(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 616 076**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.10.2011 PCT/EP2011/068491**

(87) Fecha y número de publicación internacional: **03.05.2012 WO2012055794**

(96) Fecha de presentación y número de la solicitud europea: **24.10.2011 E 11781464 (0)**

(97) Fecha y número de publicación de la concesión europea: **28.12.2016 EP 2586178**

(54) Título: **Procedimiento para la gestión de claves segura frente a manipulaciones**

(30) Prioridad:

29.10.2010 DE 102010043102

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.06.2017

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München , DE

(72) Inventor/es:

FALK, RAINER;
SATTLER, CARSTEN y
SEIFERT, MATTHIAS

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO PARA LA GESTIÓN DE CLAVES SEGURA FRENTE A MANIPULACIONES

DESCRIPCIÓN

La presente invención se refiere a un procedimiento para la gestión de claves segura frente a manipulaciones, en particular para una red privada virtual.

Estado de la técnica

Los aparatos de campo industriales, como por ejemplo aparatos de control para instalaciones ferroviarias y de vías férreas, comunican cada vez con más frecuencia mediante protocolos de comunicación abiertos como TCP/IP, en lugar de mediante protocolos propietarios. Entonces utilizan los mismos redes públicas como por ejemplo Internet para transmitir datos de comunicación a una central o a otros aparatos de campo. Para proteger la transmisión de datos frente a manipulaciones, se utilizan mecanismos de protección criptográficos, por ejemplo SSL/TSL o IPsec.

No obstante, a menudo no es factible dotar los propios aparatos de campo de una tal técnica de red, por lo que la mayoría de las veces se utilizan aparatos externos para constituir redes privadas virtuales (VPN) para la comunicación de aparatos de campo a través de redes públicas como Internet y para poder garantizar la seguridad necesaria. Tales aparatos externos deben configurarse para la comunicación con datos asegurados criptográficamente. Para ello es necesaria una clave de comunicación criptográfica secreta, con la cual puedan codificarse y decodificarse datos que se envíen y reciban a través de la VPN.

El documento US 2010/0037311 A1 da a conocer una red con nodos de red que disponen en cada caso de un entorno de claves protegido frente a manipulaciones, en el que están memorizadas claves de comunicación.

El documento WO 02/078290 A1 da a conocer procedimientos para iniciar enlaces de comunicación seguros entre nodos de una red privada virtual.

La configuración de los aparatos externos puede ser costosa, en particular cuando tras presentarse una falta es necesaria una reconfiguración. Una posibilidad es dirigirse a los aparatos externos localmente y reconfigurarlos. Esta posibilidad requiere mucho tiempo. Otra posibilidad adicional es la reconfiguración autónoma de los aparatos externos, lo que desde luego implica ciertos riesgos en cuanto a la seguridad para los datos de configuración memorizados en los aparatos externos.

Existe por lo tanto la necesidad de un procedimiento para gestionar claves para un aparato VPN externo para aparatos de campo, con el que con una configuración sencilla quede garantizada a la vez una elevada seguridad de los datos criptográficos.

Resumen de la invención

Una forma de realización de la presente invención de acuerdo con la reivindicación 1 consiste por lo tanto en un procedimiento para la gestión de claves segura frente a manipulaciones para una red privada virtual, en el que la autentificación de un aparato terminal de comunicación se realiza en un servidor de autentificación con ayuda de una primera clave a través de una red pública. Tras realizarse la autentificación con éxito, se proporciona de forma protegida a través de la red pública una clave de comunicación para el aparato terminal de comunicación autentificado, que es adecuada para la comunicación a través de una red privada virtual en la red pública. A continuación se codifica la clave de comunicación en el aparato terminal de comunicación con ayuda de una segunda clave, que proporciona un equipo de vigilancia protegido frente a manipulaciones. Este procedimiento tiene la ventaja de que es posible configurar un aparato terminal de comunicación para una comunicación en una red privada virtual a través de una red pública, sin que peligre la seguridad de los datos criptográficos necesarios para la comunicación a través de la red privada virtual frente a manipulaciones en el aparato terminal de comunicación.

Ventajosamente incluye un procedimiento de acuerdo con la invención la detección de procesos de manipulación en el equipo de vigilancia protegido frente a manipulaciones y la invalidación de la segunda clave cuando se detecta un proceso de manipulación en el equipo de vigilancia protegido frente a manipulaciones. Esto tiene la ventaja de que en un ataque a la red privada virtual en el lado del aparato terminal de comunicación se inutilizan con fiabilidad los datos criptográficos.

Ventajosamente se memoriza en una memoria la clave de comunicación codificada con ayuda de la segunda clave, con lo que la decodificación por parte del aparato terminal de comunicación de la clave de comunicación memorizada sólo es posible con ayuda de la segunda clave.

