(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 605 781**

(51) Int. CI.:

***G01D 4/00*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.01.2012 PCT/EP2012/050786**

(87) Fecha y número de publicación internacional: **09.08.2012 WO12104149**

(96) Fecha de presentación y número de la solicitud europea: **19.01.2012 E 12700492 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2671052**

(54) Título: **Medidor de servicios para medir un consumo de servicios y optimizar comunicaciones aguas arriba y método para la administración de estas comunicaciones**

(30) Prioridad:

**02.02.2011 US 201161438665 P**
**27.04.2011 EP 11163844**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**16.03.2017**

(73) Titular/es:

**NAGRAVISION S.A. (100.0%)**
**Route de Genève 22-24**
**1033 Cheseaux-sur-Lausanne, CH**

(72) Inventor/es:

**LE BUHAN, CORINNE;**
**NICOLAS, CHRISTOPHE y**
**CONUS, JOËL**

(74) Agente/Representante:

**TOMAS GIL, Tesifonte Enrique**

## DESCRIPCIÓN

Medidor de servicios para medir un consumo de servicios y optimizar comunicaciones aguas arriba y método para la administración de estas comunicaciones.

Introducción

[0001] Esta invención concierne al campo de medidores de servicios que están monitorizados y gestionados por al menos un centro de gestión de servicios a través de una red de comunicación de un sistema de medida.

Antecedentes

[0002] La desregulación en curso en los mercados de distribución de energía a nivel mundial está generando la necesidad de que las redes de distribución inteligentes y medidores inteligentes permitan a proveedores y consumidores de servicios controlar el consumo detallado de un usuario final en cualquier momento a través de redes de comunicación o redes de comunicación inseguras, tales como internet.
El mercado de energía está particularmente afectado, pero por ahora las cuestiones relacionadas también son relevantes para otros mercados de servicios tales como agua o gas.

[0003] Los medidores automatizados permiten que proveedores de servicios lean remotamente los registros del medidor que registran en una base regular la información de consumo del usuario.
Sin embargo, esta lectura solo se produce de vez en cuando a discreción del proveedor de servicios y usa típicamente una red privada (inalámbrica o por cable) bajo el control estricto del proveedor de servicios.
La generación siguiente de metros automatizados (denominados metros inteligentes) habilitará proveedores de servicios, tales como centro de gestión de servicios remotos, para controlar el consumo detallado de un usuario final en cualquier momento y a una granularidad mucho más precisa, a través de unas redes de comunicación abiertas.
Se espera que esta supervisión mucho más clara aliente índices previstos más precisos y ofertas al usuario final, posiblemente por la competición de proveedores de servicios, ya que los mercados de servicios se desregulan de forma similar a los mercados de telecomunicaciones en los 90s.
Será aún más pertinente cuando las (redes domésticas) HAN se interconectan con la red inteligente para informar directamente de su información de uso final antes que concentrar este informe de información a través del medidor inteligente.

[0004] El proveedor de servicios también puede remotamente administrar, configurar y mejorar el medidor a través de la red de comunicación.
En mercados determinados, los medidores inteligentes incluso se requieren para implementar una característica de desconexión remota, de modo que los servicios pueden remotamente parar la distribución de servicios por ejemplo en el caso de falta de pago.

[0005] Consecuentemente, un medidor inteligente genera típicamente o pasa através de la caja de interconexión HAN, mensajes de lectura automatizada aguas arriba al equipo de gestión de proveedor de servicios remotos a un índice mucho más frecuente del que lo hacían los medidores automatizados anteriores.
Aquellos mensajes también llevan posiblemente una carga útil significativamente más larga, ya que se monitorizan más detalles mediante el proveedor de servicios.

[0006] Claramente, la dependencia resultante de los servicios públicos y funcionalidad de facturación en los mensajes de comunicación remotos levantan nuevos intereses sobre la privacidad y confidencialidad de datos, así como también la robustez de sistema eficaz para fallos de software y amenazas emergentes, tales como gusanos de red inteligente y virus toma ventaja de defectos de diseño de seguridad de medidor inteligente.
Aquellos defectos no se pueden saber en el momento del despliegue, pero se pueden volver críticos más tarde.
Esto es particularmente evidenteen el caso de la característica de desconexión remota, como una gran objetivo de interrupción para el ciber-terrorismo, pero también un posible punto de introducción para robos locales como una vía para desconectar algunas alarmas de las casas de su fuente de energía.

