(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 671 788**

(51) Int. CI.:

G06F 12/14 (2006.01)
G06F 21/78 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.04.2015 PCT/EP2015/057683**

(87) Fecha y número de publicación internacional: **15.10.2015 WO15155274**

(96) Fecha de presentación y número de la solicitud europea: **09.04.2015 E 15720606 (1)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 3129888**

(54) Título: **Transmisión de datos de un almacenamiento seguro**

(30) Prioridad:

11.04.2014 AT 502752014

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.06.2018

(73) Titular/es:

AVL LIST GMBH (100.0%)
Hans-List-Platz 1
8020 Graz, AT

(72) Inventor/es:

ALDRIAN, ANDREAS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Transmisión de datos de un almacenamiento seguro

La invención se refiere a un dispositivo para la transmisión de datos entre al menos una unidad generadora de datos y una unidad de comunicación remota, presentando el dispositivo al menos una interfaz para un protocolo de comunicación capaz de web para la comunicación segura con la unidad de comunicación remota, a través de una red no propietaria y, preferiblemente, de acceso público y al menos una interfaz para un protocolo de comunicación cercano a hardware para la comunicación con la unidad generadora de datos. Además, la invención se refiere a un procedimiento para la transmisión de datos entre un dispositivo de este tipo y una unidad de comunicación remota.

El desarrollo técnico en la tecnología de comunicación posibilita cada vez más prestaciones de servicio, que hasta hace poco eran imposibles, ya que ahora hay cada vez más objetos técnicos que son capaces de transmitir datos a través de la Internet y, por ejemplo, recibir órdenes de mando remotamente a través de la Internet. Ejemplos de ello son el control remoto de una instalación de calefacción desde el teléfono inteligente, o en el sector industrial la monitorización y el mantenimiento remoto de productos.

Un sector importante de estas estrategias nuevas se denomina “Smart Services”, entendiéndose entre ellos prestaciones de servicio que se realizan por un fabricante o un proveedor de servicios a través de la Internet en aparatos y dispositivos de un cliente. Un problema consiste, sin embargo, en que a menudo todavía deben crearse las suposiciones para tales prestaciones de servicio, ya que la arquitectura orientada al servicio (SOA) necearía todavía no está disponible.

Una suposición para la implementación de una arquitectura orientada al servicio está en que todos los aparatos implicados tienen que ser capaces de alguna manera de una comunicación capaz de web. Como “capaz de web” se consideran protocolos en relación con la presente solicitud, que permiten constituir una conexión de comunicación securizable, preferiblemente conforme a AAA y capaz de cifrado, a través de redes abiertas, es decir, accesible a terceros, en particular la Internet, y desarrollar el tráfico de datos sobre ello. La pila de protocolo de un protocolo capaz de web reproduce en este caso todas las 7 capas del modelo de referencia OSI.

La conexión de comunicación se produce en este caso, en general, a través de un servicio web. Distintivo para un servicio web es, en particular, el tipo de la constitución de conexión. En este caso, la comunicación se constituye por la unidad de comunicación remota, que quiere acceder a datos de la unidad terminal. Para ello es necesario que en la arquitectura de seguridad en la ubicación de la unidad terminal estén abiertos puertos para la comunicación entrante, a través de los que pueda crearse un túnel a la unidad terminal por la unidad de comunicación remota. Estos puertos abiertos y la posibilidad de iniciar un acceso a datos remotamente, representa un riesgo de seguridad potencial y, por ello, se utilizan para ataques de hackers.

Para configurar una conexión de este tipo más segura, se utilizan certificados que están almacenados en la unidad terminal, y a través de los cuales se puede garantizar la identidad del aparato que accede y se puede constituir una conexión cifrada. Sin embargo, para constituir la comunicación segura, primero debe crearse una conexión entre la unidad de comunicación remota y la unidad terminal, lo que de nuevo presenta posibilidades de ataque.

Instalaciones industriales extremadamente complejas, por ejemplo para la producción o para la realización de pruebas, comprenden en general los aparatos de numerosos fabricantes, siendo responsables varios especialistas del mantenimiento de los componentes individuales. Para el fabricante de tales componentes es de máximo interés obtener informaciones de clientes sobre la utilización de su producto, por un lado para obtener datos para el desarrollo y por otro lado para poder ofrecer estrategias de mantenimiento y de servicio adecuadas, que también son beneficiosas para el cliente.

En entornos industriales existen sobre todo tres grandes grupos problemáticos, que retrasan la aplicación:

En primer lugar, a diferencia de productos de consumo, como por ejemplo teléfonos inteligentes, muchos componentes de sistemas industriales están destinados muy específicamente para su respectiva aplicación y disponen a menudo solo de posibilidades de comunicación muy limitadas, desde una salida de señal analógica cableada sencilla, a través de buses de campo, como por ejemplo CAN o Profibus, hasta sistemas de red sencillos, como por ejemplo Ethernet. Respecto al modelo de capas OSI, tales protocolos de comunicación cercanos al hardware se han de clasificar la mayoría de las veces en las capas 1, 2 y 3. Tales soluciones de conexión son solo adecuadas para redes locales y faltan en sistemas de seguridad. Una conexión a la Internet en tales sistemas sería solo posible a través de pasarelas, pero de este modo el sistema estaría expuesto a un riesgo considerable de ataques, en particular cuando a terceros, es decir a modo de ejemplo un proveedor de servicio, debe concederse un acceso a datos del sistema. Por ello, tales sistemas se utilizan solo aislados y esta arquitectura aislada excluye la integración en una arquitectura orientada al servicio.

En segundo lugar, la mayoría de las veces se trata de sistemas desarrollados, en los que se utilizan elementos constructivos de varias generaciones juntos. A causa de la larga vida útil de los componentes industriales, estos

pueden a menudo estar en uso durante décadas. Cambiar todos los componentes de una instalación al mismo tiempo por aparatos “capaces de Internet”, no se considera la mayoría de las veces por motivos de costes y plantearían otros problemas de seguridad.

En tercer lugar, en el caso de datos de sistema se trata a menudo de datos muy sensibles, que deben mantenerse ocultos ante los competidores, y que a menudo tampoco deben divulgarse a los fabricantes de los sistemas o a los proveedores de servicio. Es de gran importancia para las empresas que puedan determinar en todo momento sobre la utilización de sus datos. Por motivos claros de la seguridad de datos, por eso no se consideran la mayoría de las veces sistemas de comunicación creados para consumidores, para fines industriales.

Como ejemplo de tecnología ya existente se remite a la enseñanza de la publicación EP1276271-A1, en la que se presentan dispositivos que están equipados con controladores de seguridad y almacenamientos de seguridad particionados, para el envío de datos a través de una red de comunicación. La presente invención se dirige a superar los inconvenientes del estado de la técnica. En particular, debe ser posible integrar también aparatos en una arquitectura orientada al servicio que solo pueden comunicarse a través de protocolos de comunicación cercanos al hardware. No obstante, debe poder descartarse un acceso a estos aparatos por personas no autorizadas. De acuerdo con la invención, debe poderse en este caso integrar también aparatos antiguos existentes que todavía están en uso en la arquitectura orientada al servicio. Como otro requisito de seguridad, debe ser posible de acuerdo con la invención de manera sencilla y entendible establecer exactamente las autorizaciones de acceso a datos para todos los participantes.