En una forma de realización preferente del procedimiento se vigila el estado del suministro de energía del equipo de vigilancia protegido frente a manipulaciones y se invalida la segunda clave cuando el suministro de energía es insuficiente en el equipo de vigilancia protegido frente a manipulaciones. Con ello puede garantizarse la seguridad de los datos criptográficos incluso en el caso de un fallo del suministro de energía.

Según otra forma de realización de la presente invención incluye un equipo para la gestión de claves de protegida frente a manipulaciones para una red privada virtual según la reivindicación 7 un aparato terminal de comunicación

con una primera clave, estando diseñado el aparato terminal de comunicación para autentificarse en un servidor de autentificación con ayuda de la primera clave a través de una red pública y comunicar a través de una red privada virtual en la red pública con una clave de comunicación proporcionada de manera protegida mediante el servidor de autentificación, un equipo de vigilancia diseñado para proporcionar una segunda clave, detectar procesos de manipulación en el equipo y que cuando se detecta un proceso de manipulación invalida la segunda clave y una memoria diseñada para memorizar la clave de comunicación codificada con ayuda de la segunda clave. El equipo de acuerdo con la invención permite ventajosamente a aparatos de campo comunicar con seguridad en una red pública a través de una red privada virtual, sin que cuando exista una manipulación en el equipo peligre la seguridad de los datos criptográficos necesarios para la red privada virtual.

Ventajosamente sólo puede acceder el aparato terminal de comunicación a la clave de comunicación codificada memorizada en la memoria con ayuda de la segunda clave.

Según una forma de realización, incluye el equipo una fuente de alimentación que suministra energía al equipo de vigilancia y al aparato terminal de comunicación y un acumulador de energía, que está conectado con la fuente de alimentación y que está diseñado para suministrar energía temporalmente al equipo de vigilancia cuando se interrumpe el suministro de energía mediante la fuente de alimentación. Con ello puede garantizarse incluso en caso de un fallo del suministro eléctrico la seguridad de los datos criptográficos, ya que el equipo de vigilancia puede funcionar, al menos temporalmente, con independencia de la fuente de alimentación principal e iniciar las medidas de seguridad necesarias.

Otras modificaciones y variaciones resultan de las características de las reivindicaciones dependientes.

Breve descripción de las figuras

A continuación se describirán con más precisión diversas formas de realización y variantes de la presente invención con referencia a los dibujos adjuntos, en los que muestra la

figura 1 una representación esquemática de un entorno VPN según una forma de realización de la invención;
figura 2 una representación esquemática de un aparato de campo con un equipo para establecer una VPN según otra forma de realización de la invención; y
figura 3 un esquema de un procedimiento para una gestión de claves protegida frente a manipulaciones según otra forma de realización de la invención.

Las mejoras y perfeccionamientos descritos pueden combinarse entre sí de cualquier manera, siempre que ello tenga sentido. Otras posibles mejoras, perfeccionamientos e implementaciones de la invención incluyen también combinaciones no citadas explícitamente de características de la invención descritas antes o a continuación en relación con los ejemplos de realización.

Los dibujos adjuntos deben proporcionar una comprensión adicional de las formas de realización de la invención. Los mismos visualizan formas de realización y sirven en relación con la descripción para clarificar principios y conceptos de la invención. Otras formas de realización y muchas de las ventajas citadas resultan en relación con los dibujos. Los elementos de los dibujos no se muestran necesariamente a escala uno respecto a otro. Las mismas referencias designan aquí componentes iguales o que funcionan de igual manera.

Descripción detallada de la invención

La figura 1 muestra una representación esquemática de un entorno VPN 10 según una forma de realización de la invención. El entorno VPN 10 incluye un aparato de campo 11. El aparato de campo 11 puede ser por ejemplo un aparato de control para una instalación ferroviaria o de vías férreas, por ejemplo para agujas de control, una barrera o una señal. El aparato de campo 11 puede no obstante ser cualquier otro aparato remoto, como por ejemplo una estación meteorológica o un semáforo. Para que el aparato de campo 11 pueda intercambiar con una estación central 17, como por ejemplo un puesto de enclavamiento, mensajes de control y datos de control, existe un equipo de comunicación 12, conectado con el aparato de campo 11 y que comunica a través de una red 15 con una estación interlocutora 16, conectada a su vez con la estación central 17. El equipo de comunicación 12 puede estar constituido como aparato externo o bien estar integrado en el aparato de campo 11.

La transmisión de los datos de control se realiza a través de la red 15, que puede ser una red pública, como por ejemplo Internet, una red de telefonía móvil, como por ejemplo UMTS, LTE o WiMAX, una red inalámbrica como por ejemplo WLAN, una red ethernet, una red token-ring u otra red comparable. Los datos de control que se transmiten a través de la red 15 están sometidos por lo tanto a ataques potenciales. Por ello se ha establecido para la comunicación entre el equipo de comunicación 12 y la estación interlocutora 16 una red privada virtual 15a (VPN), a través de la cual puedan enviarse y recibirse datos con protección criptográfica mediante la codificación correspondiente. Para la codificación puede utilizarse cualquiera de las técnicas de codificación conocidas, como por ejemplo IPsec, IKE, EAP, SSL/TLS, MACsec, L2TP, PPTP, PGP, S/MIME o técnicas similares. La codificación puede estar configurada entonces como un cálculo de una suma de comprobación criptográfica (Message Authentication Code, Digital Signatur; código de autentificación del mensaje, firma digital) y la decodificación como la comprobación de una suma de comprobación criptográfica.

