(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 932 380**

(51) Int. CI.:

H04L 9/32 (2006.01)
G06F 21/33 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.10.2011 E 20154897 (1)**

(97) Fecha y número de publicación de la concesión europea: **19.10.2022 EP 3684007**

(54) Título: **Autorización físicamente asegurada para aplicaciones de servicios públicos**

(30) Prioridad:

04.11.2010 US 93970210

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.01.2023

(73) Titular/es:

ITRON NETWORKED SOLUTIONS, INC. (100.0%)
230 W Tasman Drive
San Jose, California 95134, US

(72) Inventor/es:

VASWANI, RAJ;
YEUNG, WILSON CHUEN YEW;
SEIBERT, CRISTINA;
BOLYARD, NELSON BRUCE;
DAMM, BENJAMIN N. y
STJOHNS, MICHAEL C.

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Autorización físicamente asegurada para aplicaciones de servicios públicos

Campo técnico

La presente divulgación se refiere a la gestión y control de operaciones asociadas con las compañías de servicios públicos, y más particularmente a la seguridad de los sistemas que gestionan y controlan tales operaciones.

Antecedente

Las compañías de servicios públicos tienen sistemas complejos, altamente interconectados, los cuales se ejecutan en servidores físicos que ejecutan una multitud de módulos de software asociados para gestionar y controlar las operaciones de la compañía de servicios públicos. La Figura 1 es un diagrama de bloques general de algunos de los componentes que pueden encontrarse en un sistema típico de gestión y control de una compañía de servicios públicos que suministra energía eléctrica a los clientes, y posiblemente otros productos básicos, tales como gas, agua, etc. El back office 10 del sistema comprende una serie de subsistemas individuales asociados con diversas operaciones de los servicios públicos, por ejemplo, un sistema 12 de información de cliente (CIS), un módulo 14 de relaciones de cliente (CRM), un sistema 16 de gestión de cortes (OMS), un sistema 18 de información GPS, un sistema 20 de facturación, un módulo 22 de estabilidad de la red, y una interfaz 24 de usuario. Aunque no se ilustra en la Figura 1, pueden estar presentes módulos funcionales adicionales en el back office 10. Algunos de estos subsistemas pueden tener la capacidad de comunicarse con los dispositivos en la red de distribución de los productos básicos que se suministra, y controlar de manera remota las operaciones asociadas con esos dispositivos. Por ejemplo, el servidor de back office puede comunicarse con los medidores 26 individuales ubicados en las instalaciones de los clientes para obtener datos de consumo con fines de facturación, y ordenar a los medidores para desconectar selectivamente, o volver a conectar, el cliente o el suministro de uno o más de los productos básicos proporcionados por la compañía de servicios públicos. Otros comandos a partir del servidor de back office a los medidores individuales pueden incluir comandos para aceptar el flujo de energía saliente de los clientes.

En el ejemplo de la Figura 1, los medidores constituyen nodos de punto final que se comunican con el back office por medio de una red 30 de área local que tiene puntos 32 de acceso que proporcionan salida hacia y fuera de la red. En una realización, la red de área local puede ser una red de malla inalámbrica. Los puntos 32 de acceso se comunican con los servidores del back office 10 por medio de una red 34 de área amplia o un enlace de comunicaciones dedicado.

En un sistema de este tipo, un tema de preocupación es la gestión segura de las desconexiones y reconexiones remotas, las cuales pueden producirse cuando un cliente abandona una instalación o incumple los pagos, o cuando un nuevo cliente toma posesión de las instalaciones, respectivamente. Los comandos maliciosos y/o emitidos de manera errónea para la desconexión y/o reconexión remota de instalaciones pueden tener el potencial de desestabilizar la red de distribución de energía eléctrica. Las reconexiones no autorizadas también podrían resultar en el robo de energía distribuida. Para limitar tales posibilidades, se deben hacer esfuerzos para garantizar que las operaciones de comando y control tengan lugar de manera segura, y sólo mediante las entidades que están autorizadas para llevar a cabo tales operaciones. Sin embargo, dado que el back office de un compañía de servicios públicos típica consiste en una variedad de sistemas interconectados, la aplicación del acceso seguro se hace difícil. Muchos grupos diferentes dentro de la compañía de servicios públicos necesitan el acceso a todo o parte del sistema de software, lo cual complica la capacidad de limitar el acceso lógico y/o físico a subsistemas individuales.

Una posible solución a este problema es colocar determinados sistemas, o partes de tales sistemas, dentro de un entorno físicamente seguro, denominado de aquí en adelante búnker. Los ejemplos de un búnker incluyen una sala o contenedor de acceso restringido, por ejemplo, una sala cerrada con clave, y una carcasa o recinto a prueba de manipulaciones alrededor de un sistema protegido. El búnker restringe severamente el acceso físico a los dispositivos de hardware en los cuales se ejecutan los sistemas, o porciones protegidas de los sistemas. Además, los sistemas dentro del búnker exportan un acceso lógico muy limitado. Sin embargo, esta solución sigue presentando un problema desafiante, ya que es difícil refactorizar los sistemas de software de las compañías de servicios públicos para determinar qué porciones deben estar dentro del búnker, y qué porciones pueden permanecer fuera de él para proporcionar un acceso más flexible a quienes lo necesitan.

El documento US2003/196083 describe un procedimiento el cual comprende la generación de un par de claves criptográficas asociadas con un centro de datos. El procedimiento también incluye el almacenamiento de una clave privada del par de claves criptográficas dentro de una plataforma. La clave privada se utiliza para firmar un valor almacenado en la plataforma para la validación de la inclusión de la plataforma en el centro de datos.

El documento EP1519531 describe un servidor el cual se dice, proporciona un entorno seguro para establecer comunicaciones entre pares entre clientes. Cuando dos clientes del servidor desean establecer una comunicación

entre pares, primero se conectan al servidor. El servidor autentifica a cada cliente y proporciona información a los clientes autentificados para que puedan establecer una comunicación entre pares. Cualquier cliente que abuse de los privilegios de comunicación entre pares puede perder los privilegios de ser autentificado.

Sumario

La invención se define en la reivindicación independiente.

Para proporcionar seguridad general a un sistema de gestión de servicios públicos, se requiere que los mensajes de comando y control críticos que se emiten a los componentes del sistema sean aprobados de manera explícita por una autoridad segura. La aprobación explícita autentifica la acción solicitada y autoriza la ejecución de la acción específica indicada en un mensaje. Los componentes clave del sistema de gestión y control de los servicios públicos que están asociados con el control de acceso se encuentran en un entorno físicamente seguro. Con este enfoque, sólo es necesario asegurar físicamente los subsistemas que se encargan de aprobar las acciones de la red, por ejemplo, por medio de un búnker. En otras palabras, la mayoría de los módulos de gestión, tales como el CIS, CRM, OMS, facturación, etc. pueden permanecer fuera del búnker, evitando así la necesidad de dividir esos subsistemas en componentes bunkerizados y no bunkerizados. El acceso a los componentes críticos de cada uno de los subsistemas no bunkerizados se controla a través del sistema de aprobación bunkerizado.

Breve descripción de las figuras

La Figura 1 es un diagrama de bloques general de un sistema de gestión y control de servicios públicos;

La Figura 2 es un diagrama de bloques de un sistema de back office de una compañía de servicios públicos con componentes bunkerizados;

La Figura 3 es un diagrama de bloques, que representa esquemáticamente el flujo de datos cuando se envía un mensaje a un medidor;

La Figura 4 es un diagrama de bloques de la configuración de un módulo de seguridad de hardware;

La Figura 5 es un diagrama de bloques de un tampón multietapa que cuenta las operaciones criptográficas sobre una ventana deslizante;

La Figura 6 ilustra un ejemplo de sistema y procedimiento para la emisión de permisos de comandos;

La Figura 7 es un diagrama de bloques de un formato ejemplar de una carga útil de permiso; y

La Figura 8 es un diagrama de bloques de un sistema de control y gestión de servicios públicos implementado en múltiples centros de datos.