Como “protocolo de comunicación cercano al hardware” se designan en relación con la presente memoria descriptiva, en general, protocolos de comunicación, cuya estructura de capas o bien pila de protocolo no abarca todas las 7 capas del modelo OSI, en particular protocolos que no presentan una capa de representación (capa 6) y, por lo tanto, no permiten una comunicación solapante del sistema ni un cifrado de los datos. Una característica de protocolos de comunicación cercanos al hardware es que no posibilitan implementación alguna de protocolos de seguridad que permitiera una comunicación fiable y segura a través de redes (de la nube) distribuidas.

Interfaces de comunicación existentes para protocolos cercanos al hardware, que pueden utilizar, por ejemplo, una tecnología de bus de campo o una conexión de Ethernet de punto a punto están limitadas, por lo tanto, al mero mínimo de las 7 capas del modelo OSI. Protocolos de comunicación cercanos al hardware, particularmente sencillos, utilizan únicamente la capa de transmisión de bits (capa 1) o una combinación de la capa de transmisión de bits y de seguridad (capa 2).

A ejemplos de protocolos de la capa de transmisión de bits pertenecen V.24, V.28, X.21, RS 232, RS 422, RS 423 o RS 499. A ejemplos que utilizan las combinaciones a base de capas 1 y 2, o solo la capa 2, pertenecen el protocolo de Ethernet HDLC, SDLC, DDCMP, IEEE 802.2 (LLC), ARP, RARP, STP, IEEE 802.11 (WLAN), IEEE 802.4 (bus Token), IEEE 802.5 (anillo Token) o FDDI.

Adicionalmente, en protocolos de comunicación cercanos al hardware pueden encontrar también uso protocolos de capas mayores. A ejemplos de protocolos de las capas 3 a 5 pertenecen X.25, ISO 8208, ISO 8473 (CLNP), ISO 9542 (ESIS), IP, IPsec, ICMP, ISO 8073/X.224, ISO 8602, TCP, UDP, SCTP, ISO 8326 / X.215 (servicio de sesión), ISO 8327 / X.225 (protocolo de sesión orientado a la conexión) o ISO 9548 (protocolo de sesión sin conexión).

A ejemplos de protocolos de comunicación cercanos al hardware, que se utilizan particularmente para aplicaciones industriales en el sector de entornos de prueba, por ejemplo en el sector del automóvil, pertenecen, entre otros, el protocolo AK a través de RS232, CANopen a través de CAN y Profibus-DP a través de RS485. Particularmente, el protocolo AK del “Verband der Automobilindustrie e. V. / Círculo de Trabajo Técnicas para la Normalización de la Medición de los Gases de Escape” sigue siendo una norma de facto en muchas instalaciones de ensayo en el sector del automóvil. Fue creado como un protocolo sencillo para la transmisión de datos cercana al hardware y no ofrece posibilidad de conversión en un sistema triple A (autentificación, autorización, contabilización-AAA).

Conforme a la invención, los objetivos arriba definidos se alcanzan mediante un dispositivo del tipo mencionado al comienzo que presenta un controlador de seguridad que está capacitado para el control de la comunicación a través de la o las interfaces capaces de web y a través de la o las interfaces cercanas al hardware, estando asociado al controlador de seguridad un almacenamiento seguro que presenta zonas definidas de almacenamiento, estando asociado a al menos una zona de almacenamiento al menos un certificado. Un dispositivo de este tipo puede comunicar a través de las interfaces cercanas al hardware con las unidades generadoras de datos, es decir, en particular con componentes individuales de la instalación que deben ser integrados en la arquitectura orientada al servicio, a través de sus protocolos de comunicación próximos al hardware y generar datos correspondientes que pueden ser depositados en una zona de almacenamiento determinada. Con el fin de acceder a los datos, por parte de la unidad de comunicación lejana puede llevarse a cabo una consulta a distancia a través de la interfaz capaz de web, pudiendo verificarse la autorización para la consulta a través del certificado. Para cada una de las zonas de almacenamiento se pueden establecer individualmente los certificados autorizados en cada caso para su acceso (o bien los “beneficiarios del certificado” que disponen de este certificado). El controlador de seguridad garantiza que la

conexión de comunicación (el denominado “túnel”) termine en el controlador de seguridad y no sea posible que una unidad de comunicación remota cree una conexión directa con el aparato final (es decir, la unidad generadora de datos). Por lo tanto, también correspondientes certificados están depositados en un almacenamiento seguro del controlador de seguridad y no en un almacenamiento de la unidad generadora de los datos.

Un certificado designa, en general, un objeto, a través del cual se puede garantizar la confianza y la imputabilidad/no repudiación de una persona o instancia. Esto afecta, en particular, a las etapas de la autentificación y autorización de la denominada conformidad AAA. Los certificados pueden utilizarse, en particular, para la protección frente al transporte y el acceso. En este caso, la parte pública del certificado (“clave pública” o bien “public key”) se utiliza para la protección, de modo que solo el titular de la parte privada correspondiente del certificado (“clave privada” o bien “private key”) tiene la posibilidad de acceder a o inspeccionar los datos. La norma actualmente más difundida de certificados es X.509, también conocida como “PKI-Store”, pero el experto en la materia conoce, sin embargo, también otros procedimientos utilizables.

De manera ventajosa, al menos una zona de almacenamiento puede contener un código de programa que pueda ejecutarse en el controlador de seguridad. Con ello, pueden protegerse incluso en el almacenamiento seguro frente a manipulaciones, partes de programa relevantes para la seguridad que definen, por ejemplo, el modo de trabajo del controlador de seguridad, y se encuentran asimismo disponibles para un control de acceso a través de certificados.

De manera ventajosa, la zona de almacenamiento que contiene el código de programa puede estar asociada al certificado de un proveedor del hardware del controlador de seguridad. Partes de programa fundamentales sólo pueden ser modificadas, por consiguiente, por el proveedor del hardware del chip de seguridad, de modo que se excluye una desactivación errónea de características de seguridad por parte de colaboradores o un perjuicio intencionado por parte de atacantes.

Una forma de realización ventajosa de la invención puede prever que al menos una zona de almacenamiento esté asociada a una unidad generadora de datos determinada, conteniendo la zona del almacenamiento una identificación inequívoca (ID único), datos de funcionamiento, datos de control, datos de configuración y/o datos históricos de la unidad. Con ello, por ejemplo, es posible para el proveedor del servicio acceder a datos relevantes por medio de un acceso remoto y también modificar éstos en función de su autorización (p. ej., para reinicializarlos después de un servicio). Al asociar varias zonas de almacenamiento a una única unidad, mediante la asignación de diferentes certificados pueden realizarse también estructuras de autorización complejas. Dado que la conexión de la comunicación termina en el controlador de seguridad, se excluye una comunicación con la unidad generadora de datos y una manipulación de la unidad generadora de datos por parte de la unidad de comunicación a distancia.