El equipo de comunicación 12 dispone por lo tanto de una (o varias) clave(s) de comunicación, con la(s) que se codifican criptográficamente los datos de control del aparato de campo 11 a enviar y se decodifican criptográficamente los datos a recibir para el aparato de campo 11. Una clave de comunicación puede utilizarse directamente. Igualmente puede utilizarse la clave de comunicación en un protocolo de autentificación y de acuerdo de claves, como por ejemplo en el protocolo IKE, para establecer una clave de sesión. La clave de sesión establecida puede entonces utilizarse para la transmisión protegida criptográficamente de mensajes de control y/o datos de control con la estación interlocutora 16. El equipo de comunicación 12 incluye un aparato terminal de comunicación 13, que por ejemplo puede ser un microprocesador, que a través de las correspondientes interfaces de comunicación puede establecer una comunicación a través de la red 15. En particular puede estar diseñado el aparato terminal de comunicación 13 para establecer una VPN. El equipo de comunicación 12 incluye además un equipo de vigilancia 14 protegido frente a manipulaciones, un llamado “Tamper-Watchdog” (derivado de los conceptos del inglés “tamper”, que significa "manipular, entrometerse” y “watchdog”, que significa “perro guardián”). El equipo de vigilancia 14 protegido frente a manipulaciones y su forma de funcionamiento se describirán posteriormente en relación con la figura 2.

El entorno VPN 10 incluye además un servidor 18, que dispone de las llamadas funciones “bootstrapping” (da autoarranque), por ejemplo un servidor de autentificación. El bootstrapping designa una transmisión entre aparatos terminales y servidores previamente desconocidos entre sí, que permite la autentificación unilateral o mutua y a raíz de ello el intercambio de claves secretas, con lo que resulta posible un mayor aprovechamiento de aplicaciones que presuponen una autentificación y una relación de comunicación segura. El servidor 18 dispone de una dirección, por ejemplo de una dirección IP o de una URL, que puede estar fijamente programada o ser variable mediante ajuste en el equipo de comunicación 12. En una forma de realización la dirección del servidor 18 es una dirección del fabricante del equipo de comunicación 12. En otra forma de realización la dirección del servidor 18 es una dirección del operador del equipo de comunicación 12. No obstante es posible también determinar mediante otra dirección del equipo de comunicación 12 primeramente otra dirección de un servidor 18 competente para el correspondiente equipo de comunicación 12 y a continuación construir la otra dirección para establecer un enlace bootstrapping con el servidor 18. También puede ser factible consultar un banco de datos para la elección del servidor 18 correspondiente en cada caso a un equipo de comunicación 12. Además puede ser factible hacer depender la elección de la dirección del correspondiente servidor 18 de un lugar de estancia físico del aparato de campo 11, por ejemplo de datos GPS u otras coordenadas espaciales. El servidor 18 puede estar integrado también en la estación interlocutora 16, o también puede ser factible que la estación interlocutora 16 disponga de la correspondiente funcionalidad bootstrapping. En una variante puede estar conectado el servidor 18 también directamente con el equipo de comunicación 12. Debe quedar claro que es posible una pluralidad de posibilidades adicionales para la asignación de un servidor 18 al correspondiente equipo de comunicación 12.

Una configuración VPN incluye por ejemplo informaciones sobre la dirección del servidor 18, la dirección de la estación interlocutora 16, una clave pública o bien un certificado digital de la estación interlocutora 16, el protocolo VPN a utilizar, descripción de los ajustes de seguridad, por ejemplo de la clave y del modo para el correspondiente enlace VPN 15a y/o reglas de filtrado sobre el tráfico de datos admisible. Estas informaciones pueden estar presentes textualmente, por ejemplo como par de atributo y valor o como documento XML. Puede ser también factible establecer varios enlaces VPN 15a para un aparato de campo 11, para realizar por ejemplo distintas clases de tráfico, por ejemplo control, vigilancia, acceso de mantenimiento y funciones similares en enlaces VPN 15a separados.

La figura 2 muestra una representación esquemática de un aparato de campo 20 con un equipo para establecer una VPN de acuerdo con otra forma de realización de la invención. El aparato de campo 20 incluye un aparato terminal de comunicación 13, un equipo de vigilancia 14 protegido frente a manipulaciones, una interfaz de comunicación 21 con entradas y salidas de comunicación 28, una memoria 22 y una fuente de alimentación 26.