[0007] En la práctica, los diseños de seguridad de hoy de redes inteligentes y medidores inteligentes están inspirados en gran medida por la industria de telecomunicación y una gran parte de estos está sujeta a la estandarización emergente por comités internacionales tal como ANSI o IEC.
Los mensajes importantes necesitan ser protegidos por un canal autentificado de seguridad que se va a establecer utilizando protocolos criptográficos sobre una comunicación punto a punto individual entre el medidor de servicios y el equipo de gestión de proveedor de servicios remotos.
Por lo tanto, recientes especificaciones estándar en ese área, tal como ANSI C12.22 o IEC 62056/COSEM, definen cómo encriptar y firmar las cargas útiles de mensaje, típicamente mediante una disposición de clave de sesión entre el centro de gestión de servicios o el concentrador de colección de datos y el medidor de servicios.

[0008] Como se describe en el informe oficial de Itron "OpenWay by Itron Security Overview", para cuestiones prácticas operativas, algunos de los mensajes aguas abajo desde el centro de gestión de servicios o el concentrador

colector pueden ser de difusión o de multidifusión en la red de suministro sin un reconocimiento de recepción segura de cada medidor de servicios objetivo, típicamente debido al gasto de administrar los mensajes aguas arriba correspondientes en una utilización de medida de gran escala (por ejemplo 10 millones de metros).
Sin embargo, la información de consumo de uso de servicios de medidor individual, tal como uso de servicios reales o registros de evento, se deben comunicar punto a punto desde el medidor de servicios al centro de gestión de servicios o el concentrador colector.
Por lo tanto, para ampliar su sistema de medida inteligente para sostener hasta 10 millones de medidores, Itron informa de la necesidad de procesar hasta 24000 mensajes por segundo aguas arriba, mientras la mensajería aguas abajo de difusión/multidifusión permite factorizar los mensajes hasta 200 por segundo.

[0009] En la práctica, los problemas de escalabilidad se harán aún más críticos, ya que la red inteligente se vuelve además muy implementada y desregulada debido a tres factores independientes mayores:

- La desregulación permite al usuario final elegir entre diferentes ofertas actuales de servicio de proveedores de servicios a partir de un medidor de servicios único, posiblemente al mismo tiempo.
  En ese escenario, el medidor de servicios necesitará comunicarse aguas arriba con diferentes centros de gestión de servicios o concentradores colectores y así multiplicar básicamente el número de mensajes aguas arriba por el número de proveedores de servicios.
- La necesidad de imponer sistemáticamente la mensajería de seguridad de medidor de servicios y mejorar la implementación de seguridad de medidor de servicios interna para prevenir el riesgo de ataque ciberterrorista de red inteligente, al igual que el incentivo de fraude de hackear el medidor de usuario final.
  Por lo tanto, el módulo criptográfico de medidor de servicios altamente sensible necesita operar lo más profundamente posible en el diseño de sistema de medidor, típicamente hasta los datos de medidor de servicios y registros de clave, antes que en la interfaz de red de comunicación, requeriendo así protocolos criptográficos adicionales y mecanismos de mensajería además de las especificaciones de estándar actuales.

[0010] El documento US 2006/0271244 divulga un dispositivo de supervisión de energía incluyendo procedimientos para la comunicación segura de salida de datos de este dispositivo.
El dispositivo de supervisión de energía incluye un par de claves públicas/privadas usadas para encriptar y/o firmar digitalmente comunicaciones por el dispositivo.
Esto permite que los receptores de estas comunicaciones autentiquen las comunicaciones para asegurar que el dispositivo y/o comunicaciones no hayan sido comprometidos.
Sin embargo, el uso del par de claves públicas/privadas y/o firma digital se hace según un esquema tradicional que es conocido hoy en día por el experto en la materia. Tal esquema no optimiza las comunicaciones cambiadas entre el dispositivo de supervisión de energía y la entidad que cobra por el uso de energía.
Este dispositivo de supervisión de energía es más bien capaz de comunicaciones vía una "red" red eléctrica ad-hoc para facilitar comunicaciones entre dispositivos que son inaccesibles sustancialmente debido a limitaciones físicas o económicas.