Otra forma de realización ventajosa de la invención puede prever que al menos una zona de almacenamiento contenga certificados y/o asignaciones. Por consiguiente, también los propios certificados pueden ser protegidos con el mismo sistema frente a un acceso ajeno. Además, se puede establecer quien está autorizado para modificar las asignaciones y, por consiguiente, las autorizaciones de acceso. Particularmente ventajoso puede ser en este caso que la zona del almacenamiento que contiene los certificados y/o las asignaciones esté asociada al certificado de un titular del dispositivo. Esto es a menudo conveniente, ya que con ello el propio titular puede definir qué derechos otorga a terceros y, en particular, al proveedor del servicio. Una etapa de seguridad particularmente elevada se puede conseguir cuando la autorización de acceso esté definida en el código de programa del controlador de seguridad.

De manera ventajosa, el controlador de seguridad puede presentar medios para vigilar las unidades generadoras de datos conectadas a las interfaces cercanas al hardware. Con ello se puede reconocer, en el caso de que, por ejemplo, un aparato fuese sustituido sin autorización y si los datos del aparato son plausibles, por ejemplo si un contador de horas de funcionamiento aumenta de forma estrictamente monótona.

En una forma de realización preferida, el controlador de seguridad puede estar integrado en un chip del hardware. Esto impide manipulaciones de los programas realizados por el controlador de seguridad.

Con el fin de proteger adicionalmente frente a ataques al controlador de seguridad, el chip del hardware puede comprender, de manera ventajosa, un almacenamiento seguro y una CPU integrada.

En una forma de realización ventajosa, el chip del hardware puede contener un cripto-módulo. El cripto-módulo controla el cifrado de la comunicación. Al estar integrado el cripto-módulo en el chip del hardware, se pueden impedir ataques que vayan dirigidos a una perturbación del procedimiento de cifrado.

Mediante la combinación de un almacenamiento seguro, CPU integrada y cripto-módulo en un controlador de seguridad, que está integrado en un chip del hardware, el controlador de seguridad está en condiciones de administrar no sólo el almacenamiento seguro, sino también de realizar por sí mismo de forma segura las operaciones de cálculo. Esto tiene la ventaja de que el controlador de seguridad funciona de forma “autártica” y que no depende de una CPU atacable. En este caso, el controlador de seguridad puede comprender partes del programa codificadas por hardware que no pueden ser manipuladas a través de ataques basados en datos.

Como almacenamiento seguro se designa en relación con la presente memoria descriptiva, un almacenamiento que está protegido frente a un acceso no autorizado. En particular, éste puede ser un almacenamiento al que exclusivamente tenga acceso el controlador de seguridad y que, por lo tanto, no pueda ser manipulado por parte de terceros.

Con ayuda del dispositivo se puede llevar a cabo de manera ventajosa un procedimiento para la transmisión de datos entre el dispositivo y una unidad de comunicación remota, el cual se caracteriza por las siguientes etapas: creación de una conexión de comunicación a través de una interfaz capaz de web con una unidad de comunicación de un beneficiario del certificado al que está asociado un certificado; determinación del certificado del beneficiario del certificado; determinación de una zona de almacenamiento de los datos a transmitir; verificación de la asignación del certificado del beneficiario del mismo a la zona de almacenamiento y, en el caso de un examen positivo, transmisión de datos almacenados en la zona de almacenamiento a la unidad de comunicación remota y/o recepción de datos de la unidad de comunicación remota y almacenamiento de los datos recibidos a la zona de almacenamiento. Con ayuda de este procedimiento se pueden realizar de forma práctica y sencilla complejas arquitecturas de seguridad.

De manera ventajosa, el procedimiento puede presentar, además, las siguientes etapas: recepción o bien acceso de datos (de funcionamiento) de una unidad a través de una interfaz cercana al hardware; y almacenamiento de los datos de funcionamiento en una zona de almacenamiento asociada a la unidad del almacenamiento seguro. Con ello, se puede acceder a datos (de funcionamiento) de las unidades en base a un horario, por un suceso definido determinado o en virtud de una consulta del usuario del dispositivo. En el caso de una consulta remota subsiguiente, ya no se requiere acceso alguno a la unidad, dado que los datos ya están depositados en un almacenamiento seguro. Por consiguiente, conforme a la invención, no es necesario que la persona autorizada identificada por el certificado para el acceso a los datos acceda directamente a la propia unidad. Con ello, se impiden de manera segura manipulaciones en la instalación en la que se encuentra la unidad.

En una forma de realización particularmente preferida, la comunicación del dispositivo con la unidad de comunicación remota puede tener lugar de forma cifrada. Dado que el respectivo participante en la comunicación está identificado por parte del certificado, la codificación puede tener lugar de una manera sencilla a través de pares de códigos que están asociados a los certificados.

De manera ventajosa, en la interfaz capaz de web puede estar implementado un protocolo que funcione puramente a través de mecanismos push. Protocolos de este tipo, por ejemplo conforme a la especificación MQTT, permiten por parte de la interfaz capaz de web la realización de directrices Firewall que bloquean el tráfico de entrada. Una manipulación del sistema a través de servicios de web y una estructura de una conexión de extremo a extremo hasta la unidad generadora de datos puede, por consiguiente, excluirse. En el caso de protocolos que funcionan puramente a través de mecanismos push tales como, por ejemplo, conforme al protocolo MQTT, de manera conocida no se crea una conexión de extremo a extremo directa, sino que la comunicación es transmitida siempre a través de un bróker intercalado que adquiere datos de un “editor” y los proporciona a uno o varios “abonados”, pudiendo estar prevista una identificación protegida por el certificado de editores y/o abonados. Cada uno de los puntos extremos “abre” la comunicación con el bróker y ésta no se introduce “desde el exterior”.

Dado que los dos participantes en la comunicación pueden actuar tanto como abonados como en calidad de editores, también es posible intercambiar datos en ambas direcciones, sin que para ello se tenga que concebir un servicio web potencialmente atacable.

Desde el controlador de seguridad se crea para ello a intervalos definidos una conexión con el bróker y se proporcionan datos para un acceso por parte de terceros autorizados (es decir, el dispositivo trabaja como editor) o se accede a datos por parte de terceros (es decir, el dispositivo trabaja como abonado).

La invención se describe de manera detallada en lo que sigue con referencia a los dibujos adjuntos, en donde

la Fig. 1 muestra una representación esquemática de componentes de la red con los que comunica un dispositivo de acuerdo con la invención;

la Fig. 2 muestra una representación esquemática de elementos esenciales de un dispositivo de acuerdo con la invención;

la Fig. 3 muestra otra representación esquemática del dispositivo de acuerdo con la invención, para la explicación de protocolos de comunicación a modo de ejemplo; y

la Fig. 4 muestra esquemáticamente una red con una arquitectura orientada al servicio en la que se utiliza el dispositivo de acuerdo con la invención en varios puntos.