El aparato terminal de comunicación 13 está conectado con el equipo de vigilancia 14 protegido frente a manipulaciones, la interfaz de comunicación 21 y la memoria 22. El aparato terminal de comunicación 13 puede ser por ejemplo una unidad de cálculo/unidad de control como por ejemplo un microprocesador, que a través de la interfaz de comunicación 21, por medio de entradas y salidas de comunicación 28, puede establecer una comunicación, en particular una comunicación VPN con un ordenador de gestión de orden superior, como por ejemplo una estación central 17 en la figura 1. La interfaz de comunicación 21 puede estar diseñada para establecer enlaces con distintas redes, por ejemplo Internet, una red de telefonía móvil como por ejemplo UMTS, LTE o WiMAX, una red inalámbrica, como por ejemplo WLAN, una red Ethernet, una red token-ring u otra red comparable. Puede estar previsto que el aparato de campo 20 disponga de varias interfaces de comunicación 21 distintas, que pueden controlarse mediante el aparato terminal de comunicación 13.

La memoria 22 puede ser por ejemplo un módulo de memoria, en el que de manera duradera y reescribible pueden archivarse ajustes de configuración del aparato terminal de comunicación13, por ejemplo una EEPROM serie, una memoria flash o un equipo de memoria comparable. En particular está diseñada la memoria 22 para memorizar claves que pueden configurarse y claves que no pueden configurarse. La memorización se realiza entonces mediante el aparato terminal de comunicación 13.

El aparato terminal de comunicación 13 está conectado con un equipo de vigilancia 14 protegido frente a manipulaciones, por ejemplo un “tamper-watchdog”. El equipo de vigilancia 14 protegido frente a manipulaciones puede incluir por ejemplo un circuito integrado, un módulo lógico programable, como un GAL ó FPGA o un

microprocesador. El equipo de vigilancia 14 protegido frente a manipulaciones puede estar conectado con una interfaz de entrada/salida 24, a través de la que es posible una comunicación con el exterior a través de conexiones de entrada/salida 27 y a las que pueden conectarse otros aparatos, como por ejemplo un sensor 23. El sensor 23 puede ser por ejemplo un sensor "tamper", es decir, un sensor que puede detectar una manipulación física en el aparato de campo 20 o en partes del aparato de campo 20. En particular puede estar diseñado el sensor 23 para vigilar la zona 29 abarcada por trazos dentro del aparato de campo 20. La zona 29 puede incluir por ejemplo el equipo de vigilancia 14 protegido frente a manipulaciones, el propio sensor 23 y la interfaz de entrada/salida 24. No obstante es posible también que la zona 29 incluya otras partes integrantes del aparato de campo 20, por ejemplo el aparato terminal de comunicación 13, la memoria 22, la fuente de alimentación 26 y/o la interfaz de comunicación 21. Además es posible conectar varios sensores 23 a la interfaz de entrada/salida 24, para vigilar diversas zonas 29 del aparato de campo 20 y/o para poder captar diversos procesos físicos de manipulación. El sensor 23 puede incluir por ejemplo una barrera de luz, un sensor de temperatura, un interruptor externo, un sensor de campo magnético o dispositivos similares. En particular puede estar previsto que el aparato de campo 20 esté alojado en un armario de maniobra, cuya puerta pueda vigilarse mediante un sensor de conexión para detectar una apertura no autorizada. Igualmente puede detectar un sensor 23 una apertura de la carcasa del aparato de campo 20 o el desmontaje del aparato de campo 20 de un soporte. El sensor 23 puede estar integrado, al igual que la interfaz de entrada/salida 24, en el equipo de vigilancia 14 protegido frente a manipulaciones.

El aparato de campo 20 puede disponer además de una fuente de alimentación externa, que puede aportarse mediante la unidad de suministro de energía 26. La unidad de suministro de energía 26 puede estar diseñada para suministrar energía a diversos componentes del aparato de campo 20, por ejemplo corriente eléctrica. En particular pueden alimentarse con corriente eléctrica el aparato terminal de comunicación 13, la interfaz de comunicación 21, el equipo de vigilancia 14 protegido frente a manipulaciones y la interfaz de entrada/salida 24.

Al equipo de vigilancia 14 protegido frente a manipulaciones puede estar conectado un acumulador de energía 25, en el que puede almacenarse temporalmente energía para el suministro de energía al equipo de vigilancia 14 protegido frente a manipulaciones. El acumulador de energía 25 puede ser por ejemplo un condensador de tampón (buffer), por ejemplo un condensador de doble capa. El acumulador de energía 25 puede así proporcionar temporalmente electricidad para el suministro de energía al equipo de vigilancia 14 protegido frente a manipulaciones, cuando falle la unidad de suministro de energía 26 o la fuente de alimentación externa. Puede estar previsto por ejemplo que el equipo de vigilancia 14 protegido frente a manipulaciones detecte cuándo debe recurrirse al acumulador de energía 25 para garantizar un suministro de energía suficiente. En este caso puede realizarse una desconexión controlada y tomarse las correspondientes medidas de seguridad para los datos de comunicación y claves, para garantizar la seguridad del aparato de campo 20. El acumulador de energía 25 puede por lo tanto elegirse convenientemente tal que la energía acumulada sea suficiente al menos para ejecutar las medidas de seguridad deseadas. De esta manera es posible ventajosamente una vigilancia de manipulaciones independientemente del aparato terminal de comunicación 13 y el consumo de energía de esta vigilancia puede minimizarse selectivamente, sin que debido a ello quede comprometida la seguridad de los datos de comunicación del aparato de campo 20.