[0011] El documento US 2011/0224935 se refiere a un dispositivo de medición, en particular, un contador de energía para la detección segura y visualización de los datos de cuenta y a un método para el reconocimiento de manipulaciones.
Se refiere a la necesidad de que los valores que se toman y se muetran en la factura deberían estar fuera de duda para la protección de consumidor.
Estos valores son tomados localmente, se digitalizan y se transfieren a una oficina central para ser procesados.
El objetivo sugerido por este documento es el diseño de una comunicación de datos de presentación del dispositivo de medición al menos a un sistema, de manera que permita al sistema identificar los datos de medición devueltos como sus propios datos, incluyendo un control de manipulación de datos.
Con este fin, el dispositivo tiene la capacidad de recibir datos de medición firmados o encriptados, almacenar dichos datos de medición en una memoria en vistas de distribución y tiene la capacidad de ofrecer información de tiempo relacionada con una referencia temporal.

[0012] El documento US 2006/0206433 sugiere que indicativos digitales se apliquen a datos de energía dosificada que se recogen por un sistema de colección de datos comunes.
El sistema recibe datos de medidores (cada uno de un cliente determinado) que pueden tener una o más utilidades.
Los datos enviados por cada uno de los medidores se encriptan previamente y se firman.
Después de la recepción de los datos por el sistema de colección de datos comunes, los datos se almacenan por este sistema, usando criptografía de clave pública para asegurar que sea accesible solo por el consumidor destinado de los datos.
Cuando los datos se transmiten al consumidor destinado, se firman digitalmente por el sistema para asegurar la autenticidad de los datos, ya que se han recibido por el consumidor.
El uso de distintivos de encriptación e indicativos digitales permite al sistema asegurar la integridad de los datos recogidos aún después de que los datos hayan sido comunicados desde el sistema (es decir, que hayan sido publicados externamente).
Sin embargo, para recopilar todos los datos medidos por millones de medidores, el sistema de colección de datos comunes tiene que estar provisto de bases de datos enormes, por una parte, y estas bases de datos deben estar conectadas a un sistema (ordenadores) de manipulación de datos muy potente para proporcionar rápidamente los

datos de una manera eficaz.

[0013] Por lo tanto, hay una necesidad de un sistema de comunicación segura y método que optimice además la manipulación de datos, en particular, los mensajes aguas arriba sobrecargados entre un dispositivo de supervisión de uso de servicios (medidor de servicios) y una pluralidad de dispositivos o centros de gestión de servicios remotos.

Resumen de la invención

[0014] La presente invención se refiere a un medidor de servicios para la medida de al menos un consumo de servicios y para la optimización del tráfico de mensajes intercambiados con una pluralidad de centros de gestión de servicios remotos según la reivindicación 1 y el método según la reivindicación 7.

[0015] Con este fin, este medidor de servicios comprende:
- una unidad de medición para la medida de al menos un valor de consumo de servicios V,
- una unidad de comunicación para el envío de mensajes a los centros de gestión remotos asignados al medidor de servicios para el tratamiento del valor de consumo de servicios V por los centros de gestión remotos,
- una memoria para depositar un identificador único ID que pertenece al medidor de servicios y una primera clave K1 para el encriptado de mensajes que se van a enviar por la unidad de comunicación,
- una unidad de encriptación para el encriptado del valor de consumo de servicios V como un primer criptograma C1,
- un generador de mensaje para generar un mensaje de servicio que contiene dicho primer criptograma C1 para ser enviado a los centros de gestión remotos,
- la unidad de comunicación que además es capaz de recibir mensajes de dichos centros de gestión de servicios remotos y el medidor de servicios comprende además:
- un generador de clave para generar una clave de carga útil Kp destinada a ser compartida por la pluralidad de centros de gestión de servicios remotos, la clave de carga útil es usada por la unidad de encriptación para el encriptado del valor de consumo de servicios V, para formar un mensaje de carga útil compartida adecuada para ser enviada a la pluralidad de centros de gestión de servicios remotos,
- la unidad de encriptación que además es capaz de generar un segundo criptograma C2, para cada uno de los centros de gestión de servicios remotos, por el encriptado de la clave de carga útil Kp con la primera clave K1, el segundo criptograma C2 está destinado a ser incluido, por el generador de mensaje, en un mensaje de control para ser enviado a un centro de gestión remoto dedicado.

[0016] Preferiblemente, el segundo criptograma C2 se incluye con el primer criptograma C1 en el mismo mensaje de servicio, ya que comprende el primer criptograma C1.
Así, los primeros y segundos criptogramas se pueden enviar bien en el mismo mensaje o en dos mensajes separados.

