. El servidor de red de control remoto no participa en el establecimiento de la conexión real de transferencia de datos después de que haya enviado las direcciones IP de los dispositivos para que estén disponibles para estos últimos.

En dicha disposición de control remoto, se requiere una interconexión física del dispositivo de bloqueo y el dispositivo de clave, en caso de que sea necesario emparejar los dispositivos entre sí. En el sistema, es posible añadir nuevos dispositivos de clave paralelos o subordinados a los que se están utilizando. Esto se puede realizar de la misma manera que la constitución del primer par de dispositivo de clave/dispositivo de bloqueo; conectando el nuevo dispositivo de clave al puerto USB del dispositivo de bloqueo. En la práctica, esto puede implicar el desplazamiento de varios cientos de kilómetros por parte de la persona que está llevando la conexión de la clave nueva con el sistema de control remoto.

El mismo dispositivo de clave puede controlar varios objetos de control remoto independientes, por medio de varios dispositivos de bloqueo independientes. No son posibles cambios de la relación de control mutua entre

estos dispositivos de bloqueo. Un cierto dispositivo de bloqueo no se puede asignar como dispositivo maestro para otro dispositivo de bloqueo, el cual actuaría como dispositivo de bloqueo subordinado del dispositivo de bloqueo que sirve como dispositivo maestro.

Objetivo(s) de la invención:

Es un objetivo de la invención proporcionar un nuevo procedimiento de asignación de derechos de funcionamiento o bien de un nuevo dispositivo de clave o bien de un nuevo dispositivo de bloqueo, utilizado en la disposición de control remoto de propiedades que se puede realizar a través del acceso remoto al dispositivo/dispositivos de bloqueo.

Los objetivos de la invención se logran mediante un procedimiento en el que el certificado del dispositivo de clave se transfiere desde el dispositivo de procesamiento de datos utilizado, a través de una red de transferencia de datos, al(a los) dispositivo(s) de bloqueo, firmado con una clave PKI (Infraestructura de Clave Pública) privada válida del dispositivo de clave, tras lo cual tanto la clave PKI como el certificado del dispositivo de clave nuevo recibidos en el(los) dispositivo(s) de bloqueo se identifican, después de lo cual se lleva a cabo, en el dispositivo de bloqueo, la adición o el cambio del derecho de funcionamiento determinado para el nuevo dispositivo de clave identificado. Si se controlan varios dispositivos de bloqueo independientes con el mismo dispositivo de clave, la relación mutua entre dispositivos de bloqueo se puede modificar de forma correspondiente enviándoles los mensajes de modificación firmados con una clave PKI privada.

Una de las ventajas del método y de la disposición de acuerdo con la invención es que la asignación de derechos de funcionamiento para un dispositivo de clave nuevo se puede llevar a cabo sin necesidad de conectar el dispositivo de clave nuevo físicamente al dispositivo de bloqueo de destino.

Además, una de las ventajas de la invención es que las relaciones de control mutuas de varios dispositivos de bloqueo subordinados al dispositivo de clave se pueden modificar a través de un acceso remoto.

Además, una de las ventajas de la invención es que, utilizando el acceso remoto, por medio del dispositivo de clave puede establecerse una red privada virtual entre dos o más dispositivos de bloqueo, con lo cual un dispositivo de bloqueo sirve como dispositivo de conexión a Internet.

El método según la invención está caracterizado por que

- un dispositivo de clave de confianza transmite un mensaje cifrado con una clave de cifrado privada de un dispositivo de clave de confianza a por lo menos un dispositivo de bloqueo, comprendiendo el mensaje el certificado del dispositivo de clave de confianza y el certificado de por lo menos otro dispositivo, con el cual el dispositivo de bloqueo receptor establecerá una relación de confianza, y definiciones de medidas realizadas en el establecimiento de la relación de confianza

- un dispositivo de bloqueo abre y confirma, con la clave de cifrado pública conocida del dispositivo de clave de confianza, la autenticidad del emisor del mensaje recibido por él;

- el dispositivo de bloqueo guarda certificados de dispositivos relacionados con el mensaje enviado por el dispositivo identificado en su memoria;

- el dispositivo de bloqueo establece una relación de confianza con por lo menos otro dispositivo indicado en el mensaje.

El procesador, la memoria y el código de software de ordenador guardado en la misma, de acuerdo con la invención, se caracterizan por que el dispositivo de clave está configurado para:

- transmitir, desde el dispositivo de clave de confianza, un mensaje cifrado con una clave de cifrado privada del dispositivo de clave de confianza por lo menos al dispositivo de bloqueo, el mensaje que comprende un certificado del dispositivo de clave de confianza y un certificado de por lo menos otro dispositivo, con el cual el dispositivo de bloqueo receptor establecerá una relación de confianza, y definiciones de medidas realizadas en el establecimiento de la relación de confianza;

- recibir y guardar en su memoria, un mensaje de confirmación de una relación de confianza establecida entre por lo menos el dispositivo de bloqueo y otro dispositivo indicado en el mensaje de confirmación del dispositivo de bloqueo.

El programa de ordenador según la invención destinado a proporcionar funciones de dispositivo de clave del sistema de control remoto de accionadores en una propiedad, está caracterizado por que comprende

- unos medios de código para transmitir, desde un dispositivo de clave, un mensaje cifrado con una clave

de cifrado privada del dispositivo de clave de confianza, a por lo menos un dispositivo de bloqueo, comprendiendo el mensaje un certificado del dispositivo de clave de confianza y un certificado de por lo menos otro dispositivo de clave u otro dispositivo de bloqueo, con el cual el dispositivo de bloqueo receptor establecerá una relación de confianza, y definiciones de medidas realizadas en el establecimiento de la relación de confianza, y

- unos medios de código para recibir un mensaje de confirmación de establecimiento de una relación de confianza de un dispositivo de bloqueo desde por lo menos un dispositivo de bloqueo y para guardar el certificado del dispositivo de bloqueo que envió el mensaje en por lo menos la memoria del dispositivo de clave de confianza.

Algunas formas de realización preferidas de la invención se dan a conocer en las reivindicaciones dependientes.

La idea básica de la invención es la siguiente: para llevar a cabo un control remoto, en algunas propiedades existen un par de dispositivos, un dispositivo de bloqueo y un dispositivo de clave, de manera que en dicho par de dispositivos hay por lo menos un dispositivo de bloqueo y por lo menos un dispositivo de clave, que pueden formar una conexión de transferencia de datos sobre la base de una red privada virtual únicamente entre sí.

El dispositivo de bloqueo en la propiedad a controlar de manera remota está instalado en una red de intranet o red de Internet existente, en la propiedad a controlar. Establece una subred, una red de intranet de control, en la red de intranet o Internet, conectándose con dicha red de intranet de control varios accionadores utilizados en el control o la gestión de la propiedad, con una conexión de transferencia de datos o bien por cable o bien inalámbrica.

En una forma de realización ventajosa de la invención, un único dispositivo de clave o varios dispositivos de clave pueden funcionar como par de dispositivo de dos o más dispositivos de bloqueo en propiedades diferentes. El código de identificación propio, el certificado y la clave PKI privada y la pública del dispositivo de bloqueo y el dispositivo de clave, se guardan en dichos dispositivos durante su fabricación. Usando certificados, el dispositivo de bloqueo y el dispositivo de clave pueden establecer entre ellos una conexión segura y bidireccional de transferencia de datos.