La Fig. 1 muestra una disposición de red a modo de ejemplo que esencialmente se puede dividir en cinco zonas, a saber, la zona de una ubicación de la industria 4, tres zonas 3a, 3b, 3c de participantes en la comunicación denominados en lo sucesivo como “beneficiarios del certificado”, a saber, un proveedor de hardware 3a, un

proveedor de servicio 3b y un titular 3c, en cada caso con una unidad de comunicación 5a, 5b, 5c remota y la zona de una red 7 no propietaria que presenta una estructura de nube, en particular la Internet.

La ubicación de la industria 4 puede ser, por ejemplo, un sitio de producción o una instalación de prueba, p. ej., para el sector del automóvil, estando asociado a la ubicación un determinado titular 3c. Al titular de la ubicación industrial 4 se le otorga una importancia particular, dado que debe establecer las autorizaciones de acceso, tal como se explicará todavía más adelante. En la ubicación de la industria 4 se encuentra una pluralidad de unidades 2a a 2f generadoras de datos, considerándose como "unidad generadora de datos" esencialmente todos los dispositivos cuyo estado pueda ser monitorizado de alguna manera. En especial, puede tratarse, en particular, de unidades que proceden de un determinado proveedor que tiene interés en monitorizar los productos vendidos por el mismo, con el fin de poder proporcionar posibles prestaciones de servicio de una forma rápida, planificada y sencilla. Al proveedor de servicio está asociada en la Fig. 1 una zona 3b propia.

En la ubicación de la industria 4 está previsto un dispositivo 1 de acuerdo con la invención, presentando el dispositivo 1 varias interfaces 8a-8i cercanas al hardware que están unidas de diferente manera con las unidades 2a-2f generadoras de datos. Las unidades 2a-2f generadoras de datos pueden estar dispuestas en varios grupos, en donde en la disposición representada las unidades 2c-2f forman un grupo que está conectado a un bus de campo común, a través del cual comunican las unidades, pudiendo utilizarse para sistemas de bus de campo cualquier protocolo de comunicación conocido en el sector, por ejemplo CANopen o Profibus-DP. El dispositivo 1 está conectado a través de la interfaz 8i asimismo con el bus campo con el fin de poder comunicar con las unidades 2c-2f del grupo. Otro grupo lo forman las unidades 2a y 2b que en cada caso están conectadas en un protocolo de extremo a extremo a una interfaz 8b, 8d del dispositivo 1.

Se ha de hacer la observación de que las unidades no presentan, por lo general, medios con el fin de transmitir a través del Internet datos a través de protocolos capaces de web. Sin embargo, también puede ser que, a pesar de la capacidad en principio de una unidad para la comunicación capaz de web, no sea permitida una conexión de esta unidad a una red pública, dado que en la red se encuentran otras unidades que podrían exponerse con ello a un acceso no autorizado.

Al proveedor de hardware del dispositivo 1 o bien al proveedor de hardware de elementos relevantes para la seguridad del dispositivo 1, en particular del controlador de seguridad 9 contenido en el dispositivo, está asociada otra zona 3a. Por la expresión "proveedor de hardware" puede considerarse, en el sentido de la presente descripción, en particular el propio fabricante de chip o también un tercer proveedor, por ejemplo un lugar de certificación. La expresión "proveedor de hardware" designa, en particular, el lugar que es responsable del modo de funcionamiento y del desarrollo del controlador de seguridad. Una característica de seguridad particular del dispositivo puede prever que una actualización del código de programa en el que se fundamenta el controlador de seguridad sólo pueda ser realizado por el lugar designado como proveedor de hardware y, eventualmente, bajo otras premisas de seguridad especiales.

El dispositivo 1 de la Fig. 1 presenta varias interfaces 6a-6d capaces de web, a través de las cuales puede crearse una comunicación que se solapa con el sistema con otras unidades a través de redes públicas o propietarias tales como, por ejemplo, una Intranet, una red GSM y/o la Internet. La estructura de uniones capaces de web, la comunicación a través de estas uniones y los protocolos utilizados para ello son ampliamente conocidos en el sector y, por lo tanto, no necesitan ser explicados aquí con mayor detalle. En el ejemplo de realización representado en la Fig. 1, el dispositivo 1 comunica con una unidad de comunicación 5c remota del titular 3c de la ubicación de la industria 4 a través de una conexión de Intranet, y con unidades de comunicación 5a y 5b lejanas del proveedor de servicio 3a o bien del proveedor de hardware 3a a través de una conexión de Internet.

Haciendo referencia a la Fig. 2 se explica ahora el modo de funcionamiento del dispositivo 1 de acuerdo con la invención, pasando a considerar en particular la función del controlador de seguridad 9. El controlador de seguridad 9 del dispositivo 1 puede realizarse como chip individual o como combinación de varios chips, trabajando conjuntamente el controlador de seguridad con un microcontrolador 11 (ARM-CPU). También es posible integrar el controlador de seguridad 10 y el microcontrolador 11 en un único chip. Esto posibilitaría ciertamente elevadas normas de seguridad, pero también estaría ligado a una elevada complejidad de desarrollo.

El controlador de seguridad regula la comunicación con las unidades 2a-2f generadoras de datos a través de las interfaces 8a-8i cercanas al hardware, la comunicación a través de las interfaces 6a-6d capaces de web y el acceso a un almacenamiento 10 seguro.

El almacenamiento 10 seguro está delimitado por la técnica del hardware, de manera que un acceso puede tener lugar exclusivamente por parte del controlador de seguridad 9. Con el fin de poder utilizar el dispositivo, debe ser primeramente "inspeccionado" por una unidad emisora, llevándose a cabo la inspección en el caso representado por el proveedor de hardware. En el caso de la inspección, se define una división del almacenamiento 10 en zonas de almacenamiento A, B, C, D, etc. individuales, depositándose en la primera zona de almacenamiento A el código de programa para el control del procesador de seguridad 9. En la zona de almacenamiento B se depositan para todas

las instancias que deban de ser tenidas en cuenta para un acceso certificados a, b, c, d, tratándose de la parte pública del certificado. Junto a la definición de las zonas de almacenamiento A, B, C, D, el código de programa establece también qué titulares del certificado deben tener acceso a qué zonas de almacenamiento y si la autorización de acceso permite también la modificación de datos.