Descripción detallada

Para facilitar la comprensión de los principios en los cuales se basa la presente invención, ésta se describe de aquí en adelante con referencia al control seguro de los comandos de conexión y desconexión remotos en un sistema de distribución de energía eléctrica. Sin embargo, se apreciará, que un tal ejemplo no es la única aplicación práctica de estos principios. Más bien, pueden emplearse en conexión con cualquier tipo de comando crítico el cual, si se emite de manera inadecuada o errónea, podría tener el potencial de interrumpir o dañar gravemente un sistema. Asimismo, pueden utilizarse junto con todos los comandos y mensajes de control enviados a un componente crítico del sistema cuya operación correcta es esencial en todo momento.

La Figura 2 ilustra un ejemplo de un centro 40 de datos en el cual se implementan los conceptos de la invención. Como es convencional, el centro de datos contiene un número de servidores físicos en los cuales se ejecutan varias aplicaciones 12, 14, 16. Aunque en la figura sólo se ilustran algunas aplicaciones representativas, se apreciará que se pueda implementar un número mayor de tales aplicaciones dentro del centro de datos. Por el contrario, las funciones realizadas por dos o más de las aplicaciones pueden integrarse en un programa único y completo.

También está ubicado dentro del centro de datos un búnker 42 físico que tiene acceso físico limitado, tal como una sala cerrada con paredes reforzadas. Como otro ejemplo, el búnker puede ser, además de o en lugar de estar cerrado, un área vigilada de cerca o protegida utilizando cámaras de seguridad, detectores de movimiento, etc. Como aún otro ejemplo, el búnker puede estar distribuido físicamente, con una relación de seguridad que ha sido establecida entre las partes distribuidas. Como aún otro ejemplo, el búnker puede estar asegurado de manera lógica, tal como mediante el uso de software y/o firmware de ejecución segura cuya funcionalidad está asegurada contra la manipulación física, tal como el embalaje autodestructivo. El búnker no tiene por qué ser una sala, sino que, por ejemplo, puede ser una caja físicamente segura.

Uno o más dispositivos de servidor adicionales que tienen un módulo 44 de seguridad de hardware asociado están ubicados dentro del búnker, para la implementación de un motor 46 de autorización que tiene módulos de software que realizan operaciones relacionadas con la seguridad, tales como la autorización, la autenticación y la contabilidad. El módulo de seguridad de hardware contiene claves privadas y otras claves secretas en una forma segura. También puede contener certificados públicos que están vinculados a las claves privadas. El módulo de seguridad de hardware utiliza preferentemente un algoritmo de seguridad robusto, tal como la criptografía de curva elíptica u otro procedimiento criptográfico de alta seguridad, para realizar las operaciones criptográficas. Un ejemplo de módulos de seguridad de hardware que son adecuados para las aplicaciones descritas en la presente memoria es la línea de módulos de seguridad de hardware *SafeGuard CryptoServer* de Utimaco Safeware AG.

El acceso seguro al búnker, y a los dispositivos del servidor ubicados dentro de este, puede reforzarse con tecnología de biosensores, por ejemplo, detección de huellas dactilares, claves físicas o tokens, y/o protección por contraseña. En una implementación, se puede emplear un sistema de seguridad jerárquico, por capas para maximizar la protección. Si falla una de las capas de seguridad, por ejemplo, si se revelan o roban accidentalmente las contraseñas, puede activarse un mecanismo de seguridad de nivel mayor, tal como un bloqueo de seguridad accionado por clave o token, para mantener la seguridad física de todo el sistema.

Determinados tipos de comandos de las aplicaciones 12-16 etc. de back office no bunkerizadas, están restringidos, de tal manera que no serán ejecutados a menos que sean autenticados individualmente. Por ejemplo, los comandos de desconexión y reconexión remota son una categoría de estos comandos restringidos, debido al potencial que presentan para la interrupción grave de la estabilidad de la red de distribución de energía. Para reforzar la seguridad que forma parte de esos tipos de operaciones, las aplicaciones que las llevan a cabo sólo pueden aceptar comandos para hacerlo si se originan a partir de una consola dentro del búnker 42, o son autenticadas de otra manera por un permiso emitido a partir del búnker 42. Por lo tanto, sólo el personal que tenga autoridad para emitir esos comandos, y que posea los medios necesarios para acceder al búnker, por ejemplo, contraseña, clave, huella digital, etc., será capaz de emitir los comandos restringidos a la aplicación.

Cuando se inicia una operación que provoca la generación de un comando, éste puede ser firmado o autenticado de otra manera por el motor 46 de autorización, y luego reenviado a una interfaz de programación de aplicación (API) asociada con la aplicación adecuada externa al búnker 42. Por ejemplo, el comando puede ser firmado por una clave privada almacenada dentro del módulo 44 de seguridad de hardware. Tras la recepción del comando firmado en una aplicación externa, por ejemplo, una de las aplicaciones 12-16 o una aplicación que se ejecuta en uno de los medidores 26, se verifica por medio de una clave pública a la cual la aplicación tiene acceso. Una vez verificado que se ha originado dentro del búnker, se ejecuta el comando mediante la aplicación externa.

En algunas situaciones, puede no ser práctico que una entidad que emita comandos de desconexión remota esté físicamente presente dentro del búnker. Sin embargo, si se admite la generación remota de tales comandos, tales comandos podrían ser emitidos de manera maliciosa por usuarios que se hagan pasar por entidades autorizadas. Para limitar la posibilidad de tales ocurrencias, de acuerdo con la invención se implementa un módulo 48 de política dentro del búnker. El módulo de política puede ser un componente de software o firmware separado, como se representa en la Figura 2, o estar lógicamente incorporado en el módulo de seguridad de hardware, como se describe de aquí en adelante. El módulo 48 de política puede ser reconfigurado o reprogramado de manera segura, tal como por comandos introducidos desde el interior del búnker. Este módulo contiene la lógica de negocio que examina una acción solicitada y determina si se permitirá llevarla a cabo. Por ejemplo, si los comandos de reconexión se emiten en una secuencia, o con un tiempo relativo, que podría interrumpir la estabilidad de la red de distribución de energía, pueden ser bloqueados por la política y no pasar al motor de autorización para su firma. Además, se pueden levantar banderas de política y tomar acciones adecuadas, tales como desconectar una entidad que emite comandos, cuando se detectan determinadas condiciones. Estas condiciones pueden incluir, por ejemplo:

1. Un gran número de comandos de desconexión remota se emiten al mismo tiempo, por ejemplo, dentro de un intervalo de tiempo predeterminado, indicando una posible intención de desconectar de manera maliciosa a los usuarios de la red de distribución de energía;

2. Los comandos se emiten en un orden sospechoso, tal como una secuencia de comandos repetitivos de conexión y desconexión que se asocian con el mismo cliente, o comandos que son inconsistentes con el estado actual de un cliente, por ejemplo, emitir un comando de desconexión a un usuario que no está ya conectado a la red de energía;

3. Una aplicación solicitante no proporciona las credenciales necesarias, o no se autentifica de otra manera;

4. Una aplicación solicitante no se encuentra entre un conjunto de aplicaciones aprobadas que tienen permiso para emitir determinadas operaciones; y

5. El estado de la red de distribución, basado en las cargas reales de energía y los requerimientos de energía previstos.

Para implementar esta funcionalidad, el búnker puede contener un proxy 50 para las interfaces de programación de aplicaciones (APIs) de las aplicaciones que son externas al búnker. En la operación, cuando se realiza una llamada a la API para una de estas aplicaciones “externas”, la llamada se dirige al proxy 50 dentro del búnker. El proxy consulta la lógica de negocio de servicios públicos en el módulo 48 de política que puede ser necesaria para autorizar la solicitud, y hace que la solicitud sea firmada por la lógica de negocio adecuada. A continuación, la solicitud se pasa al motor 46 de autorización para su firma. Una vez autorizado, el proxy invoca la API normal para la aplicación llamada que es externa al búnker, y pasa a lo largo de la llamada autorizada.