En relación con la puesta en marcha, ambos dispositivos determinan información de encaminamiento de los dispositivos desde su red de ubicación íntegramente hasta un terminal de red conectado a Internet, siendo necesaria dicha información de encaminamiento para el establecimiento de la conexión. Esta información de encaminamiento se almacena en un servidor de red de control remoto, conectado a Internet.

En el procedimiento de establecimiento de una relación de confianza de acuerdo con la invención, el dispositivo de clave se puede conectar a algún dispositivo de transferencia de datos, el cual puede establecer una conexión de transferencia de datos con Internet. Los posibles dispositivos de transferencia de datos son, por ejemplo, un PC, un ordenador de tipo tableta o teléfono inteligente.

En una forma de realización ventajosa de la invención, el programa de ordenador que implementa las funciones del dispositivo de clave se guarda en unos medios de almacenamiento de datos portátiles, por ejemplo, una unidad de memoria USB, desde la cual el programa de ordenador a utilizar en el control remoto se puede instalar, cuando se requiera, en un dispositivo adecuado de procesamiento de datos. Por tanto, el programa de ordenador instalado en el dispositivo de procesamiento de datos lleva a cabo las funciones necesarias del dispositivo de clave.

En una forma de realización ventajosa, del dispositivo de clave USB se conecta a un dispositivo de transferencia de datos conectado a la red local. De este modo, el dispositivo de clave USB en primer lugar determina su propio encaminamiento a través de diferentes subredes hacia el servidor de red de control remoto. Cuando se determine el encaminamiento, la información de encaminamiento actual del dispositivo de clave USB se guarda en el servidor de red de control remoto de acuerdo con la invención.

Cuando es necesario conectar un dispositivo de clave nuevo a una disposición existente de control remoto, tanto el dispositivo de clave USB ya operativo como un dispositivo de clave USB nuevo que se va a introducir se conectan al dispositivo usado de transferencia de datos. En esta situación, los dispositivos de bloqueo controlados por el dispositivo de clave USB operativo se muestran en la pantalla del dispositivo usado de procesamiento de datos. A partir de esta lista, el usuario selecciona los dispositivos de bloqueo para los cuales el nuevo dispositivo de clave USB que se conectará al sistema va a actuar como clave. Después de la selección, un mensaje de solicitud para establecer una relación de confianza, confirmado con el certificado del dispositivo de clave USB ya operativo, se envía a los dispositivos de bloqueo seleccionados, cifrado con una clave PKI privada de un dispositivo de clave USB de confianza. Cada dispositivo de bloqueo abre el mensaje recibido con una clave PKI pública de un dispositivo de clave USB de confianza. Después de esto, cada dispositivo de bloqueo comprueba que el certificado recibido se corresponde con el certificado del dispositivo de clave USB emparejado con el mismo y qué certificado es por lo tanto conocido. Si la identificación es satisfactoria, el certificado del

nuevo dispositivo de clave USB que se entregó con el certificado del dispositivo de clave USB de confianza y su clave PKI pública, se guardan en el dispositivo de bloqueo respectivo. Un mensaje sobre el éxito de la identificación y el establecimiento de una relación de confianza se envía al dispositivo de clave USB que envió el mensaje, memorizando dicho dispositivo de clave, sobre la base del mensaje recibido, el certificado del dispositivo de bloqueo conocido en la memoria del dispositivo de bloqueo USB nuevo. Después de esto, el dispositivo de bloqueo respectivo se puede controlar con ambos dispositivos de clave USB. Cuando se han establecido satisfactoriamente los nuevos derechos de funcionamiento solicitados (relaciones de confianza con dispositivos de bloqueo) para el dispositivo de clave USB nuevo, el mismo se puede separar del dispositivo de procesamiento de datos y enviar, por ejemplo, por correo, a una persona que tenga el derecho de usar dicho dispositivo de clave nuevo.

En lo sucesivo se describirá la invención de forma detallada. En la descripción, se hace referencia a los dibujos adjuntos, en los cuales

la figura 1 muestra un ejemplo de una disposición de control remoto, en donde puede establecerse una conexión bidireccional de transferencia de datos entre un dispositivo de cliente que gestiona el control remoto y un dispositivo de gestión o control individual de una propiedad,

la figura 2 muestra, en forma de diagrama de flujo ejemplificativo, cómo se asignan derechos de funcionamiento para un dispositivo de clave nuevo

la figura 3 muestra, como diagrama de flujo ejemplificativo, cómo se establece una red privada virtual entre dos dispositivos de bloqueo, y

la figura 4 muestra, a título de ejemplo, un dispositivo de clave USB según la invención.

Las formas de realización de la siguiente descripción se aportan únicamente como ejemplos, y una persona versada en la materia puede materializar la idea básica de la invención también de alguna manera diferente a la que se describe en la descripción. Aunque la descripción puede referirse a una cierta forma de realización o formas de realización en diversos lugares, esto no significa que la referencia vaya dirigida a solamente una forma de realización descrita o que la característica descrita sea utilizable solamente en una forma de realización descrita. Las características individuales de dos o más formas de realizaciones se pueden combinar, y por lo tanto, se pueden proporcionar formas de realización nuevas de la invención.

La figura 1 muestra una forma de realización ventajosa 1 del sistema de control remoto. En el ejemplo de la figura 1, con un dispositivo de clave USB 34 se establece una conexión de transferencia de datos, utilizando un dispositivo de procesamiento de datos 32, hacia un dispositivo de bloqueo 61 situado en una propiedad en algún otro lugar. No obstante, el dispositivo de clave USB 32 puede funcionar también, ventajosamente, con dispositivos de bloqueo independientes (no mostrados en la figura 1) situados en dos o más propiedades.

En la figura 1, Internet se designa con la referencia 2. Alguna red pública o una intranet, referencia 3, está conectada también a Internet 2. La red 3 puede ser una red de transferencia de datos fija o inalámbrica. En la figura 1, un dispositivo de cliente 32 que implementa un control remoto se une a la red 3. Para obtener la conexión de control remoto, el dispositivo de clave USB 34 se conecta al puerto USB 33 del dispositivo de cliente.

La intranet doméstica en la propiedad a controlar de manera remota se designa con la referencia 5 en la figura 1. Dispositivos ejemplificativos de procesamiento de datos, referencias 55 y 56, están conectados a la red de intranet doméstica 5. Además, otra red de transferencia de datos 6, una intranet de control doméstica, está conectada a la red de intranet doméstica 5. Los accionadores 62 a 65 que se van a controlar de manera remota en la propiedad se conectan a la intranet de control doméstica 6 o bien con una conexión de transferencia de datos inalámbrica o bien con una conexión por cable.

El dispositivo de clave USB 34 y el dispositivo de bloqueo 61 necesitan la información de encaminamiento mutua a través de Internet 2, para poder establecer entre ellos una conexión de transferencia de datos de extremo-a-extremo basada en la capa de enlace de datos o la capa de red, en el ejemplo de la figura 1, una conexión de transferencia de datos VPN 41. La información de encaminamiento en tiempo real, determinada, es guardada tanto por el dispositivo de clave USB 34 como por el dispositivo de bloqueo 61 en un servidor de red de control remoto 21 en Internet por medio de la conexión 42.