[0017] Según la presente invención, el uso de una clave de carga útil para el encriptado, según un esquema de encriptación simétrico, valores de consumo de servicios V que deben ser frecuentemente proporcionados por cada medidor de servicios, como mensajes aguas arriba a un centro de gestión de servicios remoto, permite optimizar el tráfico de mensajes intercambiados entre estas entidades.
De esta manera, cada mensaje aguas arriba puede ser ventajosamente dividido en un mensaje de carga útil compartida y un mensaje de control dedicado.
Por lo tanto, el mismo mensaje de servicios encriptado puede ser enviado, como un mensaje de informe de servicios, a una pluralidad de centros de gestión remotos que pueden compartir este mensaje gracias a su encriptación por una clave de carga útil compartida.
Esto puede ser particularmente ventajoso en el caso de este mensaje de servicios se difunda por el medidor de servicios.
La presente invención también sugiere varias formas de realización para generar la clave de carga útil.
En una forma de realización, el dispositivo de supervisión de uso de servicios publicos pre-procesa la generación de clave de carga útil y operaciones de encriptación de carga útil compartidas cuando se almacenan los datos de carga útil en dichos registros del dispositivo y comunica los mensajes de carga útil compartidos al centro de gestión de servicios remotos posteriormente.

[0018] La presente invención también se refiere a un método para la administración de una comunicación entre un medidor de servicios, usado para la medida de al menos un consumo de servicios, y al menos un centro de gestión de servicios remota a cargo de tratar el consumo de servicios.
Esta red de comunicación se supervisa por al menos un centro de supervisión que actúa como una entidad de confianza en las comunicaciones, particularmente, durante una fase de inicialización de estas comunicaciones.
Con este fin, el medidor de servicios del presente método comprende:
- una unidad de medida para la medida de al menos un valor de consumo de servicios V,
- una unidad de comunicación para el envío de mensajes al centro de gestión de servicios remotos,
- una memoria para depositar un identificador único ID que pertenece al medidor de servicios y una primera clave K1 requerida para la encriptación/desencriptación de mensajes que se van a enviar/recibir por la

unidad de comunicación,
- una unidad de encriptación para el encriptado del valor de consumo de servicios V como un primer criptograma C1,
- un generador de mensaje para generar un mensaje de servicios con el primer criptograma C1 para ser enviado al centro de gestión de servicios remotos.

[0019] El método incluye los pasos de:
- lectura, por el medidor de servicios, del valor de consumo de servicios V medido por la unidad de medida,
- generación, por el medidor de servicios, del mensaje de servicio comprende el primer criptograma C1,
- envío, por el medidor de servicios, del mensaje de servicio al centro de gestión de servicios remotos en vistas de su tratamiento por este centro de gestión de servicios remotos,
- la comunicación se establece entre el medidor de servicios y una pluralidad de centros de gestión de servicios remotos encargados del tratamiento de al menos una parte del consumo de servicios y la comunicación es supervisada por al menos un centro de supervisión, la unidad de comunicación, además, es capaz de recibir un mensaje desde los centros de gestión de servicios remotos.

[0020] Este método comprende además los pasos de:
- para cada uno de los centros de gestión de servicios remotos, enviar una solicitud al centro de supervisión preguntando por la asignación del medidor de servicios al centro de gestión de servicios remotos, esta solicitud comprende al menos el identificador único ID del medidor de servicios,
- transmisión por el centro de supervisión de unos datos de clave al centro de gestión de servicios remotos; dichos datos de clave son usados según sean necesarios los datos de entrada de una operación criptográfica para la desencriptación/encriptación de los mensajes.

[0021] Otras formas de realización acerca el presente método se describen en la siguiente descripción detallada.

Breve descripción de los dibujos

[0022]
La Figura 1 muestra un diagrama de bloques de un centro de gestión de servicios remotos conectado a un medidor de supervisión de uso de servicios públicos por una red de comunicación que soporta difusiones unidireccionales o mensajería de multidifusión y mensajería de unidifusión bidireccional.
La Figura 2 muestra un diagrama de bloques de diferentes centros de gestión de servicios remotos conectados al mismo medidor de supervisión de uso de servicios por una o más redes de comunicación donde la mensajería aguas arriba desde el medidor al centro de gestión de servicios se divide en mensajes de control dedicado y mensajes de carga útil compartida.
La Figura 3 representa un diagrama de bloques que muestra el procesamiento de un valor de inicialización por un módulo criptográfico inicializado por una clave secreta para generar como resultado una clave compartida.
La Figura 4 representa el diagrama de flujo de una operación del dispositivo de monitorización de uso de servicios conforme a una forma de realización de la presente invención.
La Figura 5 representa el diagrama de flujo de la operación de centro de gestión de servicios conforme a una forma de realización de la presente invención.
La Figura 6a, 6b y 6c muestra diferentes variantes de un sistema de servicios que comprende un centro de supervisión como una tercera entidad, además del medidor de servicios y el centro de gestión de servicios remotos.