El aparato de campo 20 puede presentar una protección frente a manipulaciones total o parcialmente física, por ejemplo embutiéndolo en resina epoxi y dotándolo de sensores de manipulación, que pueden detectar una manipulación, por ejemplo una penetración en la masa colada. Tales sensores son por ejemplo láminas, las llamadas “tamper-meshes” (mallas de manipulación). Estas láminas incluyen mallas de vías conductoras, que pueden adherirse alrededor de aparatos a proteger. Un intento de manipulación de un aparato así protegido provoca interrupciones y/o cortocircuitos, que aportan la correspondiente señal para un sensor. Es posible dotar el aparato de campo por completo o sólo en parte de las antes citadas medidas de protección frente a manipulación. Puede ser ventajoso por ejemplo dotar sólo la zona 29 de la figura 2 de la correspondiente protección frente a manipulaciones. Debe quedar claro que es posible una pluralidad de variantes para la protección frente a manipulaciones.

La figura 3 muestra un esquema de un procedimiento 30 para la gestión de claves segura frente a manipulaciones según otra forma de realización de la invención. El procedimiento 30 puede realizarse entonces en particular mediante un aparato de campo y un equipo de comunicación según una variante de una de las figuras 1 ó 2.

En una primera etapa 31 se realiza una autentificación de un aparato terminal de comunicación, como por ejemplo del aparato terminal de comunicación 13 de la figura 2 en un servidor de autentificación, por ejemplo un servidor 18 en la figura 1, con ayuda de una primera clave a través de una red pública. Para ello se autentifica el aparato terminal de comunicación mediante una red pública, como por ejemplo Internet o una red de telefonía móvil. La primera clave puede ser entonces por ejemplo una clave del aparato, que es específica para el correspondiente aparato terminal de comunicación y que por ejemplo puede introducirse por programación en fábrica durante la fabricación. La primera clave puede estar archivada en una memoria, como por ejemplo la memoria 22 en la figura 2. La comunicación entre el aparato terminal de comunicación y el servidor de autentificación puede realizarse por ejemplo protegida mediante SSL/TLS. La primera clave puede ser por ejemplo una Private Key (clave privada) ECC ó RSA. No obstante queda claro que también son procedentes otras clases de clave para la primera clave, como por ejemplo un Key Pair (par de claves) pública/privada o una clave simétrica.

En una segunda etapa 32 se aporta una clave de comunicación, que es adecuada para la comunicación a través de una red privada virtual (VPN) en la red pública para el aparato terminal de comunicación autentificado a través de la red pública. Entonces pueden aportarse ajustes de configuración VPN, que incluyen la clave de comunicación. La

clave de comunicación puede incluir cualquier clase de claves que sean adecuadas para un enlace VPN, por ejemplo una clave IPsec. La clave de comunicación puede transferirse en particular al aparato terminal de comunicación cuando ha tenido éxito una autentificación del aparato terminal de comunicación por parte del servidor de autentificación. Esto puede incluir entre otros la comprobación de la primera clave y/o la comprobación del estado correcto de funcionamiento del aparato terminal de comunicación.

En una tercera etapa 33 se realiza la codificación de la clave de comunicación en el aparato terminal de comunicación con ayuda de una segunda clave, que proporciona un equipo de vigilancia protegido frente a manipulaciones. El equipo de vigilancia protegido frente a manipulaciones puede transferir para ello un parámetro TPSP como segunda clave al aparato terminal de comunicación. El parámetro TPSP puede generarse por ejemplo mediante un generador aleatorio y presentar un valor determinado aleatoriamente. El parámetro TPSP puede entonces ventajosamente tener validez mientras no se detecte ningún intento de manipulación mediante el equipo de vigilancia protegido frente a manipulaciones y/o quede garantizado un aporte suficiente de energía al equipo de vigilancia protegido frente a manipulaciones. En el caso de una manipulación o de que el nivel de suministro de energía al equipo de vigilancia protegido frente a manipulaciones quede por debajo de un nivel crítico, puede por ejemplo invalidarse el parámetro TPSP válido en ese momento o sobreescribirse por otro valor TPSP2 generado aleatoriamente.