Para que sea posible establecer la conexión de transferencia de datos, el dispositivo de clave USB 34 y el dispositivo de bloqueo 61 deben determinar su ruta de red real desde su propia red por lo menos hasta Internet 2. Esta determinación de la ruta de red se puede realizar de varias maneras conocidas, las cuales pueden ser utilizadas, de manera ventajosa, por el dispositivo de clave USB 34 y el dispositivo de bloqueo 61.

En el ejemplo de la figura 1, los cortafuegos de NAT 31 (FW2) y 51 (FW1), que separan las redes locales de

Internet, ventajosamente no limitan el tráfico de UDP saliente (Protocolo de Datagrama de Usuario). Por tanto, en el ejemplo de la figura 1, en la capa de enlace de datos puede establecerse una conexión a nivel de Ethernet entre el dispositivo de clave de control remoto 34 y el dispositivo de bloqueo 61, cuando los mismos conocen las direcciones IP del otro.

También en aquellos casos, en los que los cortafuegos 31 y/o 51 limitan el tráfico saliente por lo menos en algunos procedimientos de conexión, los cortafuegos pueden saltarse usando otros protocolos de tráfico adecuados y, por medio de ello, puede establecerse una conexión de transferencia de datos entre el dispositivo de clave USB 34 y el dispositivo de bloqueo 61.

Cuando, en el sistema de control remoto 1 según la figura 1, se desea a establecer una red privada virtual (VPN) 41 entre el dispositivo de procesamiento de datos 32 conectado al dispositivo de clave USB 34 y el dispositivo de bloque 61, entonces, en la primera etapa, ambos dispositivos 34 y 61 recuperan, del servidor de red de control remoto 21, la información de encaminamiento guardada en el mismo, por parte del dispositivo homólogo, por medio de la conexión de transferencia de datos 42. Antes de entregar la información de encaminamiento, el servidor de red de control remoto 21 comprueba que se trata realmente de un par permitido de dispositivo de clave USB – dispositivo de bloqueo. Después de esto, por medio de la información de encaminamiento recuperada, el dispositivo de clave USB 34 y el dispositivo de bloqueo 61 establecen una conexión VPN directa 41 entre ellos. Cuando se completa la conexión VPN 41, un dispositivo de procesamiento de datos 32 en la red de transferencia de datos 3 puede realizar una conexión con uno o más dispositivos 62, 63, 64 o 65 en la red doméstica de control 6.

La figura 2 muestra en forma de un diagrama de flujo ejemplificativo, cómo se utiliza un dispositivo de clave USB existente en el establecimiento de los derechos de funcionamiento, la denominada relación de confianza, de un dispositivo de clave USB nuevo paralelo. En lo sucesivo, a estos dispositivos de clave se les hace referencia como dispositivo de clave USB 1 y dispositivo de clave USB 2. Al dispositivo de clave USB 1 se le puede hacer referencia también con el número de referencia 34 de la figura 1. En el método de establecimiento de una relación de confianza, se utilizan métodos cifrados con una clave PKI privada (método de clave criptográfica pública). Los dispositivos se envían entre sí mensajes cifrados con una clave PKI privada propia, pudiéndose abrir dichos mensajes por parte del dispositivo receptor con la clave PKI pública conocida del dispositivo emisor. El emisor del mensaje se confirma con el certificado del emisor relacionado con el mensaje recibido, siendo conocido dicho certificado por el dispositivo receptor. El certificado, la clave criptográfica privada y la clave criptográfica pública forman conjuntamente la información necesaria en el uso del método PKI.

La etapa 200 describe una situación en la que la disposición de control remoto está en condiciones operativas y en uso. De este modo, por lo menos un dispositivo de bloqueo 61 está conectado al sistema de control remoto 1. En este estado, el dispositivo de bloqueo 6 está preparado constantemente para recibir mensajes o bien de su dispositivo de clave USB 34 (dispositivo de clave USB 1) o bien del servidor de red de control remoto 21, mostrado en la figura 1.

En la etapa 210, se inicia el establecimiento de una relación de confianza de un dispositivo de clave USB nuevo 2 con el dispositivo de bloqueo 61 paralelo a un dispositivo de clave existente 1 (referencia 34 en la figura 1). Ambos dispositivos de clave USB 1 y 2 son de un tipo tal que se pueden conectar a los puertos USB del dispositivo de transferencia de datos 32 en uso. Se inicia el procedimiento de establecimiento de una relación de confianza, cuando al mismo tiempo, tanto el dispositivo de clave USB 1 como el dispositivo de clave USB 2 se conectan a dos puertos USB de un dispositivo de procesamiento de datos 32, siendo necesarios para dichos dispositivos de clave, derechos de funcionamiento para al menos un dispositivo de bloqueo. Después de esto, el software utilizado en el control remoto se activa con el dispositivo de procesamiento de datos 32. El software se puede preinstalar en el dispositivo de procesamiento de datos 32, o el dispositivo de procesamiento de datos inicia la ejecución de dicho programa en el dispositivo de clave USB 34 (dispositivo de clave USB 1).

En esta etapa, todos los dispositivos de bloqueo con los cuales se ha emparejado el dispositivo de clave USB 1 (es decir, existe una relación de confianza entre ellos), se visualizan en la pantalla del dispositivo de procesamiento de datos 32. A partir esta lista se seleccionan un dispositivo de bloqueo o dispositivos de bloqueo con los cuales es necesario emparejar el nuevo dispositivo de clave USB 2. Se forma un mensaje individual sobre la selección para cada dispositivo de bloqueo implicado en el emparejamiento, comprendiendo el mensaje un certificado y una clave PKI pública del dispositivo de clave nuevo 2. El mensaje a enviar se firma con una clave PKI privada del dispositivo de clave USB 1. El mensaje se puede formar, por ejemplo, de la manera siguiente:

Para: Bloqueo 61
De: Clave 1
Mensaje: Permitir conexión de Clave 2
Permiso de emparejamiento: No
Modo fijado: Bloqueo
Certificado: <Certificado Clave 2>

Firma: <Firma Clave 1>

En la etapa 220, el software de control remoto que está funcionando en el dispositivo de procesamiento de datos 32 envía un mensaje al dispositivo de bloqueo 61 formado en la etapa 210, cuya firma se cifra con una clave criptográfica privada del dispositivo de clave USB 1.

En la etapa 230, el dispositivo de bloqueo 61 en primer lugar recibe el mensaje del dispositivo de clave USB 1. A continuación, con una clave PKI pública conocida del dispositivo de clave USB 1, abre el mensaje y la firma del dispositivo de clave relacionado 1. Después de esto, el dispositivo de bloqueo 61 lee también el certificado del otro dispositivo de clave USB 2 incluido en el mensaje.

En la etapa 240, el dispositivo de bloqueo 61 compara el certificado relacionado con la firma recibida del dispositivo de clave USB 1, con el certificado del dispositivo de clave USB 1 guardado en su propia memoria. Si no se produce ninguna coincidencia en la comparación, el proceso finaliza en la etapa 280.

Si el resultado de la comparación en la etapa 240 muestra que el mensaje fue enviado por el dispositivo de clave USB 1, el proceso continúa hacia la etapa 250.