Descripción detallada

[0023] En el sistema propuesto, el centro de gestión de servicios remotos 20 de la figura 1 implementa varios procesos de gestión de servicios 21 tales como la facturación de manipulación de datos, gestión de carga y control de interrupción, en la colaboración con el sistema de gestión de medidor remoto.

[0024] El mismo sistema de gestión de medidor remoto 22 de la figura 1 comprende componentes funcionales encargados de la supervisión de uso de medidor de imposición, actualizaciones de microprograma de medidor y control de operaciones de medidor mediante comunicaciones seguras 6, 7 con los metros individuales 10 a través de la red de comunicación 5.

[0025] La red de comunicación 5 de la figura 1 puede ser cualquier red física de comunicación de medida de servicios, tal como, pero no limitada a, una red de cable, el hilo de línea de potencia o una red inalámbrica, que soporte cualquier protocolo de conexión de redes de comunicación, tal como, pero no limitado a, Protocolo de Internet (IP) v4 o v6.
Los encargados de comunicaciones seguras de la figura 1 ambos en el lado de centro de gestión de servicios remotos y el lado de medidor de servicios individuales necesitan además cumplir una especificación de mensajería común.
Esta especificación puede ser privada cuando el sistema de gestión de medidor de servicios remotos y los medidores de servicios 10 son todos proporcionados por el mismo fabricante de medidor.

Sin embargo, como el mercado de servicios se desregula, hay una necesidad en aumento de estandarizar esta interfaz de comunicación, de modo que varios vendedores de servicios y varios fabricantes de medidor pueden proporcionar sistemas interoperables y un equipo que cumpla con las especificaciones estándares comúnes.
Los protocolos de mensajería de híbrido son otra alternativa, donde la mensajería estándar que maneja la funcionalidad de medida básica se combina con extensiones de mensajería privada avanzada.
El método privado, completo o híbrido es de relevancia particular para asegurar una supervisión de seguridad, mantenimiento y renovabilidad a lo largo del tiempo, ya que cualquier especificación estándar, una vez publicada, debe ser obligatoria como se específica para la vida estándar y, por lo tanto, no puede proporcionar cualquier flexibilidad de actualización en caso de una infracción en la especificación de seguridad sin revisar el mismo estándar.
Los ejemplos de especificaciones de estándar de conexión de redes de datos de medidor de servicios incluyen las series DLMS IEC62056 en combinación con las especificaciones complementarias COSEM o ANSI C12.22 en combinación con el estándar industrial para tablas de datos del dispositivo final ANSI C12.19.

[0026] El medidor de servicios 10 de la figura 1 comprende una unidad de medida 11 que dispone de al menos un contador principal para la medida de al menos un valor de consumo de servicios V en referencia a un consumo de servicios, tales como energía eléctrica [Kw/h] o gas o agua [m3].
También comprende una unidad de comunicación 12 para el envío/recepción de mensajes 8 (es decir, mensajes de informe o mensajes de estado) a/de al menos un centro de gestión de servicios remotos que se asigna al medidor de servicios.
En muchos casos, tal medidor de servicios será asociado a solo un centro de gestión de servicios remotos, típicamente un proveedor de servicios y/o una entidad de facturación, que procesa el valor de consumo V en vistas de facturación.
Sin embargo, debido a la desregulación en curso en los mercados de distribución de energía a nivel mundial, el medidor de servicios puede también estar asociado a más de un centro de gestión de servicios remotos, bien proporcionando consumos de servicios diferentes (por ejemplo gas y electrico) o para el tratamiento de uno o más consumos de servicios, según intervalos de tiempo diferentes o en días específicos de la semana.
El medidor de servicios comprende además una memoria 13 para depositar cualquier tipo de datos, en particular, un identificador único ID que pertenece al medidor de servicios y una primera clave K1 para el encriptado de mensajes 8 que van a ser enviados por la unidad de comunicación 12.
El valor de consumo de servicios V puede ser también almacenado en esta memoria, en particular, para una duración limitada durante la que su tratamiento puede ser realizado, típicamente cuando su tratamiento es diferido con respecto a su introducción por la unidad de medida.
El medidor de servicios 10 también comprende una unidad de encriptación 14 para el encriptado de mensajes o datos para ser enviados fuera del medidor de servicios, en particular, para el encriptado del valor de consumo de servicios V como un primer criptograma C1, teniendo en cuenta que un criptograma es un texto cifrado o un valor cifrado.
El medidor de servicios 10 también comprende un generador de mensaje 15 para generar mensajes 8 tal como un mensaje de servicio que contiene el primer criptograma C1 para ser enviado al centro de gestión de servicios remotos 20.
Un procesador CPU, que está encargado de la administración de todas las funciones y los componentes del medidor de servicios, se ilustra esquemáticamente en el área central del medidor de servicios 10 de la figura 1.
Típicamente, el procesador CPU está encargado de administrar la seguridad de comunicaciones realizada con el medidor de servicios a través de la red 5, por un lado, y está encargado de las operaciones de medidor de servicios local de administración, por otro lado.