En una implementación alternativa, el búnker 42 puede no incluir un proxy. En este caso, se puede hacer una solicitud directamente a la API de una aplicación externa. A su vez, la aplicación externa llama al motor de autorización dentro del búnker si determina que la operación solicitada requiere una firma. Por defecto, todas las solicitudes podrían pasar al búnker para su autorización, para evitar la necesidad de cualquier determinación por la aplicación externa. Las solicitudes enviadas al búnker son primero verificadas y firmadas por el módulo de política, y luego pasadas al motor 46 de autorización. Una vez que se autoriza una solicitud, la aplicación llamada actúa sobre la solicitud.

El módulo 44 de seguridad de hardware incluido en el búnker 42 puede operar a dos niveles. De aquí en adelante se describen ejemplos en relación con las operaciones que se realizan en los medidores 26. En el primer nivel de operación, la compañía de servicios públicos podría instituir una política de que todas las comunicaciones entre una aplicación en el back office 10 y un medidor 26, o cualquier otro componente de la red 30, deben estar cifradas y firmadas. La implementación de esta política se representa en el ejemplo de la Figura 3. En este ejemplo, una aplicación 52 de gestión de medidor tiene un mensaje, por ejemplo, un comando, para enviar a uno o más de los medidores 26. Este mensaje se construye en un módulo 54 de comando e interfaz de medidor de la aplicación, y se envía al módulo 44 de seguridad de hardware en el búnker 42, con una solicitud para realizar el cifrado y la firma adecuados del mensaje. El módulo 48 de política puede verificar en primer lugar que la solicitud procede de una fuente autorizada. Si es así, se pasa al módulo de seguridad de hardware. El módulo 44 de seguridad de hardware realiza la operación solicitada sobre el mensaje, utilizando las claves adecuadas asociadas con la aplicación, y devuelve los datos cifrados y firmados. El módulo 54 de comando e interfaz de la aplicación de gestión de medidor crea entonces un paquete de datos que incorpora el mensaje cifrado y firmado, y lo transmite al medidor a través de la red 30.

Para los mensajes recibidos a partir de los nodos en la red 30 por la aplicación 52, estos se reenvían primero al módulo de seguridad de hardware, para ser descifrados. El módulo 48 también puede realizar cualquier verificación adecuada de la autenticidad del remitente del mensaje recibido, y de la integridad de los datos. El mensaje verificado y descifrado se devuelve luego a la aplicación 52.

Para las operaciones críticas, tales como las conexiones y desconexiones remotas, el módulo de seguridad de hardware puede operar en un segundo nivel para imponer un límite de tasa en tales operaciones. La Figura 4 representa un ejemplo de la configuración interna de un módulo de seguridad de hardware. El módulo está configurado con un número de ranuras. Cada ranura contiene una colección de claves privadas, certificados, claves secretas y privilegios de acceso, para realizar servicios criptográficos, tales como la firma, el cifrado, el descifrado, etc. Las diferentes ranuras están asociadas con diferentes contextos de seguridad, y contienen las claves, certificados y otra información pertinente a sus respectivos contextos. La realización de un servicio criptográfico en un comando con el módulo de seguridad de hardware, tal como la firma con una clave privada, permite al receptor del comando, por ejemplo, un nodo 26, autenticar la fuente del comando, utilizando una clave pública asociada. El módulo 48 de política realiza la determinación inicial de si se permite presentar un comando solicitado al módulo de seguridad de hardware para uno o más servicios criptográficos.

Cada ranura puede ser configurada de manera selectiva con uno o más límites de tasa, por ejemplo, por medio de una herramienta de administración de línea de comandos, para imponer la lógica de negocio deseada. Un ejemplo de un comando para configurar una ranura es el siguiente:

MSH_configurar ranura=2 tasa↔nombre=”tasa1” ventana=24horas conteo=10,000

Un tal comando configura la Ranura 2 con un límite de tasa máxima de 10,000 operaciones criptográficas por ventana deslizante de 24 horas. Si se produce más de este número asignado de operaciones criptográficas dentro de las 24 horas anteriores, la ranura detiene todas las operaciones criptográficas posteriores. A partir de entonces, será necesario que un administrador reinicie la ranura enviando un comando de reinicio.

Una ranura puede configurarse con más de una tasa, como se indica a continuación:

MSH_configurar ranura=2 tasa↔nombre=”tasa1” ventana=24horas conteo=40,000

MSH_configurar ranura=2 tasa↔nombre=”tasa2” ventana=60minutos conteo=2,000

Estos dos comandos configuran la Ranura 2 con dos ventanas de límite de tasa, una para 40,000 operaciones criptográficas en una ventana deslizante de 24 horas, y otra para 2,000 operaciones criptográficas en una ventana deslizante de 60 minutos.

Si una ranura está configurada con un límite de tasa, todas las operaciones criptográficas ejecutadas en la ranura son contadas contra el límite asignado sobre una ventana deslizante. En el ejemplo proporcionado anteriormente, si hay más de 40,000 operaciones criptográficas en las últimas 24 horas, o más de 2,000 operaciones criptográficas en los últimos 60 minutos, la ranura detiene cualquier operación criptográfica posterior.

En una realización, la contabilización de las violaciones del umbral puede realizarse en incrementos de 5 minutos. La Figura 5 ilustra un ejemplo en el cual se ha configurado una ranura con un límite de 800 operaciones criptográficas en una ventana deslizante de 25 minutos. La ventana deslizante puede ser implementada como un tampón de múltiples etapas 56. El tampón ilustrado comprende cinco etapas 58, cada una de las cuales representa un intervalo de tiempo de 5 minutos. Cada etapa contiene un conteo del número de operaciones criptográficas realizadas por la ranura durante su correspondiente intervalo de tiempo. La siguiente tabla proporciona una instantánea de los datos contenidos en el tampón en un momento determinado.

Etapa	Trama de Tiempo	Conteo
1	-25 a -20 minutos	15
2	-20 a -15 minutos	0
3	-15 a -10 minutos	7
4	-10 a -5 minutos	1
5	-5 a 0 minutos	6

Si la suma de todos los conteos, en este caso 15+0+7+1+6 = 29, excede el umbral, la ranura detiene entonces todas las operaciones criptográficas posteriores hasta que se reinicie administrativamente. Se puede implementar un mecanismo de advertencia para notificar al personal administrativo antes de que se detengan las operaciones. Por ejemplo, puede generarse una primera advertencia cuando el conteo total exceda el 80 % de un límite de tasa, y una segunda advertencia si alcanza el 90 % del límite.

La etapa asociada con el intervalo más reciente, en este caso la Etapa 5, mantiene un conteo consecutivo de cada nueva operación criptográfica. Al final de cada intervalo de 5 minutos, los conteos almacenados se desplazan a la siguiente etapa más antigua La última etapa se reinicia a cero, y comienza a contar de nuevo las operaciones criptográficas para el siguiente intervalo de 5 minutos.

Dado que cada ranura puede configurarse de manera selectiva con sus propios límites de tasa, se proporciona flexibilidad en la implementación de la lógica de negocio. Por ejemplo, como se describe de aquí en adelante, determinados comandos críticos pueden requerir un tipo de autenticación explícita, denominada de aquí en adelante como “permiso”, antes de que puedan ser ejecutados. Estos comandos pueden ser asignados a un contexto de seguridad que se asocia con una ranura que lleva a cabo los procedimientos de permiso, y tienen límites de tasa particularmente estrictos. Otros tipos de comandos pueden ser asignados a diferentes contextos de seguridad y ser cifrados y/o firmados a través de una ranura diferente que tenga límites de tasa menos estrictos.