En la etapa 250, el dispositivo de bloqueo 61 establece la relación de confianza solicitada con el dispositivo de clave USB nuevo 2 y, por lo tanto, guarda el certificado del dispositivo de clave USB 2 en su memoria. Después de esto, el dispositivo de bloqueo 61 envía una confirmación de la relación de confianza formada al dispositivo de clave USB 1.

En la etapa 260, el dispositivo de clave USB 1 en primer lugar recibe el mensaje sobre el establecimiento de la relación de confianza, enviado por el dispositivo de bloqueo 61, y después de ello, guarda el certificado del dispositivo de bloqueo conocido 61 en la memoria del dispositivo de clave USB 2.

Después de esto, el dispositivo de clave USB 2 puede actuar como dispositivo de clave del dispositivo de bloqueo 61, etapa 270.

La figura 3 muestra en forma de un diagrama de flujo ejemplificativo, cómo se utiliza un dispositivo de clave USB existente cuando se establece una relación de confianza entre dos dispositivos de bloqueo independientes, presentando dichos dispositivos de bloqueo una relación de confianza existente con el mismo dispositivo de clave USB. A continuación, a los dispositivos de clave se les hace referencia como dispositivo de clave USB y a los dispositivos de bloqueo como dispositivo de bloqueo 1 y dispositivo de bloqueo 2. Al dispositivo de clave USB se le puede hacer referencia también con el número de referencia 34 de la figura 1. El método de establecimiento de una relación de confianza se basa en el uso de claves PKI privadas y públicas (método de clave criptográfica pública). Tanto el dispositivo de clave como los dispositivos de bloqueo 1 y 2 se envían entre sí mensajes firmados con su clave PKI privada, de modo que el dispositivo receptor puede abrir con la clave PKI pública conocida, respectiva, del dispositivo emisor. El dispositivo receptor verifica, con el certificado del dispositivo emisor relacionado con el mensaje, que el mensaje fue enviado realmente por el dispositivo de confianza firmado.

La etapa 300 describe una situación en la que la disposición de control remoto está en condiciones operativas y en uso. De este modo, al menos los dispositivos de bloqueo 1 y 2 están conectados al sistema de control remoto 1. En este estado, los dispositivos de bloqueo 1 y 2 están preparados constantemente para recibir mensajes o bien de su dispositivo de clave USB 34 (dispositivo de clave USB) o bien del servidor de red de control remoto 21, mostrado en la figura 1.

En la etapa 310, se inicia el establecimiento de una relación de confianza entre los dispositivos de bloqueo 1 y 2. Se inicia el procedimiento de establecimiento de una relación de confianza, cuando el dispositivo de clave USB se conecta al puerto USB del dispositivo de procesamiento de datos 32, de manera que, mediante el uso de dicho dispositivo de clave, se desea establecer una relación de confianza entre los dispositivos de bloqueo 1 y 2. Después de esto, el software utilizado en el control remoto de los dispositivos de bloqueo se activa con el dispositivo de procesamiento de datos 32. El software se puede preinstalar en el dispositivo de procesamiento de datos 32, o el dispositivo de procesamiento de datos inicia la ejecución de dicho programa en el dispositivo de clave USB.

En esta etapa, todos los dispositivos de bloqueo con los cuales se ha emparejado el dispositivo de clave USB respectivo (es decir, existe una relación de confianza entre ellos), se visualizan en la pantalla del dispositivo de procesamiento de datos 32. A partir de esta lista, en el ejemplo de la figura 3, se seleccionan el dispositivo de bloqueo 1 y el dispositivo de bloqueo 2, entre los cuales se requiere el establecimiento de una relación de confianza. Al mismo tiempo, se determina el carácter de la relación de confianza, es decir, la manera según la cual los dispositivos de bloqueo establecerán posteriormente redes entre sí. En el ejemplo de la figura 3, la finalidad del establecimiento de una relación de confianza es establecer una conexión de transferencia de datos VPN entre los dispositivos de bloqueo 1 y 2. Después de seleccionar los dispositivos de bloqueo se crea un

mensaje individual para los dos dispositivos de bloqueo, el cual comprende el carácter de la relación de confianza a establecer. Los mensajes a enviar se firman con una clave PKI privada del dispositivo de clave USB, y el certificado del dispositivo de clave USB emisor se incluye en el mensaje.

En la etapa 320, con el software de control remoto, que funciona en el dispositivo de procesamiento de datos 32, se crean los mensajes para los dispositivos de bloqueo 1 y 2, necesarios en el establecimiento de una relación de confianza.

El mensaje para el dispositivo de bloqueo 1 que actuará posteriormente como servidor se puede formar preferentemente de la manera siguiente:

Para: Bloqueo 1
De: Clave
Orden: Permitir conexión de Bloqueo 2
Permiso de Emparejamiento: No
Modo fijado: Bloqueo
Certificado: <Certificado Bloqueo 2>
Firma: <Firma Clave>

El mensaje para el dispositivo de bloqueo 2 que sirve como dispositivo de cliente (dispositivo subordinado) del dispositivo de bloqueo 1 que actuará posteriormente como servidor, se puede formar preferentemente de la manera siguiente:

Para: Bloqueo 2
De: Clave
Orden: Permitir conexión de Bloqueo 1
Permiso de Emparejamiento: No
Modo fijado: Sub-bloqueo
Certificado: <Certificado Bloqueo 1>
Firma: <Firma Clave>

Al final de la etapa 320, el software de control remoto que funciona en el dispositivo de procesamiento de datos 32 envía a los dispositivos de bloqueo 1 y 2 mensajes formados sobre el establecimiento de una relación de confianza, cifrándose dichos mensajes con una clave PKI privada del dispositivo de clave USB. En la transmisión de mensajes se usa ventajosamente el servicio denominado *Matchmaking* (Búsqueda de Coincidencias).

En la etapa 330, los dispositivos de bloqueo 1 y 2 en primer lugar reciben el mensaje sobre el establecimiento de una relación de confianza, enviado por el dispositivo de clave USB al dispositivo de bloqueo respectivo. A continuación, abre el mensaje con una clave PKI pública conocida del dispositivo de clave USB. Los dispositivos de bloqueo comprueban que la firma del dispositivo de clave USB emisor se corresponde con una firma del dispositivo de clave USB en su memoria. Después de esto, los dispositivos de bloqueo leen también el certificado del otro dispositivo de bloqueo incluido en el mensaje.

En la etapa 340, los dispositivos de bloqueo 1 y 2 comparan el certificado recibido del dispositivo de clave USB, relacionado con la firma del dispositivo de clave USB, con el certificado del dispositivo de clave USB guardado en su propia memoria. Si no se produce ninguna coincidencia en la comparación, el proceso finaliza en la etapa 380.

Si el resultado de la comparación de la etapa 340 muestra que el mensaje fue enviado por el dispositivo de clave USB, el proceso continúa a la etapa 350 en ambos dispositivos de bloqueo 1 y 2.

En la etapa 350, los dispositivos de bloqueo 1 y 2 establecen la relación de confianza requerida entre ellos mismos, y, por lo tanto, guardan los certificados mutuos en sus propias memorias. Después de esto, los dispositivos de bloqueo envían una confirmación de la relación de confianza formada también al dispositivo de clave USB.