El aparato terminal de comunicación recibe la segunda clave, por ejemplo el parámetro TPSP, del equipo de vigilancia protegido frente a manipulaciones y genera a partir del mismo una clave de codificación TPCEK, que puede utilizarse para codificar la clave de comunicación. El parámetro TPSP puede por ejemplo recibirse sólo cuando el aparato terminal de comunicación se autentifica frente al equipo de vigilancia protegido frente a manipulaciones. También es posible que el parámetro TPSP pueda depender de un parámetro proporcionado por el aparato terminal de comunicación, como por ejemplo un número de serie o una clave de aparato. La clave de codificación TPCEK puede ser por ejemplo una clave simétrica, por ejemplo una clave AES. Entonces puede incluir la clave de codificación TPCEK bien directamente el parámetro TPSP o bien generarse mediante una derivación de clave en el aparato terminal de comunicación como función del parámetro TPSP. Entonces pueden utilizarse procedimientos de derivación de clave conocidos, como por ejemplo SHA-1, HMAC, CB-MAC o procedimientos similares. Además puede estar previsto incluir otros parámetros además del parámetro TPSP en la derivación de claves para la clave de codificación TPCEK, por ejemplo una cadena de caracteres fija, parámetros memorizados, parámetros de hardware como por ejemplo un número de aparato de campo o un número de serie MAC del aparato terminal de comunicación o parámetros similares.

Tras la codificación de la clave de comunicación mediante el aparato terminal de comunicación puede borrarse la clave de codificación TPCEK utilizada para la codificación en el aparato terminal de comunicación. La clave de comunicación codificada puede memorizarse codificada en una memoria. Cuando el aparato terminal de comunicación debe acceder a continuación para realizar la comunicación a través del VPN a la clave de comunicación, debe solicitarse primeramente la segunda clave, por ejemplo el parámetro TPSP del equipo de vigilancia protegido frente a manipulaciones. Esto sólo es posible - tal como se ha explicado antes - cuando no se ha detectado ningún intento de manipulación. Con ello queda protegida con seguridad la clave de comunicación codificada frente a intentos de manipulación en el aparato de campo.

En una cuarta etapa 34 puede estar previsto generar una clave de integridad con ayuda de la segunda clave para comprobar la integridad de la clave de comunicación memorizada. La clave de integridad TPCIK puede entonces estar constituida similarmente a la clave de codificación TPCEK. En particular puede estar previsto incluir para deducir la clave correspondiente a la clave de integridad TPCIK otra cadena de caracteres como parámetro adicional diferente a la de la clave de codificación TPCEK. La clave de integridad puede utilizarse entonces para verificar la integridad de la configuración memorizada en una memoria como la memoria 22 en la figura 2.

Cuando un aparato terminal de comunicación detecta en una activación, por ejemplo una conexión mediante aplicación de una tensión de alimentación, que no existe ninguna configuración válida y/o que puede decodificarse, por ejemplo porque se ha detectado un comportamiento incorrecto como un intento de manipulación o una interrupción del suministro de energía externo y la correspondiente segunda clave ha sido invalidada por el equipo de vigilancia protegido frente a manipulaciones, se inicia de nuevo un procedimiento bootstrapping a través de un enlace VPN. También puede estar previsto que el propio equipo de vigilancia protegido frente a manipulaciones transmita en el caso de un intento de manipulación una señal de alarma al aparato terminal de comunicación, que puede desencadenar a continuación las correspondientes medidas de bootstrapping. Esto ofrece la ventaja de que por ejemplo después de un comportamiento incorrecto no crítico, como un fallo de la corriente, el aparato terminal de comunicación puede configurarse de nuevo por sí mismo, sin que sea necesario configurar localmente el aparato de campo, lo cual ahorra mucho tiempo y trabajo al personal de mantenimiento. A la vez es más fácil con el procedimiento de acuerdo con la invención realizar un borrado de claves “más agresivo”, es decir, aplicar valores de umbral inferiores para la detección de intentos de manipulación o para determinar un estado de suministro de energía insuficiente, ya que se evita por lo general una costosa nueva puesta en servicio mediante el procedimiento de configuración de acuerdo con la invención.

REIVINDICACIONES

1. Procedimiento (30) para la gestión de claves segura frente a manipulaciones para una red privada virtual (15a), que incluye:
   a) autentificación de un aparato terminal de comunicación (13) en un servidor de autentificación (18) con ayuda de una primera clave a través de una red pública (15);
   b) aportación protegida mediante el servidor de autentificación (18) de una clave de comunicación, que es adecuada para la comunicación a través de una red privada virtual (15a) en la red pública (15), para el aparato terminal de comunicación (13) autentificado a través de la red pública (15); y
   c) codificación de la clave de comunicación en el aparato terminal de comunicación (13) con ayuda de una segunda clave, que proporciona un equipo de vigilancia (14) protegido frente a manipulaciones.

2. Procedimiento (30) de acuerdo con la reivindicación 1, que incluye además:
detección de procesos de manipulación en el equipo de vigilancia (14) protegido frente a manipulaciones; e
invalidación de la segunda clave cuando se detecta un proceso de manipulación en el equipo de vigilancia (14) protegido frente a manipulaciones.

3. Procedimiento (30) de acuerdo con la reivindicación 1 ó 2, que incluye además:
memorización de la clave de comunicación codificada con ayuda de la segunda clave.