Para los comandos críticos, tales como los comandos de desconexión y reconexión remota puede ser adecuado un nivel más alto de seguridad, tal como la aprobación por múltiples partes, cada una de las cuales debe ser autenticada en el nodo receptor. Sin embargo, desde el punto de vista de la eficiencia de la red, es deseable que el nodo, al cual se dirige el comando, sólo necesite ser contactado una vez para ejecutar el comando. En un aspecto de la invención, estos objetivos pueden lograrse por medio de un sistema de permisos que proporcione toda la información requerida para permitirle al nodo autenticar un comando. En esencia, cada comando crítico que se envíe a una aplicación, tal como un comando de desconexión a un medidor, puede requerir estar acompañado por un permiso. Como se ha señalado anteriormente, diferentes tipos de comandos pueden ser asignados a diferentes contextos de seguridad. Cuando se va a emitir un comando, ya sea de manera automática mediante una aplicación o a través de una interfaz de usuario, la aplicación que emite verifica el contexto de seguridad del comando. Si se requiere el cifrado, se reenvía el comando a una ranura adecuada del módulo de seguridad de hardware para una tal operación. Si se determina que el contexto de seguridad requiere un permiso, el comando se reenvía a un servidor de permisos en el búnker que emite los permisos. En una realización, la función del servidor de permisos puede ser implementada por una ranura en el módulo de seguridad de hardware.

En la Figura 6 se ilustra un ejemplo de una disposición y procedimiento de emisión de permisos, con referencia a un comando de desconexión de una instalación a partir de la red de distribución de energía. En este ejemplo, uno de los módulos de negocio en el back office 10, por ejemplo, un sistema de contabilidad emite un comando a la aplicación 52 de gestión de medidor, para desconectar las instalaciones asociadas con una cuenta. Tras la recepción de este comando, la aplicación de gestión de medidor puede programar la operación de desconexión para un momento determinado y, a continuación, envía un mensaje a un módulo 59 gestor de carga en un enlace seguro, solicitando permiso para emitir el comando. El gestor de carga es un componente de la lógica de negocio que se ubica dentro del búnker 42 y determina si los cambios de carga en la red de distribución pueden ser perjudiciales. En este ejemplo, el gestor de carga funciona como una implementación de un servidor de permisos. El gestor de carga puede rechazar la solicitud si se determina que el cambio solicitado puede ser perjudicial, aplazar la solicitud durante un periodo de tiempo, por ejemplo, si hay demasiadas solicitudes actualmente pendientes, o aprobar la solicitud. La solicitud al gestor de carga puede incluir información, tal como el nodo de destino, la hora de operación programada, y el tamaño de la ventana de tiempo necesaria para completar la ejecución del comando.

Si la solicitud es aprobada, el gestor de carga crea un permiso que puede ser reconocido por el nodo al cual se dirige el comando. Antes de que el permiso se devuelva a la aplicación 52 de gestión de medidor, se firma con una clave asociada con el gestor de carga. En el ejemplo ilustrado, el servidor de permisos, es decir, el gestor 59 de carga, está separado del módulo 44 de seguridad de hardware. En este caso, por tanto, el permiso se envía al módulo de seguridad del hardware para ser firmado con la clave privada del gestor de carga. El permiso firmado se devuelve al gestor de carga, para ser reenviado a la aplicación 52 de gestión de medidor.

Tras la recepción del permiso firmado, la aplicación de gestión de medidor envía el comando autorizado al nodo 26 que está asociado con las instalaciones que se van a desconectar, junto con el permiso firmado. A continuación, el nodo puede verificar el permiso, por ejemplo, siguiendo una cadena de certificados a partir del permiso, a través de las credenciales del gestor de carga, hasta una autoridad raíz asociada con el operador del sistema para la red de distribución de energía. El nodo también verifica que los valores de tiempo dentro del permiso sean consistentes con la hora actual. Si toda la información es correcta y está verificada, el nodo ejecuta el comando y envía un recibo firmado a la aplicación 52 de gestión de medidor, indicando la finalización del comando. Se puede enviar una copia del recibo al gestor 59 de carga, para permitirle realizar un seguimiento de las solicitudes pendientes.

La aplicación 52 de gestión de medidor también puede firmar la carga útil del paquete que se envía al nodo, para proporcionar dos autorizaciones separadas para el comando que son emitidas por diferentes entidades de control, es decir, la aplicación de gestión de medidor y el gestor de carga. Ambas formas de autorización necesitan ser verificadas por el nodo antes de ejecutar el comando. En este ejemplo, el servidor de permisos, por ejemplo, el gestor de carga no posee las credenciales necesarias para comunicarse directamente con el nodo 26. Más bien, proporciona credenciales a otra entidad de control, en este caso, la aplicación 52 de gestión de medidor, para la ejecución del comando autorizado.

La lógica de negocio para determinar si se aprueba un comando puede ser relativamente simple, por ejemplo, un algoritmo de cubo agujereado en el cual se permite una ráfaga inicial de un número predeterminado de operaciones de desconexión, seguida de un número menor de operaciones por unidad de tiempo. En este caso, la función del gestor de carga podría implementarse dentro de una ranura del módulo de seguridad de hardware, utilizando el control de tasa descrito anteriormente. Otro algoritmo más complejo, puede ser en base al estado de la red de distribución de energía, por ejemplo, haciendo un seguimiento de las cargas de energía reales y realizando determinaciones en base a las proyecciones de los requerimientos de energía. Esta última realización puede realizarse fuera del módulo de seguridad de hardware, como se representa en la Figura 6, por ejemplo, dentro de un sistema físico dedicado, un servidor virtualizado o una aplicación en un sistema compartido.

Además de las desconexiones y reconexiones remotas, se puede requerir que otros tipos de comandos tengan un permiso, tal como los comandos de limitación de carga que están dirigidos a las instalaciones de un cliente para reducir el consumo durante un periodo de tiempo especificado. Además, si la operación segura de un tipo particular de dispositivo en el sistema es crítica para la estabilidad del sistema, tal como un componente de automatización de la distribución, se puede requerir que todos los comandos emitidos a ese dispositivo tengan un permiso. Cada vez que un módulo de back office emite un comando a un tal dispositivo, reenvía el comando al servidor de permisos, para obtener el permiso necesario.

En la Figura 7 se representa un formato ejemplar para un permiso contenido dentro de la carga útil de un mensaje. El primer campo 60 de la carga útil del permiso indica una hora de inicio, es decir, la hora en la cual el permiso pasa a ser válido. Cuando un nodo recibe un mensaje que contiene una carga útil de permiso, el nodo compara la hora de inicio con su hora actual. Si la hora de inicio es posterior a la hora actual más un incremento predeterminado, por ejemplo, cinco minutos, el nodo rechaza el permiso como no válido.

El segundo campo 62 de la carga útil del permiso indica una ventana de duración durante la cual el permiso sigue siendo válido. Este campo contiene un valor que indica el número de intervalos de tiempo predeterminados, por ejemplo, bloques de cinco minutos, más allá de la hora de inicio que el permiso es válido. Si la hora actual del nodo es mayor que la hora de inicio del permiso más el producto del intervalo predeterminado y el valor de la ventana, el permiso se rechaza como no válido. Por ejemplo, si la hora de inicio es 1:00:00, el valor de la ventana es 2, y la hora actual es 1:12:38, el permiso será rechazado por haber expirado.

El siguiente campo 64 de la carga útil del permiso indica la operación que está permitida para ser llevada a cabo. Por ejemplo, este campo puede contener un valor que indique una operación de desconexión de energía, o una operación de reconexión de energía. Se pueden asociar múltiples operaciones con un único permiso. El campo 66 de tipo destino indica el formato del campo 68 destino que sigue. El campo 68 destino designa el nodo, o dispositivo, que debe realizar la operación permitida. Por ejemplo, el destino podría ser la dirección MAC del nodo. El campo 66 de tipo destino indica el formato en el cual se expresa esta dirección, por ejemplo, una cadena de octetos DER.