En la etapa 360, el dispositivo de bloqueo 1 y el dispositivo de bloqueo 2 forman, por medio de certificados conocidos del homólogo, una red VPN entre ellos mismos, donde el dispositivo de bloqueo 1 sirve como dispositivo servidor (dispositivo maestro). El proceso de establecimiento de una red privada VPN entre dos dispositivos de bloqueo es similar a lo que se da a conocer en relación con la figura 1, donde la red privada VPN se establece entre un dispositivo de clave USB y un dispositivo de bloqueo.

Después de esto, todos los mensajes del dispositivo de clave USB viajan al dispositivo de bloqueo 2 siempre por medio del dispositivo de bloqueo 1, etapa 370.

Todas las etapas de proceso mostradas en las figuras 2 y 3 se pueden realizar con órdenes de programa de

ordenador, las cuales se ejecutan en un procesador adecuado de propósito general o de propósito especial. Las órdenes de ordenador se pueden almacenar en un soporte legible por ordenador, tal como un disco de datos o una memoria, de donde el procesador puede recuperar dichas órdenes de programa de ordenador y ejecutarlas. Las referencias a un soporte legible por ordenador también pueden contener, por ejemplo, componentes especiales, tales como memorias Flash USB programables, matrices lógicas (FPLA), circuitos integrados de aplicación específica (ASIC) y procesadores de señales (DSP).

La figura 4 muestra partes principales funciones del dispositivo de clave USB 34. El dispositivo de clave USB 34 puede comprender uno o varios criptoprocesadores 341. El procesador o los medios de procesador pueden comprender una unidad aritmética lógica, un grupo de diferentes registros y circuitos de control. El criptoprocesador 341 comprende ventajosamente una unidad de memoria interna, en la cual se almacena una clave criptográfica privada individual 3421.

Una disposición de almacenamiento de datos 342, tal como unos medios de memoria o unidad de memoria Flash, en donde se pueden almacenar información legible por el ordenador o programas o información de usuario, está conectada a los medios de procesador. Los medios de memoria 342 contienen típicamente unidades de memoria, que permiten funciones tanto de lectura como de escritura (Memoria de Acceso Aleatorio, RAM), y unidades de memoria que contienen memoria no volátil, desde la cual únicamente se pueden leer datos (Memoria de Solo Lectura, ROM). El certificado del dispositivo de clave USB 34, las claves PKI privada y pública, la información de la ruta de red actual del dispositivo de clave USB, la información de identificación de los dispositivos de bloqueo que sirven como sus pares de dispositivo, certificados, las claves PKI públicas de los pares de dispositivos y todos los programas necesarios para el funcionamiento del dispositivo de clave USB 34 que se utilizarán en el establecimiento de la conexión VPN se almacenan ventajosamente en los medios de memoria 342.

Algunos ejemplos de programas almacenados en la memoria del dispositivo de clave de control remoto 34 son un sistema operativo (por ejemplo, Linux), programas de TCP/IP, un programa de VPN (por ejemplo, OpenVPN), o un programa de servidor/dispositivo de cliente de DHCP (por ejemplo, ISC DHCP), un programa de base de datos (por ejemplo, SQLite), un programa de gestión/confirmación de certificados (por ejemplo, GPG) y una biblioteca de interfaz de usuario (por ejemplo, LuCI).

El dispositivo de clave USB 34 comprende también elementos de interfaz, los cuales comprenden una entrada/salida o medios de entrada/salida 343 para recibir o enviar información. La información recibida con los medios de entrada se transfiere para ser procesada por los medios de procesador 341 del dispositivo de clave de control remoto 34. Los elementos de interfaz 343 del dispositivo de clave USB 34 se usan ventajosamente para transferir información desde la memoria 342 del dispositivo de clave USB 34, o bien a un dispositivo externo de procesamiento de datos 32 o bien al dispositivo de bloqueo 61 (en el ejemplo de la figura 1). De manera correspondiente, por medio de los elementos de interfaz se pueden recibir información u órdenes, por ejemplo, desde el dispositivo de procesamiento de datos 32, al cual está conectado el dispositivo de clave USB 34.

En relación con los niveles de derechos de funcionamiento, existen por lo menos dos niveles de los dispositivos de clave USB 34 antes descritos, por ejemplo, dispositivos de clave de nivel administrador y usuario básico. Un usuario/propietario (por ejemplo, un administrador) de un nivel de derechos de funcionamiento superior tiene derecho de control sobre todos los objetivos de control de usuarios (tales como usuarios básicos) de dispositivos de clave de control remoto 14 en un nivel inferior (tales como usuarios básicos). Por otro lado, un propietario de un nivel de derecho de funcionamiento de dispositivos de clave de nivel inferior no tiene acceso a ningún otro objetivo de control con un nivel de derechos de funcionamiento superior a sus propios objetivos.

Anteriormente se han descrito algunas formas de realización ventajosas del método y del dispositivo de acuerdo con la invención. La invención no se limita a las soluciones antes descritas, sino que la idea de la misma se puede aplicar de numerosas maneras dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Método para establecer relaciones de confianza nuevas entre unos dispositivos de clave (34) y/o unos dispositivos de bloqueo (61) utilizados en una red privada virtual (41, VPN) en un sistema de control remoto (1) de accionadores de una propiedad, método en el que:

- un dispositivo de clave de confianza (34) está eléctricamente conectado (210, 310) a un dispositivo de procesamiento de datos (32), que está en conexión con Internet (2);

- el dispositivo de clave de confianza (34) determina su ruta de red hacia Internet (2) y guarda su ruta de red en un servidor (21) conectado a Internet (2); y

- el dispositivo de clave de confianza (34) recibe información de ruta de red de por lo menos un dispositivo de bloqueo (61),

caracterizado por que

- el dispositivo de clave de confianza (34) forma una red privada virtual (41) con por lo menos un dispositivo de bloqueo (61);

- el dispositivo de clave de confianza (34) transmite (220, 320) un mensaje cifrado con una clave de cifrado privada del dispositivo de clave de confianza (34) por lo menos a un dispositivo de bloqueo (61), comprendiendo el mensaje un certificado del dispositivo de clave de confianza y un certificado de por lo menos otro dispositivo, con el cual el dispositivo de bloqueo receptor (61) establecerá una relación de confianza, y las definiciones de medidas realizadas en el establecimiento de la relación de confianza;

- un dispositivo de bloqueo (61) abre y confirma (230, 330), con una clave de cifrado pública conocida del dispositivo de clave de confianza (34), la autenticidad de un emisor del mensaje recibido por el mismo;

- el dispositivo de bloqueo guarda (250) unos certificados de los dispositivos relacionados con el mensaje enviado por el dispositivo identificado en su memoria;

- el dispositivo de bloqueo (61) establece una relación de confianza (250, 350) con por lo menos otro dispositivo indicado en el mensaje.

2. Método de establecimiento de una relación de confianza según la reivindicación 1, caracterizado por que otro dispositivo de clave está eléctricamente conectado (210) al dispositivo de procesamiento de datos (32), siendo el certificado incluido por el dispositivo de clave de confianza (34) en un mensaje enviado a por lo menos un dispositivo de bloqueo (61).