En el ejemplo representado, la zona de almacenamiento A en la que se deposita el código del programa, está asegurada por el certificado a del proveedor del hardware o bien del lugar de inspección. Esto significa que el código del programa (y, con ello, la división de las zonas de almacenamiento y la estructura de autorización al acceso) solo puede ser modificado por el proveedor del hardware 3a. Modificaciones en el código del programa no pueden efectuarse, por lo tanto, ni por el titular 3c del dispositivo ni por el proveedor del servicio 3b, sino solamente por el proveedor del hardware 3a, por ejemplo cuando deba incorporarse una actualización. Cuando el código del programa requiera una actualización, otra función de seguridad puede requerir adicionalmente una aceptación del titular 3a y/o del proveedor del servicio 3b.

En la forma de realización descrita, todo dispositivo de acuerdo con la invención se ajusta, por lo tanto, en el caso de la inspección, específicamente a las respectivas condiciones de uso, de modo que no son posibles modificaciones posteriores o solo lo son de manera limitada. En función de las condiciones de seguridad, podrían permitirse, sin embargo, modificaciones posteriores para distintos elementos, debiendo estar definidas estas posibilidades en el código del programa. Así, por ejemplo, puede permitirse un intercambio de diferentes certificados, tan pronto como éstos hayan caducado y tengan que ser renovados.

Las otras zonas de almacenamiento C, D, … están asociadas en cada caso a una unidad 2a-2f generadora de datos o a un grupo de este tipo de unidades, en donde los datos depositados en la zona de almacenamiento respectiva son asimismo controlados a través del código de programa. La actualización de datos puede desencadenarse por un suceso determinado (p. ej., cuando el proveedor de servicio 3b reinicialice un contador de servicio después de un mantenimiento) o se pueden crear de manera continua o a intervalos de tiempo determinados (p. ej., para el registro de tiempos de funcionamiento). En las respectivas zonas de almacenamiento C, D para las unidades 2a-2f pueden estar contenidas, además, una caracterización única (ID único) de la unidad e informaciones sobre el protocolo de comunicación a utilizar.

También la comunicación a través de las interfaces 6a-6d capaces de web es controlada por el controlador de seguridad 9, en donde en el caso de cada constitución de una conexión de comunicación se examina el certificado respectivo y también se cifra la conexión de comunicación preferiblemente a través del certificado, de modo que sólo el titular de la clave privada pueda acceder a los contenidos. Con ello, se define con precisión a qué zonas de almacenamiento puede acceder el titular de un certificado. Eventualmente, los datos en determinadas zonas de almacenamiento pueden estar depositados de manera cifrada adicionalmente con un certificado. Sin embargo, con ello sólo se puede acceder al contenido con un único certificado. En otros casos se prefiere que los datos estén depositados de otra manera, por ejemplo con una clave simétrica, cifrados o no cifrados en el almacenamiento y que sólo durante la transmisión de datos se proceda al cifrado por el controlador de seguridad con el certificado respectivo.

En la forma de realización representada en la Fig. 2, el titular 3c puede acceder con el certificado 3c a las zonas de almacenamiento B, C y D, el proveedor del servicio 3b puede acceder con su certificado a la zona de almacenamiento C y el proveedor del hardware 3a puede acceder con su certificado exclusivamente a la zona de almacenamiento A.

El controlador de seguridad 9 procura una separación estricta de la comunicación a través de las interfaces 8 cercanas al hardware de la comunicación a través de las interfaces 6 capaces de web, de modo que es imposible un acceso directo a las unidades 2a-2f generadoras de datos a través de una de las interfaces (6a-6d) capaces de web. Tampoco cuando los atacantes consigan evitar todas las premisas de seguridad y hackear al controlador de seguridad, con ello tampoco les es posible obtener un acceso a las unidades generadoras de datos, dado que éstas comunican en planos de protocolo muy distintos a como es el caso de los protocolos de comunicación de la interfaz capa de web.

Los aspectos de seguridad de los dispositivos y procedimientos de la presente invención se pueden adaptar de manera arbitraria a las respectivas necesidades del usuario, pudiendo implementarse tanto medidas de seguridad adicionales, como también renunciarse a determinadas características de seguridad.

La Fig. 3 muestra otra representación esquemática de una forma de realización a modo de ejemplo del dispositivo de acuerdo con la invención, estando divididos los distintos elementos en relación con los componentes funcionales y los protocolos utilizados a modo de ejemplo y de manera esquemática. El dispositivo de la Fig. 3 presenta cinco interfaces cercanas al hardware para una conexión directa de unidades, estas son las interfaces 8a (LAN), 8b (RS232 o RS485), 8c (CAN), 8d (USB) y 8e (otra). Las interfaces cercanas al hardware adicionales son las interfaces 8f (LAN), 8g (Ethercat), 8h (USB) y 8i (CAN, CANOpen).

La Fig. 4 muestra esquemáticamente una red con una arquitectura orientada al servicio de un proveedor del servicio 3b, utilizándose el dispositivo 1 de acuerdo con la invención en el caso de varios clientes (titulares 3c y 3c') del proveedor del servicio 3b con el fin de posibilitar un acceso definible por el titular respectivo a los datos de las unidades 2a-2c generadoras de datos de los clientes servidas por el proveedor del servicio 3b.

Lista de símbolos de referencia:

Dispositivo (1)

Unidad generadora de datos (2a-2f)

Beneficiario del certificado (3)

Proveedor del hardware (3a)

Proveedor del servicio (3b)

Titular (3c)

Ubicación de la industria 4

Unidad de comunicación remota (5a-5c)

Interfaz capaz de web (6a-6d)

Red no propietaria (7)

Interfaz cercana al hardware (8a-8i)

Controlador de seguridad (9)

Almacenamiento seguro (10)

Microcontrolador 11

Zonas de almacenamiento (A, B, C, D)

Certificados, a, b, c

REIVINDICACIONES

1. Dispositivo (1) para la transmisión de datos entre al menos una unidad generadora de datos (2a-2f) y una unidad de comunicación (5a-5c) remota, presentando el dispositivo (1) al menos una interfaz (6a-6d) para un protocolo de comunicación capaz de web para la comunicación segura con la unidad de comunicación (5a-5c) remota, a través de una red (7) no propietaria y, preferiblemente, de acceso público y al menos una interfaz (8a-8i) para un protocolo de comunicación cercano a hardware para la comunicación con la unidad generadora de datos (2a-2f), que es al menos una unidad generadora de datos (2a-2f) de un componente de una instalación industrial, caracterizado por que el componente para la transmisión de datos comunica solamente a través del protocolo de comunicación cercano al hardware, presentando el dispositivo un controlador de seguridad (9) que controla la comunicación a través de la o las interfaces (6a-6d) capaz o capaces de web y a través de la o las interfaces (8a-8i) cercana o cercanas al hardware, estando asociado al controlador de seguridad (9) un almacenamiento seguro (10) que presenta zonas de almacenamiento (A, B, C, D) definidas, estando asociado a al menos una zona de almacenamiento (A, B, C, D) al menos un certificado (a, b, c).

2. Dispositivo según la reivindicación 1, caracterizado por que al menos una zona de almacenamiento (A) específica contiene un código de programa que puede ser ejecutado en el controlador de seguridad (9).