Para aumentar aún más la seguridad, se puede imponer la restricción de que un comando de desconexión o reconexión sólo puede ser emitido para un medidor a la vez. Antes de emitir un permiso, el gestor de carga puede verificar para garantizar que la dirección de destino para el dispositivo está asociada con un único dispositivo, y no es una dirección de grupo o de difusión.

La carga útil del permiso puede ser firmada por la clave privada asociada con un certificado que tiene privilegios para la operación indicada. Tras la recepción del paquete de datos que contiene la carga útil del permiso, el nodo verifica primero si la operación indicada requiere un permiso. Si se requiere un permiso, el nodo confirma que el certificado y la clave privada que se utilizaron para firmar el permiso tienen los privilegios necesarios para ejecutar la operación solicitada. Si la confirmación es afirmativa, el nodo verifica la autenticidad del permiso firmado, por haber sido firmado por la correspondiente clave privada del certificado indicado. A continuación, el nodo verifica que la designación de destino identifica al propio nodo. Por último, el nodo examina los valores de la hora de inicio y la ventana, en relación con su hora actual, para confirmar que el permiso no ha expirado.

Si todas las comprobaciones de verificación tienen éxito, la operación se ejecuta, y se devuelve una respuesta para confirmar la ejecución exitosa. Si cualquiera de las etapas de verificación falla, el permiso es rechazado, y se devuelve un mensaje de error. Tan pronto como se hayan completado todas las operaciones en el paquete de datos, o se devuelva un mensaje de error, el permiso se descarta y no se retiene más.

En el caso de que el acceso al búnker esté comprometido, se puede implementar una forma adecuada de acción correctiva. Una tal solución es proporcionar un botón de pánico lógico o físico que esté asociado con un búnker. Este botón de pánico puede ser activado (tal como por una persona que presiona un botón físico o activa un elemento de la interfaz de usuario, o por una lógica que hace una determinación adecuada de manera automática) para informar al sistema de gestión de que el búnker asociado con el botón de pánico está comprometido, y ya no se debe confiar. Por ejemplo, cualquier solicitud de servicios de desconexión remota que esté firmada por un búnker comprometido debe ser ignorada.

El botón de pánico puede ser implementado en una variedad de formas. Los ejemplos adecuados incluyen señales de control que se envían a través de un sistema de comunicación inalámbrico o por cable, botones pulsadores físicos en lugares adecuados, por ejemplo, en los escritorios de los empleados, que están conectados a una red de área local o amplia, y/o los dispositivos portátiles con capacidades de comando de audio y conectividad inalámbrica.

La Figura 8 ilustra un ejemplo de un sistema en el cual se puede implementar la funcionalidad de un botón de pánico. En este ejemplo, el sistema de gestión y control de servicios públicos está alojado dentro de dos centros 70 y 72 de datos. Por ejemplo, cada centro de datos puede contener una instancia completa de los diversos subsistemas de gestión y control, por redundancia. Cada centro de datos contiene un búnker asociado, etiquetado respectivamente como “búnker1” y “búnker2”. Cada búnker tiene un certificado con una cadena de certificados cuya raíz está en una autoridad conocida. Los certificados para los dos búnkeres son diferentes entre sí.

Cada uno de los nodos en la red de control, por ejemplo, los puntos 32 de acceso y los nodos 26 de punto final, tiene la capacidad de almacenar e instalar una lista de revocación de certificados. Los puntos 32 de acceso también tienen la capacidad de filtrar las direcciones de origen.

Se describirá una operación ejemplar para una situación en la cual el acceso al búnker1 ha sido comprometido. Se activa un botón de pánico asociado con el búnker1, y la señal de pánico resultante se envía a un servidor en el búnker2 que implementa la función del botón de pánico. Esta señal de pánico incluye una indicación adecuada de la autenticación del dispositivo a partir del cual se envía. Por ejemplo, puede incluir una firma asociada con el dispositivo, o estar acompañada por un valor hash generado de acuerdo con un algoritmo predeterminado. Tras la recepción de una señal de pánico autentificada, el servidor en el búnker 2 emite comandos para configurar una regla de cortafuegos

para todos los puntos 32 de acceso, la cual les indica descartar los paquetes que se originan a partir del centro 70 de datos. El servidor en el búnker2 también emite comandos para configurar una lista de revocación de certificados en todos los puntos de acceso, la cual indica que el certificado asociado con el búnker1 ya no es válido. El servidor en el búnker2 también envía un mensaje a cada nodo de punto final, indicándole que recargue su lista de revocación de certificados a partir de un punto de acceso.

Configurando el filtro del cortafuegos en el punto de acceso para que descarte los paquetes del centro 70 de dato, un posible atacante puede ser ralentizado un periodo de tiempo suficiente para permitir que las listas de revocación de certificados se propaguen a todos los nodos de punto final. Con el fin de recuperar el búnker1 después de que se haya producido una posible brecha, se debe instalar un nuevo certificado, y realizar y propagar nuevas asociaciones con ese certificado a todos los nodos en la red de control.

En resumen, la invención divulgada proporciona una variedad de características de seguridad para reducir el riesgo de acciones maliciosas o de otra manera inapropiadas asociadas con la entrega de productos básicos proporcionados por los servicios públicos. Los comandos críticos que tienen el potencial de interrumpir la estabilidad de una red de distribución de servicios públicos están asegurados a través del mecanismo de un búnker físico que limita el acceso a los componentes sensibles del sistema de gestión de back office, junto con el uso de un módulo de seguridad de hardware para autenticar, firmar y cifrar tales comandos. Un marco de autorización basado en permisos proporciona un nivel de seguridad más fino para unos comandos particularmente críticos. El módulo de seguridad de hardware también puede configurarse para limitar la tasa en la cual se ejecutan los comandos, para impedir aún más los intentos de emitir secuencias de comandos inadecuadas.

Aquellos con conocimientos ordinarios en la técnica apreciarán que los conceptos divulgados pueden ser incorporados en otras formas específicas, siempre que permanezcan dentro del ámbito de las reivindicaciones adjuntas. Las realizaciones actualmente divulgadas se consideran, en todos los aspectos, ilustrativas y no restrictivas. El ámbito de la invención se indica en las reivindicaciones adjuntas, en lugar de la descripción anterior.

REIVINDICACIONES

1. Un procedimiento para controlar dispositivos en una red (30) de servicios públicos, que comprende:

generación de un comando para una operación que debe ser llevada a cabo por un dispositivo (26) en la red de servicios públicos;
reenvío del comando a un módulo (44) de seguridad de hardware;
dentro del módulo de seguridad de hardware, ejecutando las siguientes funciones:

conteo de un número de servicios criptográficos realizados por el módulo de seguridad de hardware en un período de tiempo especificado,
cuando el número contado de servicios criptográficos realizados dentro del período de tiempo especificado excede un límite de umbral, terminar la ejecución de servicios criptográficos en los comandos recibidos, y
cuando el número contado de servicios criptográficos realizados dentro del período de tiempo especificado no excede el límite de umbral, realizar un servicio criptográfico en el comando que permita a un receptor del comando, sobre el cual se ha realizado el servicio, autenticar el comando como uno que el receptor está permitido a ejecutar; y

transmisión del comando, sobre el cual se ha realizado el servicio criptográfico, al dispositivo en la red de servicios públicos para llevar a cabo la operación.

2. El procedimiento de la reivindicación 1, en el que el conteo del número de servicios criptográficos se realiza sobre una ventana (56) de tiempo deslizante del periodo especificado.

3. El procedimiento de la reivindicación 2, en el que el conteo del número de servicios criptográficos se realiza con respecto a una pluralidad de ventanas de tiempo deslizantes, cada una de las cuales está asociada con una longitud de tiempo y un límite de umbral respectivos diferentes.