3. Método de establecimiento de una relación de confianza según la reivindicación 2, caracterizado por que el dispositivo de clave de confianza (34) recibe un mensaje de confirmación de establecimiento de una relación de confianza desde por lo menos un dispositivo de bloqueo (61), y por que el dispositivo de clave de confianza (34) guarda en la memoria del otro dispositivo de clave el certificado del dispositivo de bloqueo (61) del cual se recibió el mensaje que confirma el establecimiento de la relación de confianza.

4. Método de establecimiento de una relación de confianza según la reivindicación 1, caracterizado por que el dispositivo de clave (34) envía por lo menos a dos dispositivos de bloqueo un mensaje individual independiente que comprende un certificado de por lo menos otro dispositivo de bloqueo y una descripción de una relación funcional entre los dispositivos de bloqueo mencionados en el mensaje.

5. Método de establecimiento de una relación de confianza según la reivindicación 1, caracterizado por que por lo menos dos medios de bloqueo establecen una red privada virtual entre ellos mismos utilizando unos certificados recibidos desde el dispositivo de clave (34), sirviendo en dicha red privada un dispositivo de bloqueo como un dispositivo servidor, y sirviendo por lo menos otro dispositivo de bloqueo como un dispositivo de cliente del servidor.

6. Dispositivo de clave (34) de accionadores del sistema de control remoto de una propiedad, que comprende:

- unos elementos de interfaz de conexión de red, que comprenden unos medios de entrada/salida (343) para conectar el dispositivo de clave a un dispositivo de procesamiento de datos (32) conectado a Internet

- un procesador (341) y

- una memoria (342), que contiene un código de programa de ordenador,

caracterizado por que el dispositivo de clave (34) está configurado para formar una red privada virtual (41) con por lo menos un dispositivo de bloqueo (61), y por que el procesador, la memoria y el código de programa de ordenador guardado en ella están configurados para:

- transmitir (220, 320) desde el dispositivo de clave de confianza (34) un mensaje cifrado con una clave de cifrado privada del dispositivo de clave de confianza (34) por lo menos al dispositivo de bloqueo (61), comprendiendo el mensaje un certificado del dispositivo de clave de confianza y un certificado de por lo menos otro dispositivo, con el cual el dispositivo de bloqueo receptor establecerá una relación de confianza, y unas definiciones de medidas realizadas en el establecimiento de la relación de confianza

- recibir y guardar (260, 350), en su memoria, un mensaje de confirmación de una relación de confianza establecida entre por lo menos el dispositivo de bloqueo (61) y otro dispositivo indicado en el mensaje de confirmación del dispositivo de bloqueo (61).

7. Dispositivo de clave de accionadores de una propiedad según la reivindicación 6, caracterizado por que el procesador, la memoria y el código de programa de ordenador guardado en ella están configurados para incluir en el mensaje enviado a por lo menos un dispositivo de bloqueo (61) un certificado de otro dispositivo de clave conectado eléctricamente (210) a un dispositivo de procesamiento de datos.

8. Dispositivo de clave de accionadores de una propiedad según la reivindicación 7, caracterizado por que el procesador, la memoria y el código de programa de ordenador guardado en ella están configurados para recibir desde por lo menos un dispositivo de bloqueo (61) un mensaje de confirmación de establecimiento de la relación de confianza, y por que el dispositivo de clave de confianza (34) está configurado para guardar en la memoria de otro dispositivo de clave, el certificado del dispositivo de bloqueo (61) del cual se recibió el mensaje que confirma el establecimiento de la relación de confianza.

9. Programa de ordenador que comprende unos medios de código de programa de ordenador guardados en un soporte legible por ordenador para proporcionar unas funciones de dispositivo de clave de un sistema de control remoto de accionadores o para establecer una relación de confianza entre por lo menos dos dispositivos de bloqueo, comprendiendo dichos medios de código de programa de ordenador:

- unos medios de código para determinar una ruta de red desde un dispositivo de clave (34) usado en el establecimiento de una relación de confianza con Internet (2) y para guardar la ruta de red en un servidor de control remoto (21) conectado a Internet (2); y

- unos medios de código para recibir información de ruta de red de por lo menos un dispositivo de bloqueo (61) desde el servidor de red de control remoto (21),

caracterizado por que el programa de ordenador además comprende:

- unos medios de código para formar una red privada virtual (41) con por lo menos un dispositivo de bloqueo (61) por medio de la información de ruta de red y un certificado del dispositivo de bloqueo (61)

- unos medios de código para transmitir (220, 320) desde el dispositivo de clave (34) un mensaje cifrado con una clave de cifrado privada del dispositivo de clave de confianza (34) por lo menos a un dispositivo de bloqueo (61), comprendiendo el mensaje un certificado del dispositivo de clave de confianza y un certificado de por lo menos otro dispositivo de clave u otro dispositivo de bloqueo, con el cual el dispositivo de bloqueo receptor (61) establecerá una relación de confianza, y unas definiciones de medidas realizadas en el establecimiento de la relación de confianza, y

- unos medios de código para recibir (260, 350) un mensaje de confirmación de establecimiento de la relación de confianza del dispositivo de bloqueo desde por lo menos un dispositivo de bloqueo (61) y para guardar el certificado del dispositivo de bloqueo (61) que envió el mensaje en por lo menos la memoria del dispositivo de clave de confianza (34).

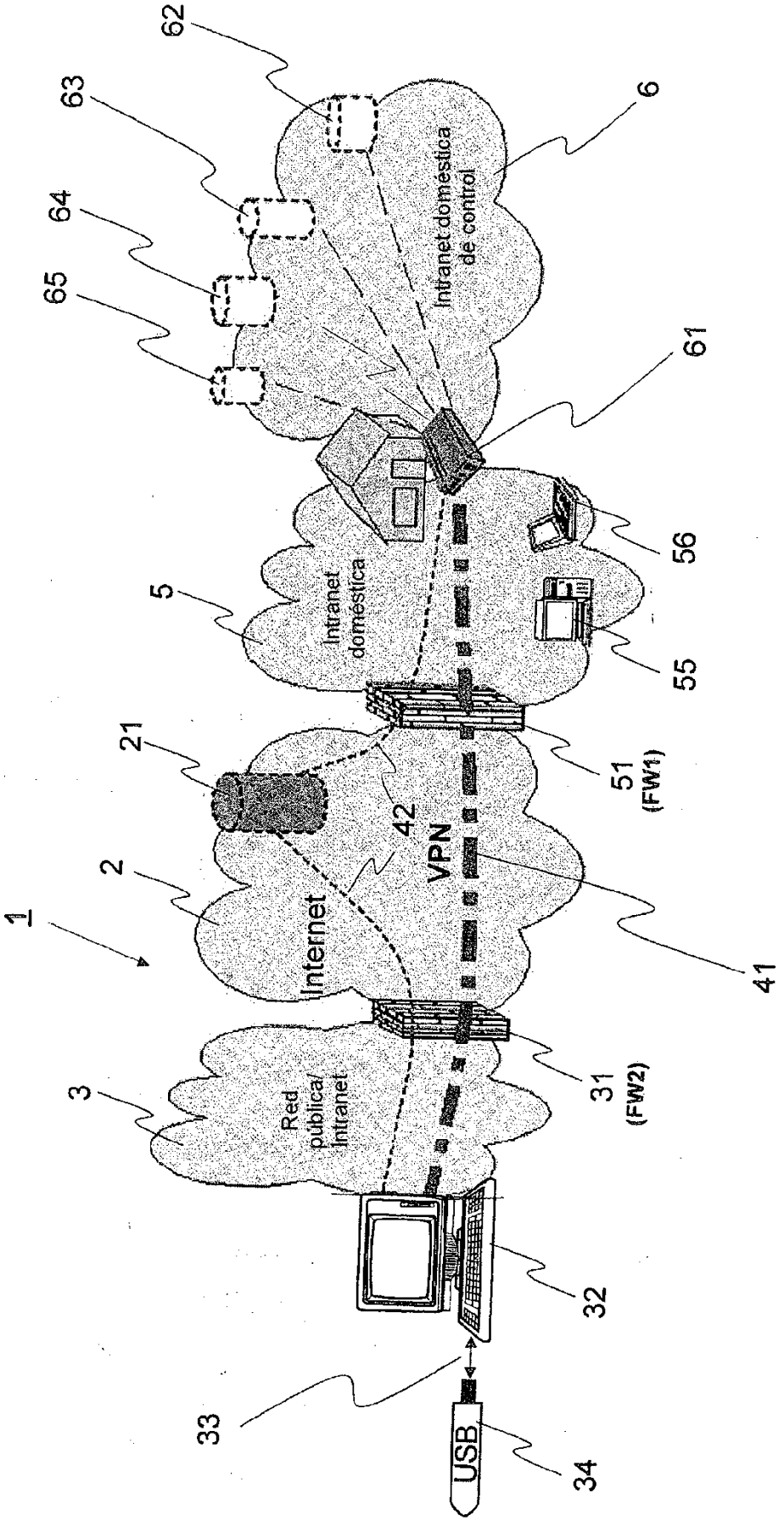
62
63
64
65
6
Intranet doméstica de control
61
56
55
5
Intranet doméstica
51 (FW1)
21
42
VPN
41
2
Internet
1
31 (FW2)
3
Red pública/ Intranet
32
33
USB
34