4. Procedimiento (30) de acuerdo con la reivindicación 3, en el que una decodificación de la clave de comunicación memorizada mediante el aparato terminal de comunicación (13) sólo es posible con ayuda de la segunda clave.

5. Procedimiento (30) de acuerdo con la reivindicación 3 ó 4, que incluye además:
generación de una clave de integridad con ayuda de la segunda clave para comprobar la integridad de la clave de comunicación memorizada.

6. Procedimiento (30) de acuerdo con una de las reivindicaciones precedentes, que incluye además:
vigilancia del estado del suministro de energía del equipo de vigilancia (14) protegido frente a manipulaciones; e
invalidación de la segunda clave cuando el suministro de energía es insuficiente en el equipo de vigilancia (14) protegido frente a manipulaciones.

7. Equipo (20) para la gestión de claves segura frente a manipulaciones para una red privada virtual (15a), que incluye:
   a) un aparato terminal de comunicación (13) con una primera clave, estando diseñado el aparato terminal de comunicación (13) para autentificarse en un servidor de autentificación (18) con ayuda de la primera clave a través de una red pública (15) y
   b1) comunicar a través de una red privada virtual (15a) en la red pública (15) con una clave de comunicación que se proporciona de manera protegida mediante el servidor de autentificación (18);
   b2) un equipo de vigilancia (14) diseñado para proporcionar una segunda clave, detectar procesos de manipulación en el equipo (20) y que cuando se detecta un proceso de manipulación invalida la segunda clave; y
   c) una memoria (22) diseñada para memorizar la clave de comunicación codificada con ayuda de la segunda clave.

8. Equipo (20) de acuerdo con la reivindicación 7, en el que el aparato terminal de comunicación (13) y el equipo de vigilancia (14) contienen microprocesadores.

9. Equipo (20) de acuerdo con la reivindicación 7 u 8, en el que el aparato terminal de comunicación (13) está diseñado para sólo poder acceder a la clave de comunicación codificada archivada en la memoria (22) con ayuda de la segunda clave.

10. Equipo (20) de acuerdo con una de las reivindicaciones 7 a 9, que incluye además:
una fuente de alimentación (26) que suministra energía al equipo de vigilancia (14) y al aparato terminal de comunicación (13); y
un acumulador de energía (25), que está conectado con la fuente de alimentación (26) y que está diseñado para suministrar energía temporalmente al equipo de vigilancia (14) cuando se interrumpe el suministro de energía mediante la fuente de alimentación (26).

11. Equipo (20) de acuerdo con la reivindicación 10, en el que el equipo de vigilancia (14) está diseñado para invalidar la segunda clave cuando se presenta una interrupción del suministro de energía por parte de la fuente de alimentación (26).

12. Equipo (20) de acuerdo con la reivindicación 8,
en el que el equipo de vigilancia (14) incluye un sensor de manipulación (23) conectado al microprocesador.