4. El procedimiento de cualquier reivindicación anterior, en el que el servicio criptográfico incluye el cifrado del comando.

5. El procedimiento de cualquier reivindicación anterior, en el que el servicio criptográfico incluye la firma del comando.

6. El procedimiento de cualquier reivindicación anterior, que incluye además la etapa de generación de una advertencia cuando el número contado de servicios criptográficos alcanza un valor predeterminado menor que dicho límite de umbral.

7. El procedimiento de cualquier reivindicación anterior, en el que el módulo de seguridad de hardware comprende una pluralidad de ranuras, y en el que dichas funciones se ejecutan en una de las ranuras.

8. El procedimiento de la reivindicación 7, en el que dichas funciones también se ejecutan en una segunda ranura, utilizando un límite de umbral respectivo diferente.

9. El procedimiento de cualquier reivindicación anterior, en el que el dispositivo está configurado para determinar si un comando recibido está autorizado utilizando una clave pública asociada con el servicio criptográfico.

10. un centro (40) de datos que comprende:

un búnker físico, teniendo el búnker (42) físico acceso restringido al mismo, y comprendiendo un módulo (44) de seguridad de hardware; y
una aplicación de back office no bunkerizada;
en la que la aplicación de back office no bunkerizada está configurada para generar un comando para una operación que se llevará a cabo en una red de servicios públicos,
en el que el módulo de seguridad de hardware está configurado para:

contar un número de servicios criptográficos realizados por el módulo de seguridad de hardware en un período de tiempo especificado,
cuando el número contado de servicios criptográficos realizados dentro del período de tiempo especificado excede un límite de umbral, terminar la ejecución de más servicios criptográficos en los comandos recibidos, y

cuando el número contado de servicios criptográficos realizados dentro del tiempo especificado no exceda el límite de umbral, realizar un servicio criptográfico en el comando que permita a un receptor del comando, sobre el cual se ha realizado el servicio, autenticar el comando como uno que el receptor está permitido a ejecutar; y

transmitir el comando, sobre el cual se ha realizado el servicio criptográfico, a un dispositivo en la red de servicios públicos para llevar a cabo la operación.

11. El centro de datos de la reivindicación 10, en el que el conteo del número de servicios criptográficos se realiza sobre una ventana (56) de tiempo deslizante del periodo especificado; y
en el que el conteo del número de servicios criptográficos se realiza de manera opcional con respecto a una pluralidad de ventanas de tiempo deslizantes, cada una de las cuales está asociada con una longitud de tiempo y un límite de umbral respectivos diferentes.

12. El centro de datos de la reivindicación 10 o la reivindicación 11, en el que el servicio criptográfico incluye el cifrado del comando, y/o en el que el servicio criptográfico incluye la firma del comando.

13. El centro de datos de acuerdo con cualquiera de las reivindicaciones 10 a 12, en el que el módulo de seguridad de hardware está configurado además para generar una advertencia cuando el número contado de servicios criptográficos alcanza un valor predeterminado menor que dicho límite de umbral.

14. El centro de datos de acuerdo con cualquiera de las reivindicaciones 10 a 13, en el que el módulo de seguridad de hardware comprende una pluralidad de ranuras, y en el que dichas funciones se ejecutan en una de las ranuras.

15. El centro de datos de la reivindicación 14, en el que dichas funciones también se ejecutan en una segunda ranura, utilizando un límite de umbral respectivo diferente.

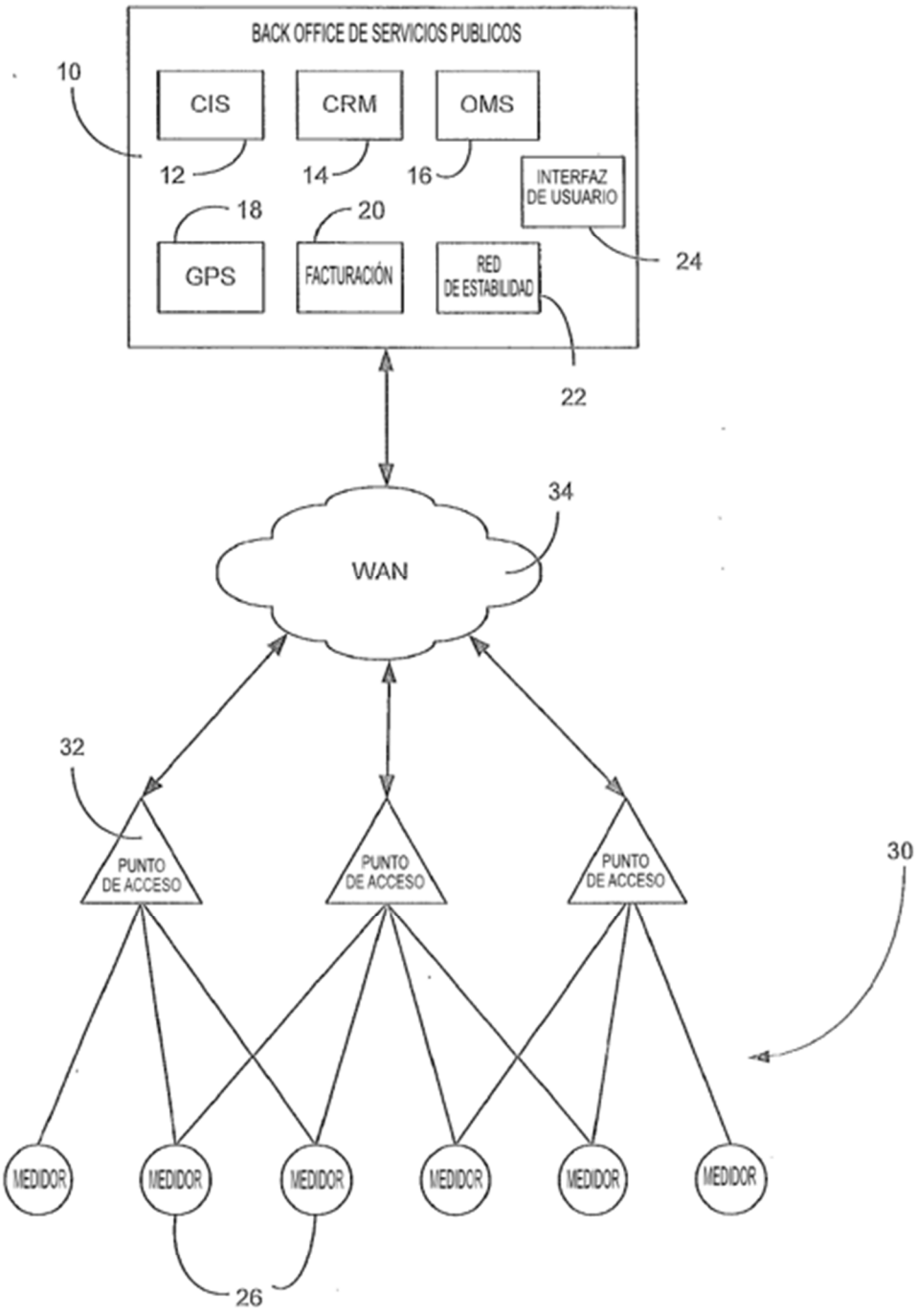
BACK OFFICE DE SERVICIOS PUBLICOS
10
CIS
CRM
OMS
12
14
16
INTERFAZ DE USUARIO
24
18
20
GPS
FACTURACIÓN
RED DE ESTABILIDAD
22
34
WAN
32
PUNTO DE ACCESO
PUNTO DE ACCESO
PUNTO DE ACCESO
30
MEDIDOR
MEDIDOR
MEDIDOR
MEDIDOR
MEDIDOR
MEDIDOR
26