Fig. 1

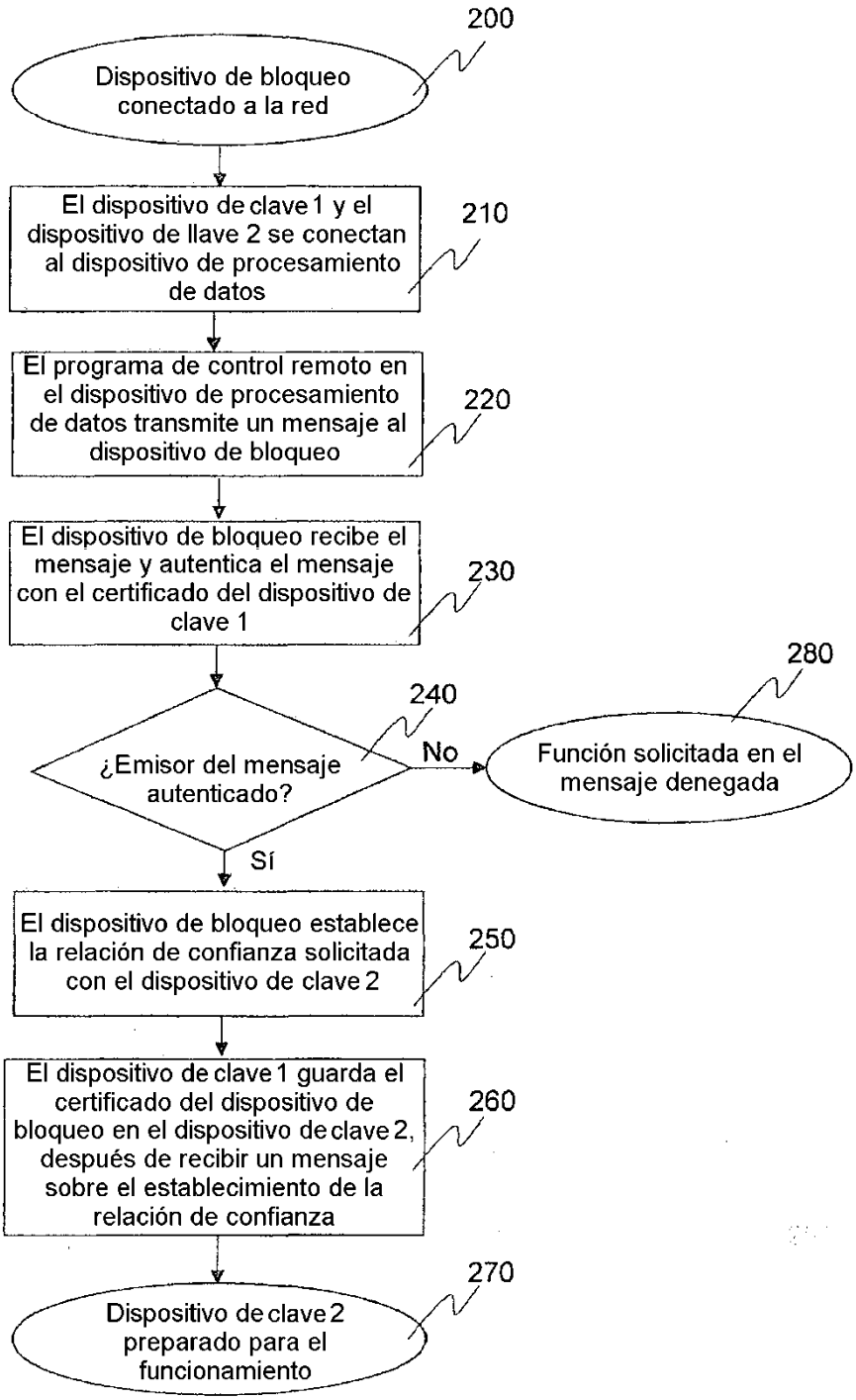
200
Dispositivo de bloqueo conectado a la red
El dispositivo de clave 1 y el dispositivo de llave 2 se conectan al dispositivo de procesamiento de datos
210
El programa de control remoto en el dispositivo de procesamiento de datos transmite un mensaje al dispositivo de bloqueo
220
El dispositivo de bloqueo recibe el mensaje y autentica el mensaje con el certificado del dispositivo de clave 1
230
240
¿Emisor del mensaje autenticado?
No
280
Función solicitada en el mensaje denegada
Sí
El dispositivo de bloqueo establece la relación de confianza solicitada con el dispositivo de clave 2
250
El dispositivo de clave 1 guarda el certificado del dispositivo de bloqueo en el dispositivo de clave 2, después de recibir un mensaje sobre el establecimiento de la relación de confianza
260
Dispositivo de clave 2 preparado para el funcionamiento
270