3. Dispositivo según la reivindicación 2, caracterizado por que la zona de almacenamiento (A) específica que contiene el código de programa está asociada al certificado (a) de un proveedor del hardware (3a) del controlador de seguridad.

4. Dispositivo según una de las reivindicaciones 1 a 3, caracterizado por que al menos otra zona de almacenamiento (C, D) está asociada a una determinada unidad generadora de datos (2a, 3b), conteniendo la zona de almacenamiento adicional una identificación inequívoca, ID único, datos de funcionamiento, datos de control, datos de configuración y/o datos históricos de la unidad.

5. Dispositivo según una de las reivindicaciones 1 a 4, caracterizado por que al menos otra zona de almacenamiento (B) contiene certificados (a, b, c) y/o asociaciones.

6. Dispositivo según la reivindicación 5, caracterizado por que la otra zona de almacenamiento (B), que contiene los certificados y/o las asociaciones, está asociada al certificado (c) de un titular (3c) del dispositivo (1).

7. Dispositivo según una de las reivindicaciones 1 a 6, caracterizado por que el controlador de seguridad (9) presenta medios para la monitorización de las unidades generadoras de datos (2a-2f) conectadas a las interfaces (8a-8i) cercanas al hardware.

8. Dispositivo según una de las reivindicaciones 1 a 7, caracterizado por que el controlador de seguridad (9) está integrado en un chip del hardware.

9. Dispositivo según la reivindicación 8, caracterizado por que el chip del hardware comprende un almacenamiento seguro y una CPU integrada.

10. Dispositivo según la reivindicación 8 o 9, caracterizado por que el chip del hardware contiene un cripto-módulo.

11. Dispositivo según una de las reivindicaciones 1 a 10, caracterizado por que en la interfaz capaz de web está implementado un protocolo, que solo funciona a través de mecanismos push.

12. Procedimiento para la transmisión de datos entre un dispositivo según una de las reivindicaciones 1 a 10 y una unidad de comunicación (5a-5c) remota, presentando el proceidmiento las siguientes etapas:

- creación de una conexión de comunicación a través de una interfaz (6) capaz de web con una unidad de comunicación (5a-5c) de un beneficiario (3) del certificado al que está asociado un certificado (a, b,c);

- determinación del certificado (a, c, b) del beneficiario (3) del certificado;

- determinación de una zona de almacenamiento (A, B, C, D) de los datos a transmitir;

- verificación de la asignación del certificado (a, b, c) del beneficiario (3) del certificado a la zona de almacenamiento (A, B, C, D) y,

- en el caso de un examen positivo, transmisión de datos almacenados en la zona de almacenamiento (A, B, C, D) a la unidad de comunicación (5a-5c) remota y/o recepción de datos de la unidad de comunicación (5a-5c) remota y almacenamiento de los datos recibidos a la zona de almacenamiento.

13. Procedimiento según la reivindicación 12, caracterizado por que el procedimiento presenta, además, las siguientes etapas:

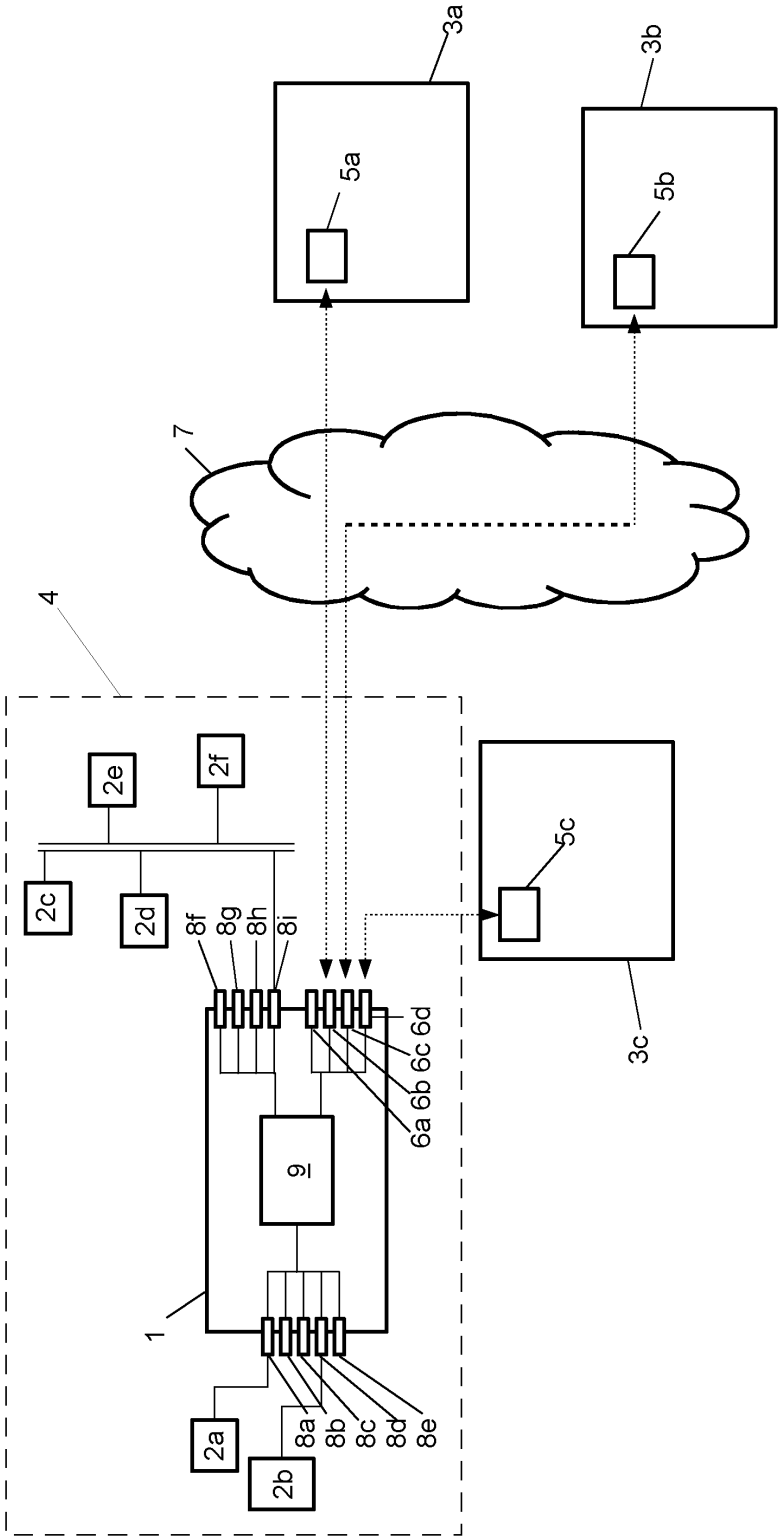
- recepción o bien acceso de datos (de funcionamiento) de una unidad (2a-2f) a través de una interfaz (8) cercana al hardware; y

- almacenamiento de los datos de funcionamiento en una zona de almacenamiento (B, C, …) asociada a la unidad (2a-2f) del almacenamiento (10) seguro.