Fig. 1

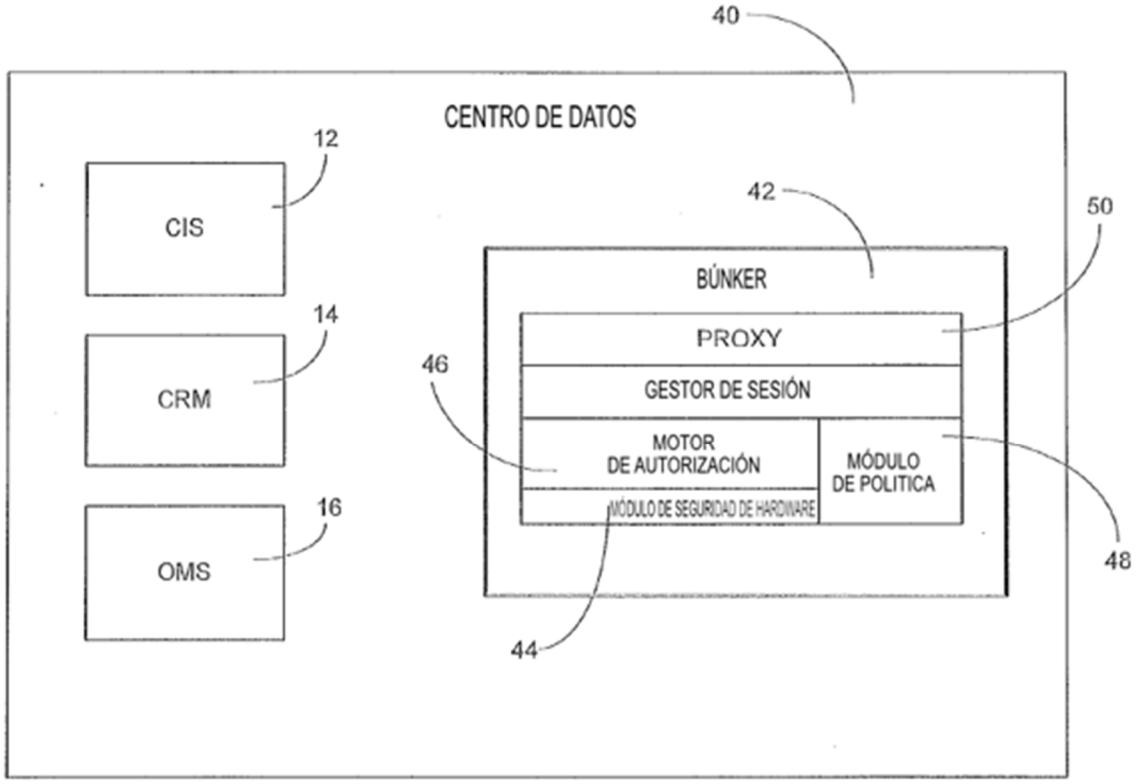
40
CENTRO DE DATOS
12
CIS
14
CRM
16
OMS
42
50
BÚNKER
PROXY
GESTOR DE SESIÓN
46
MOTOR
DE AUTORIZACIÓN
MÓDULO
DE POLITICA
MÓDULO DE SEGURIDAD DE HARDWARE
48
44

Fig. 2

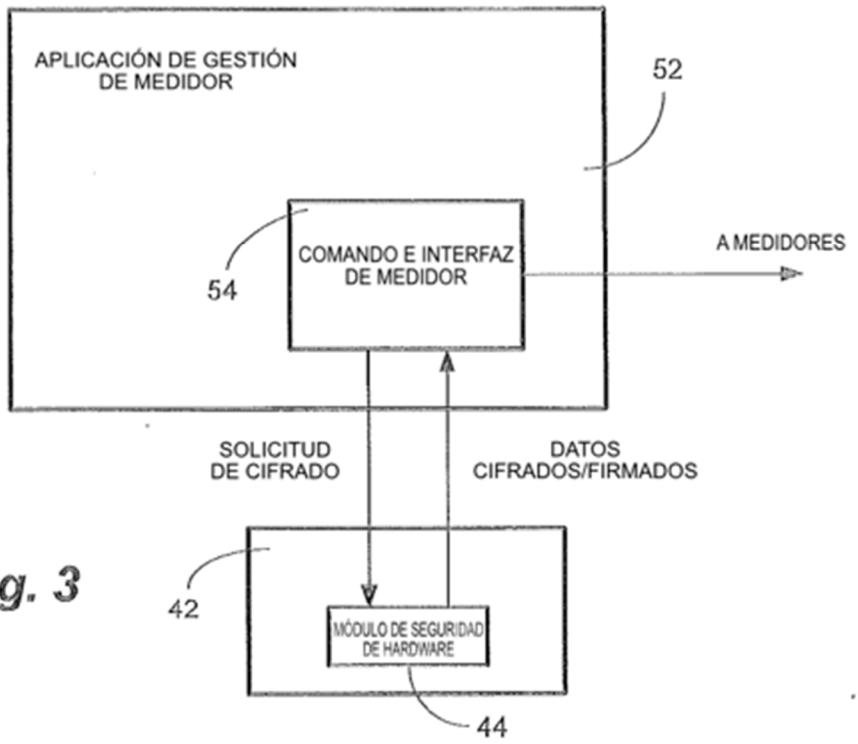
APLICACIÓN DE GESTIÓN DE MEDIDOR
52
COMANDO E INTERFAZ DE MEDIDOR
54
A MEDIDORES
SOLICITUD DE CIFRADO
DATOS CIFRADOS/FIRMADOS
42
MÓDULO DE SEGURIDAD DE HARDWARE
44

Fig. 3

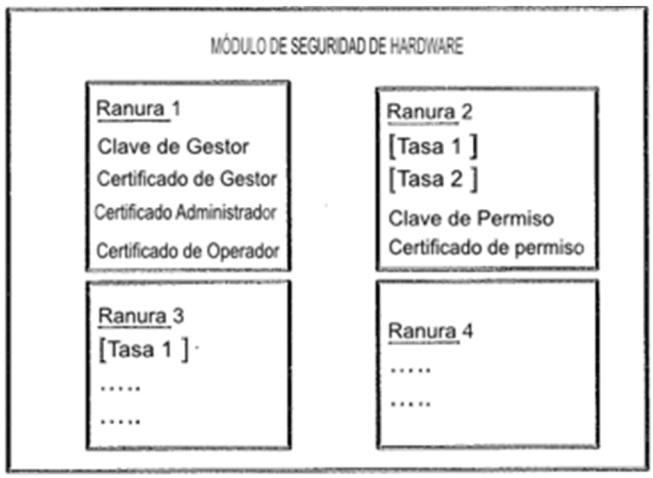
MÓDULO DE SEGURIDAD DE HARDWARE
Ranura 1
Clave de Gestor
Certificado de Gestor
Certificado Administrador
Certificado de Operador
Ranura 2
[Tasa 1]
[Tasa 2]
Clave de Permiso
Certificado de permiso
Ranura 3
[Tasa 1]
.....
.....
Ranura 4
.....
.....