Fig. 2

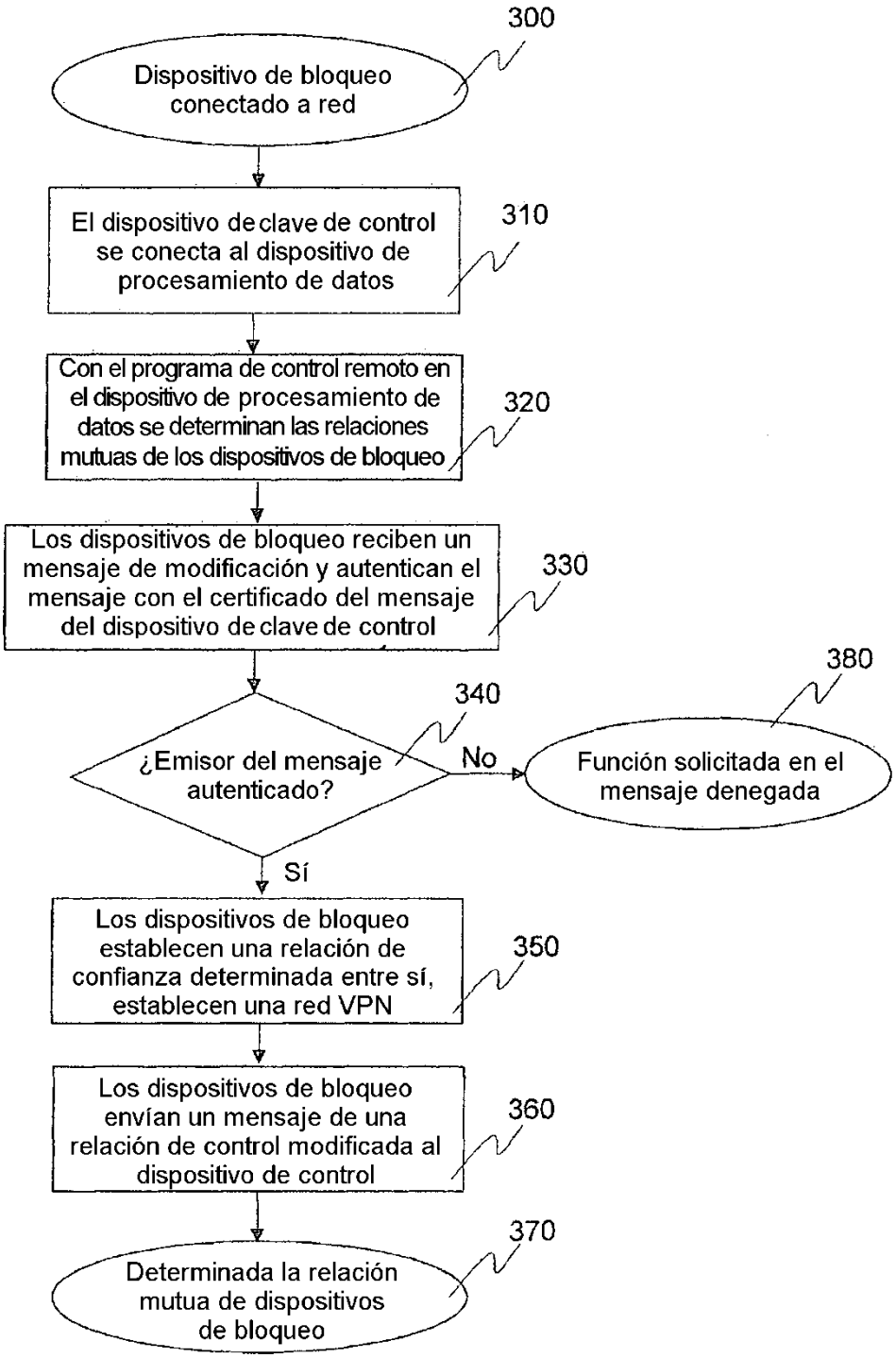
300
Dispositivo de bloqueo conectado a red
El dispositivo de clave de control se conecta al dispositivo de procesamiento de datos
310
Con el programa de control remoto en el dispositivo de procesamiento de datos se determinan las relaciones mutuas de los dispositivos de bloqueo
320
Los dispositivos de bloqueo reciben un mensaje de modificación y autentican el mensaje con el certificado del mensaje del dispositivo de clave de control
330
340
¿Emisor del mensaje autenticado?
No
380
Función solicitada en el mensaje denegada
Sí
Los dispositivos de bloqueo establecen una relación de confianza determinada entre sí, establecen una red VPN
350
Los dispositivos de bloqueo envían un mensaje de una relación de control modificada al dispositivo de control
360
370
Determinada la relación mutua de dispositivos de bloqueo

Fig. 3

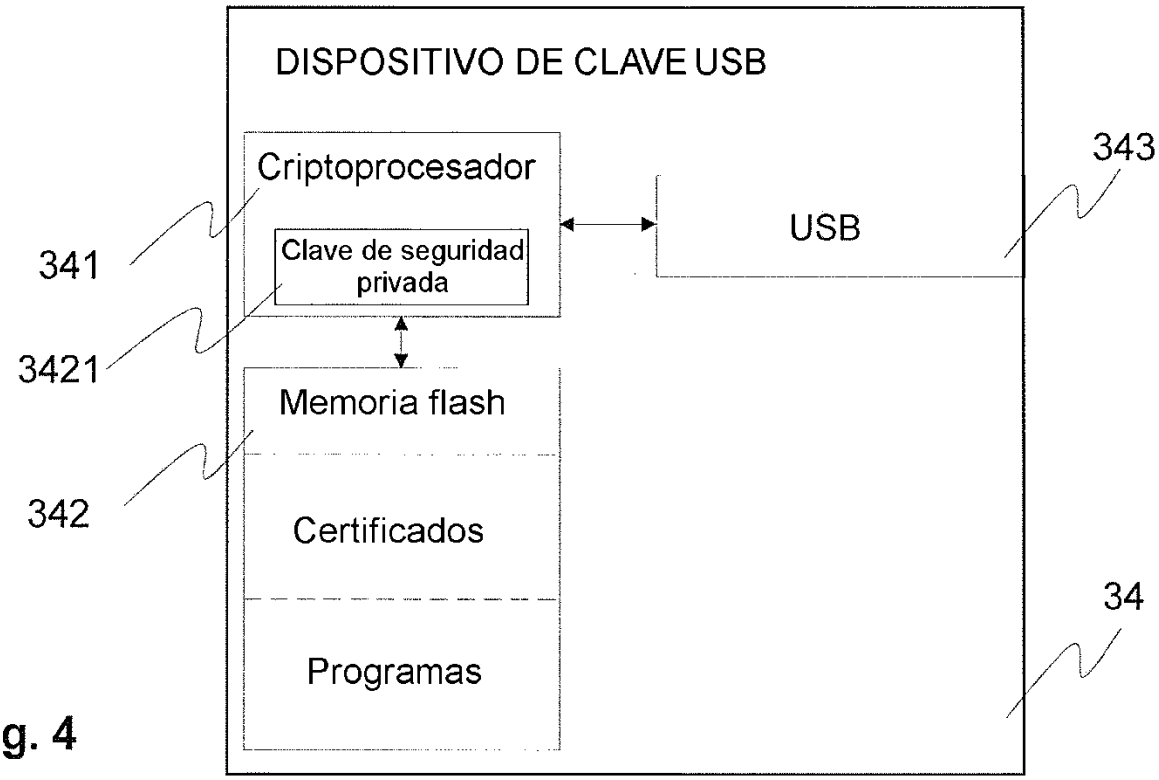
DISPOSITIVO DE CLAVE USB
Criptoprocesador
Clave de seguridad privada
USB
Memoria flash
Certificados
Programas
341
3421
342
343
34

Fig. 4