14. Procedimiento según la reivindicación 12 o 13, caracterizado por que la comunicación con la unidad de comunicación (5a-5c) remota tiene lugar de forma cifrada.

15. Procedimiento según una de las reivindicaciones 12 a 14, caracterizado por que en la interfaz capaz de web se implementa un protocolo que solo funciona a través de mecanismos push.

Fig. 1


3a
3b
5a
5b
7
4
2e
2f
2c
2d
8f
8g
8h
8i
5c
3c
6a 6b 6c 6d
9
1
2a
2b
8a
8b
8c
8d
8e

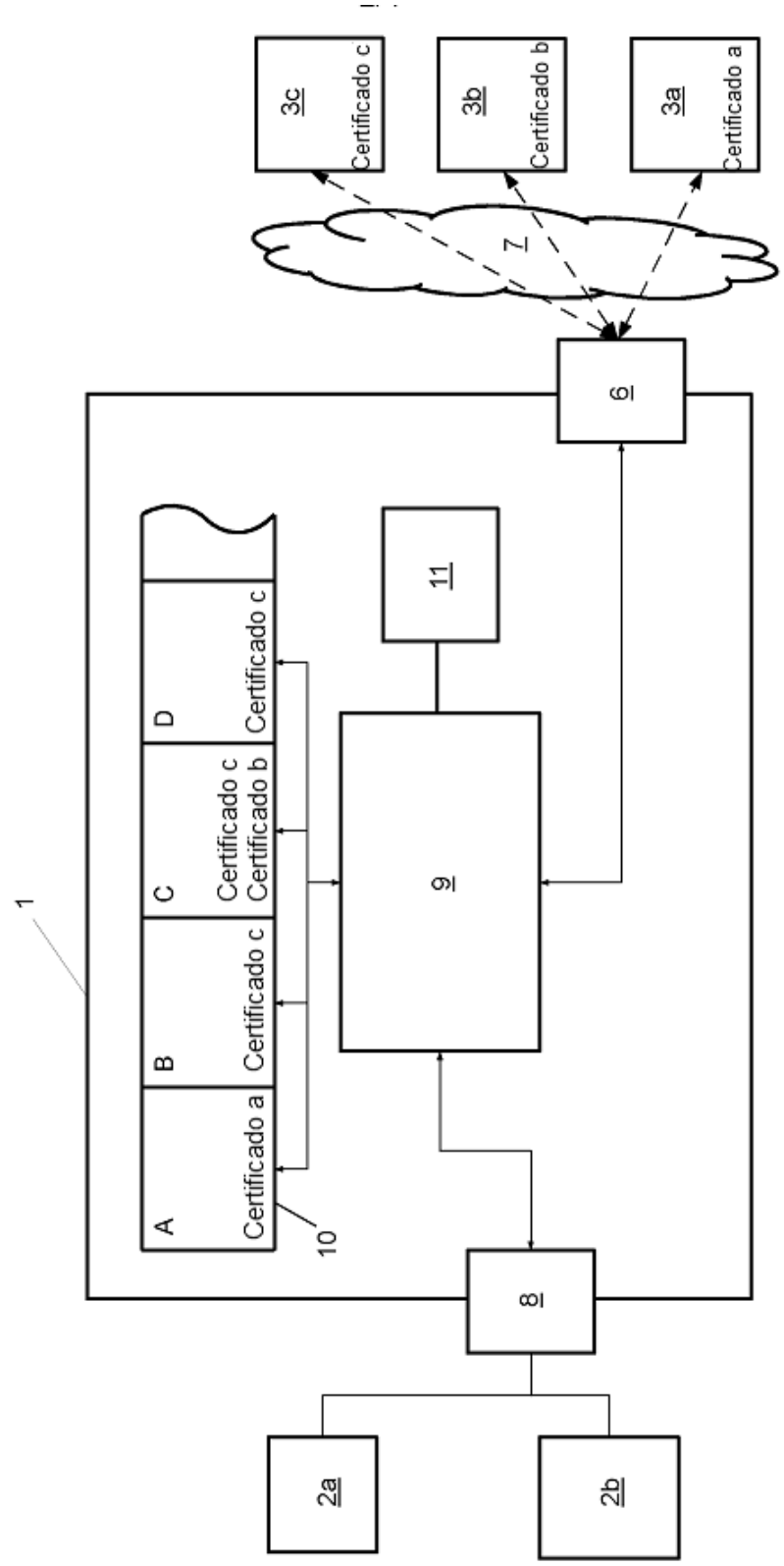

3c
Certificado c
3b
Certificado b
3a
Certificado a
7
6
1
A
Certificado a
B
Certificado c
C
Certificado c
Certificado b
D
Certificado c
10
11
9
8
2a
2b