FIG 1

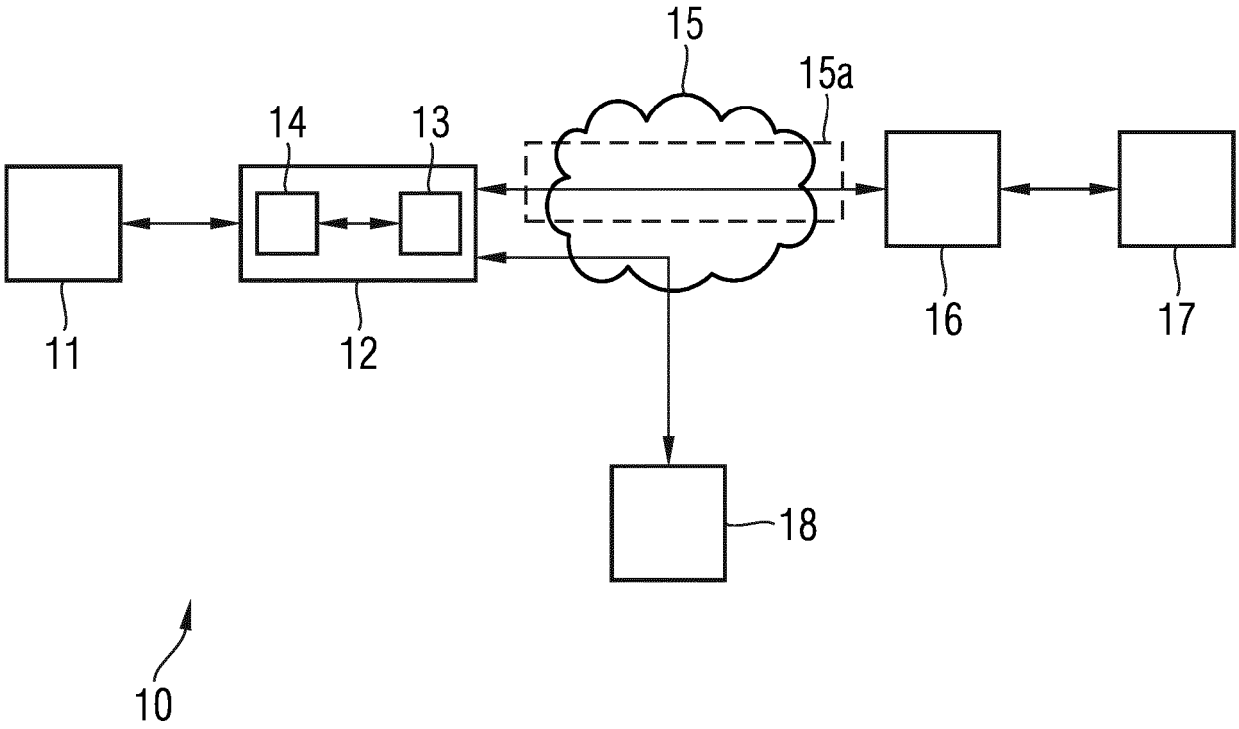

FIG 2

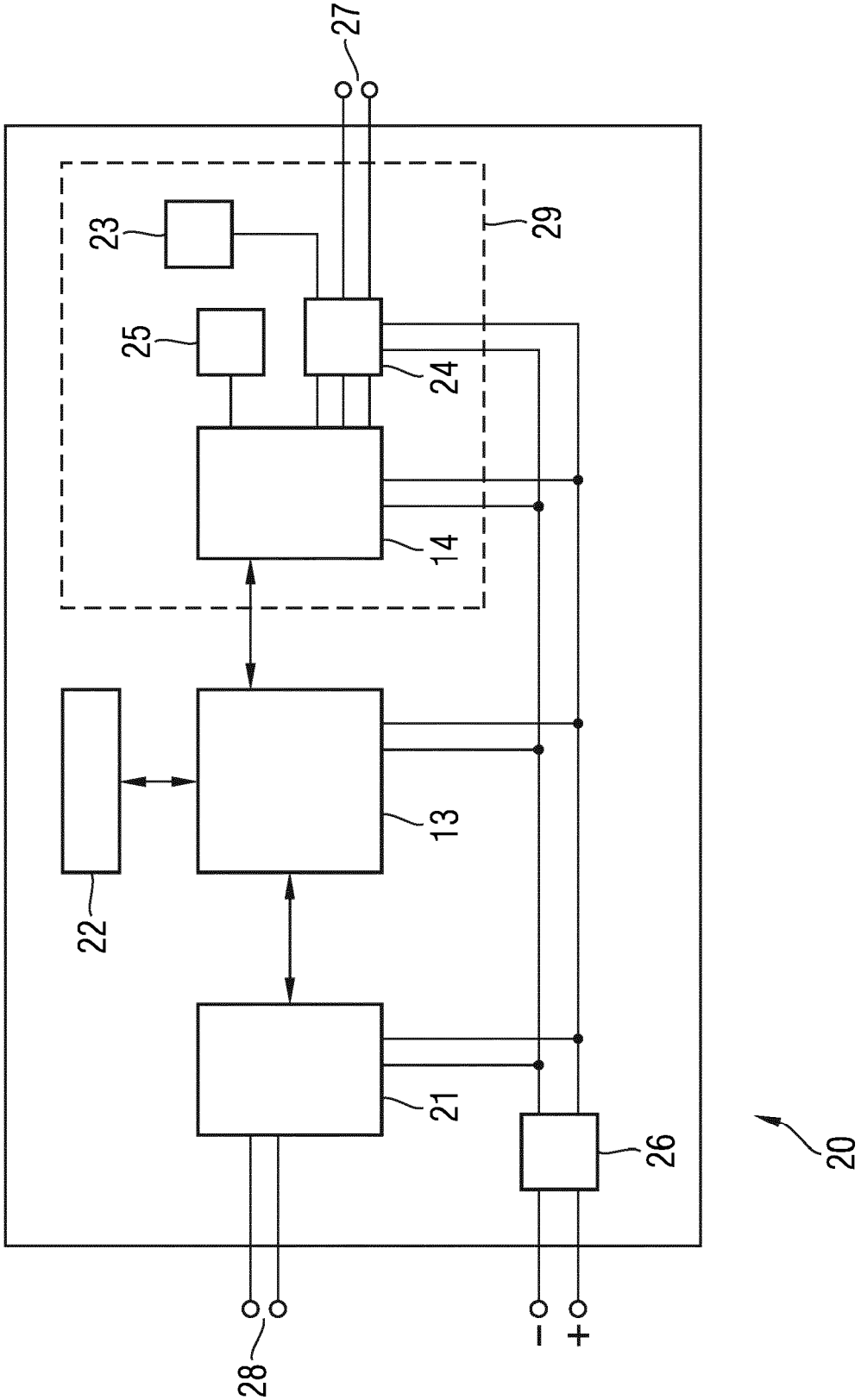

FIG 3