Fig. 4

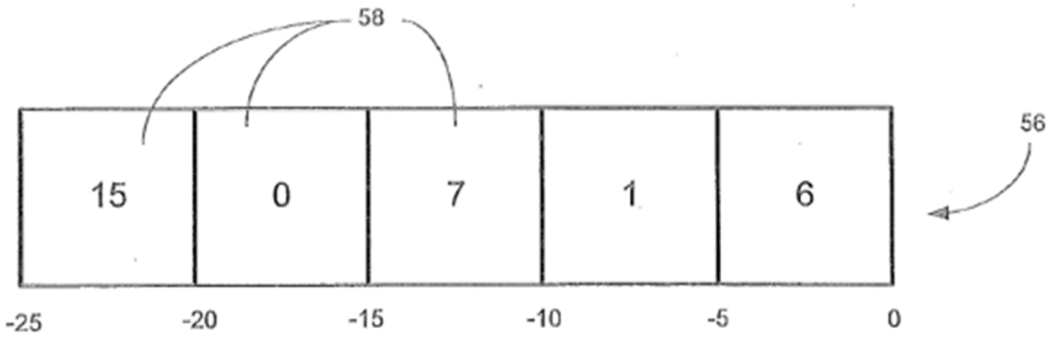

Fig. 5

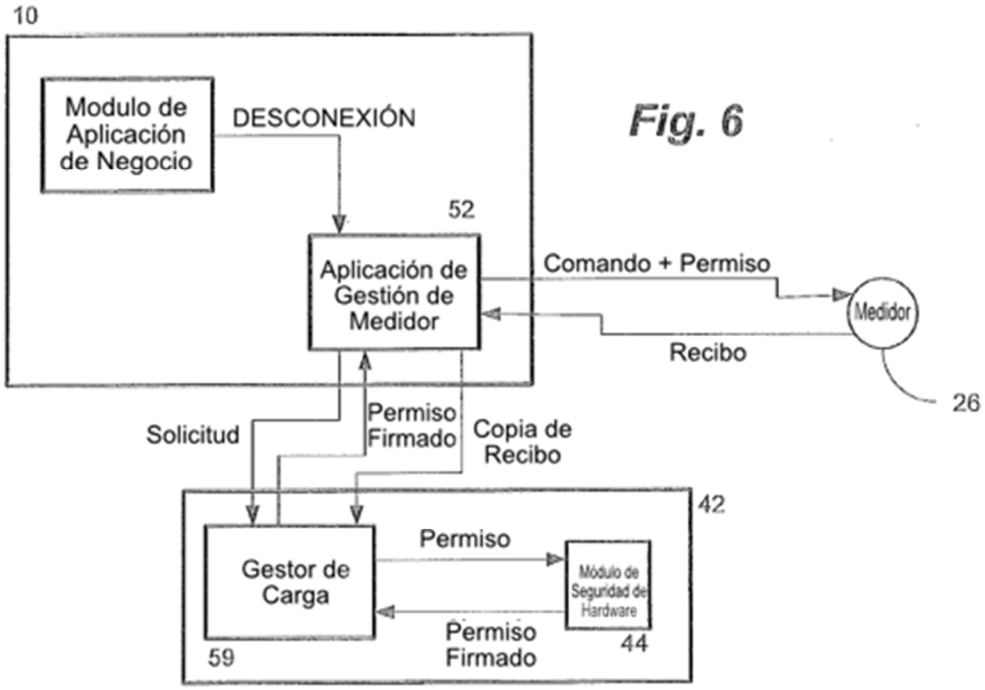

Fig. 6

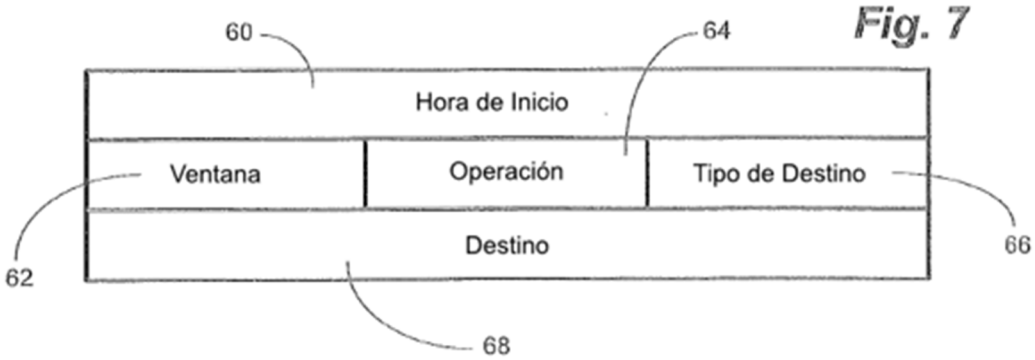

Fig. 7

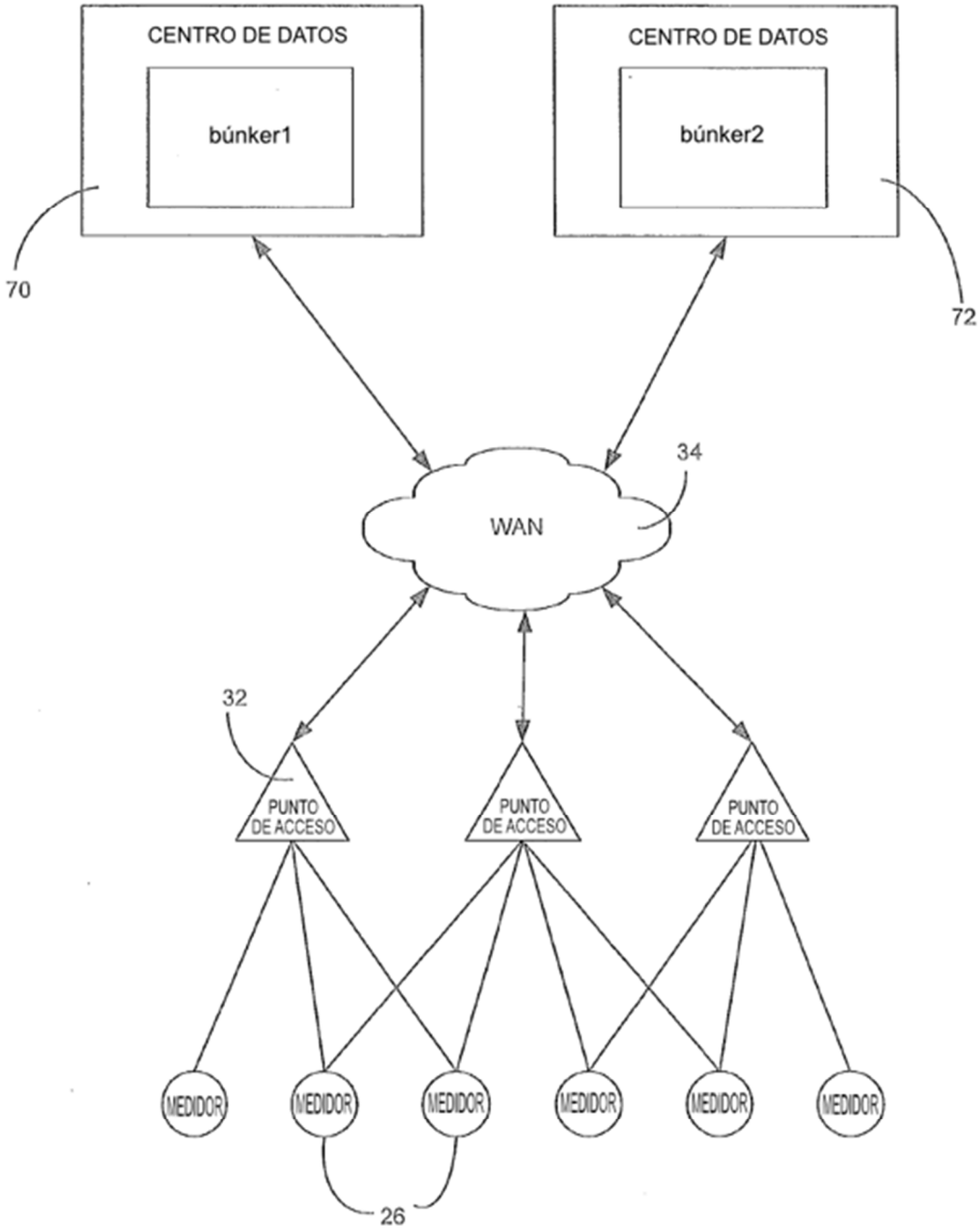
CENTRO DE DATOS
búnker1
CENTRO DE DATOS
búnker2
70
72
34
WAN
32
PUNTO DE ACCESO
PUNTO DE ACCESO
PUNTO DE ACCESO
MEDIDOR
MEDIDOR
MEDIDOR
MEDIDOR
MEDIDOR
MEDIDOR
26

Fig. 8