Fig. 2

Fig. 3

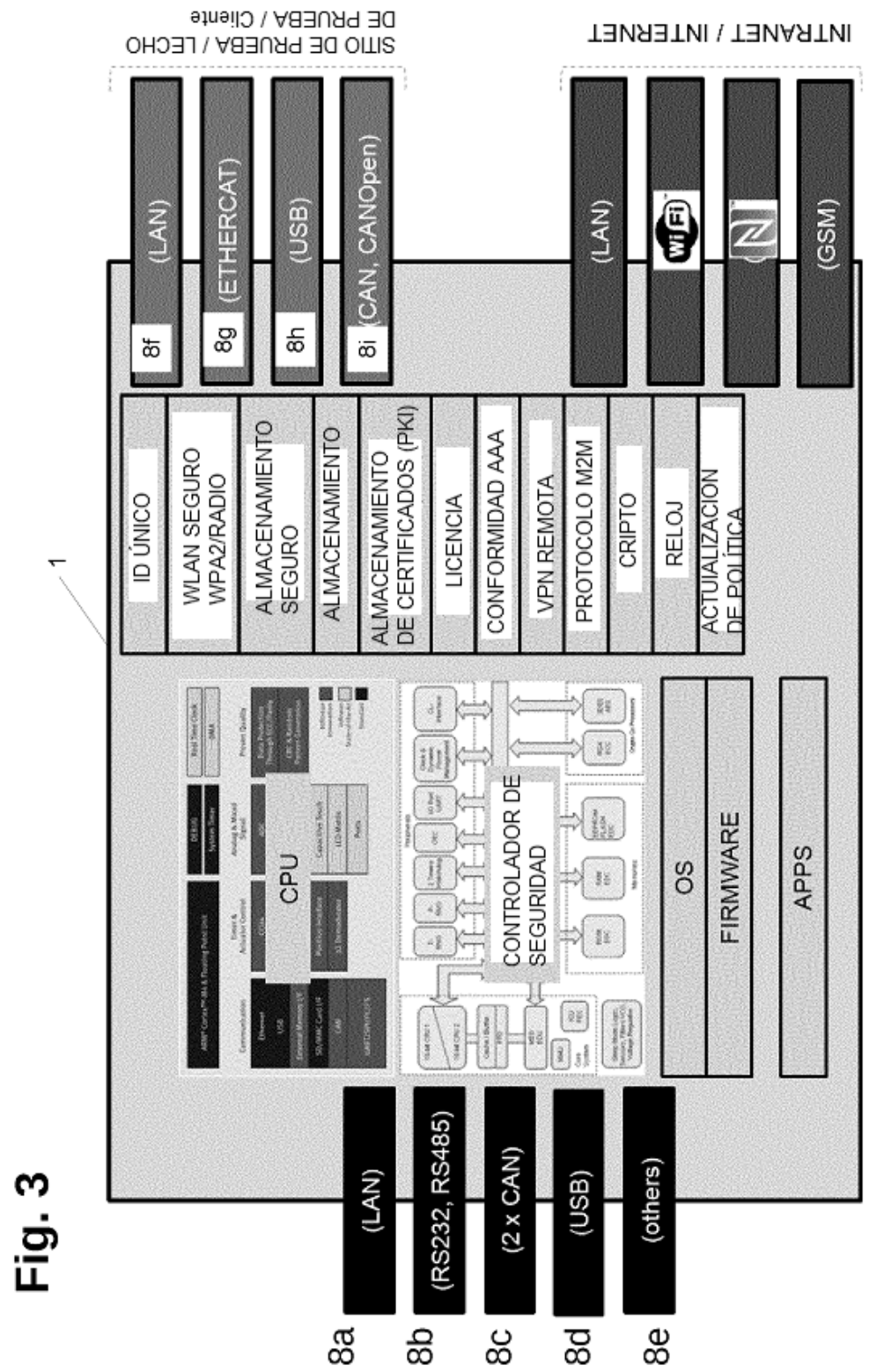
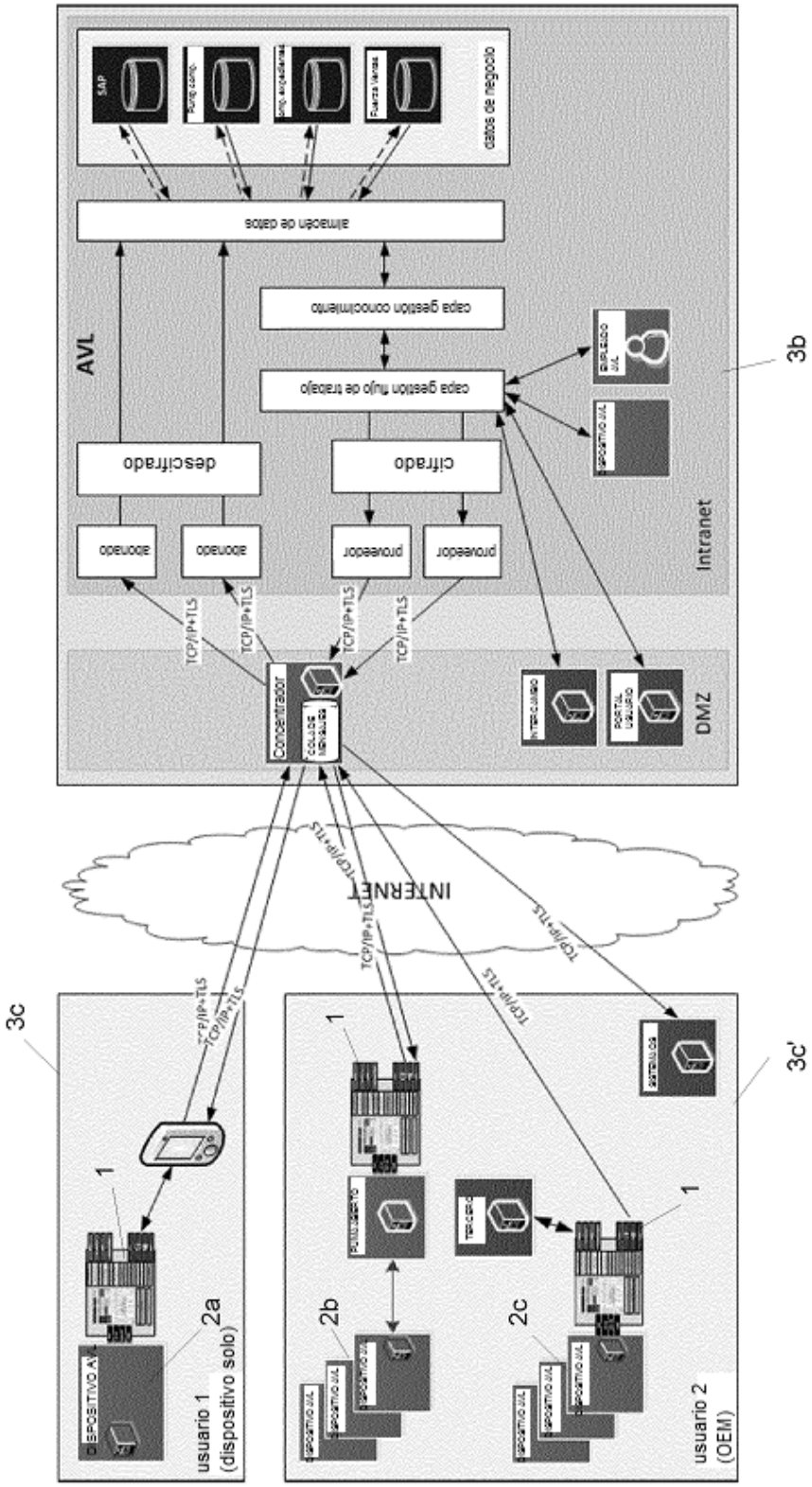

1
ID ÚNICO
WLAN SEGURO WPA2/RADIO
ALMACENAMIENTO SEGURO
ALMACENAMIENTO
ALMACENAMIENTO DE CERTIFICADOS (PKI)
LICENCIA
CONFORMIDAD AAA
VPN REMOTA
PROTOCOLO M2M
CRIPTO
RELOJ
ACTUALIZACIÓN DE POLÍTICA
CPU
CONTROLADOR DE SEGURIDAD
OS
FIRMWARE
APPS
8a (LAN)
8b (RS232, RS485)
8c (2 x CAN)
8d (USB)
8e (others)
8f (LAN)
8g (ETHERCAT)
8h (USB)
8i (CAN, CANOpen)
SITIO DE PRUEBA / LECHO DE PRUEBA / Cliente
INTRANET / INTERNET
(LAN)
(GSM)

Fig. 4


3b
3c
3c'
AVL
Intranet
DMZ
INTERNET
datos de negocio
SAP
almacén de datos
capa gestión conocimiento
capa gestión flujo de trabajo
cifrado
descifrado
proveedor
abonado
Concentrador
TCP/IP+TLS
usuario 1
(dispositivo solo)
usuario 2
(OEM)
DISPOSITIVO AVL
2a
2b
2c
1