[0027] Según la presente invención, el medidor de servicios 10 comprende además un generador de clave 16 para generar una clave de carga útil Kp.
Esta clave de carga útil Kp será usada para la unidad de encriptación para el encriptado del valor de consumo de servicios V, generando el primer criptograma C1.
Este resultado se puede apreciar C1=(V)Kp.
Un segundo criptograma C2 se genera por la unidad de encriptación 14.
Este segundo criptograma C2 resulta desde la encriptación de la clave de carga útil Kp con la primera clave K1 y se puede apreciar C2=(Kp)K1.
Este segundo criptograma C2 se destina a ser incluido, por el generador de mensaje 15, en un mensaje 8 para ser enviado al centro de gestión 20 de servicios remotos.
Preferiblemente, este segundo criptograma será incluido al menos una vez en tal mensaje, por ejemplo, al menos durante una fase de inicialización donde el medidor de servicios 10 se asigna al centro de gestión 20 de servicios remotos.
Más preferiblemente, este segundo criptograma C2 será periódicamente incluido en el mensaje 8, al menos cada vez que la clave de carga útil Kp se cambie o renueve.

[0028] La Figura 2 ilustra, mediante un diagrama de bloques, la solución sugerida por la invención para optimizar la sobrecarga de mensajería aguas arriba en un sistema de comunicación entre un dispositivo de supervisión de uso de servicios públicos 10 y al menos un centro de gestión 20 de servicios remotos.
En particular, esta figura muestra que los mensajes aguas arriba están ventajosamente divididos en mensajes de

carga útil compartida y mensajes de control dedicado.
Los mensajes de carga útil pueden ser, por lo tanto, compartidos por diferentes centros de gestión de servicios remotos (indicados por ejemplo A, B, C en esta Fig.) a través de la red de comunicación 5.
Así, todos los centros de gestión de servicios remotos pueden recibir los mismos mensajes, por ejemplo simultáneamente.

[0029] En este caso, el medidor de servicios 10 genera:

- mensajes de carga útil compartida que pueden ser unidifusión, multidifusión o difusión a la atención de centros de gestión A, B y C;
- mensajes de control A que se dedican a y unidifunden a un centro de gestión de servicios A;
- mensajes de control B que se dedican a y unidifunden a un centro de gestión de servicios B;
- mensajes de control C que se dedican y unidifunden a un centro de gestión de servicios C.

[0030] Como se ha descrito anteriormente, el medidor de servicios genera una clave de carga útil Kp, encripta en al menos una carga útil compartida (típicamente el valor de consumo de servicios V) mediante la clave de carga útil Kp para obtener el primer criptograma C1, encripta esta clave de carga útil Kp para obtener el segundo criptograma C2, transmite este primer criptograma C1 en al menos un mensaje de carga útil compartida 8 y transmite el segundo criptograma C2 en al menos un mensaje de control 8 al menos a un centro de gestión de servicios remotos 20.
La encriptación de la clave de carga útil Kp se puede realizar usando la primera clave K1 almacenada en la memoria 13 del medidor de servicios.

[0031] En una forma de realización, la primera clave K1, almacenada en la memoria 13 es una denominada clave de centro de gestión, en particular, la clave pública pertenece al centro de gestión de servicios remotos 20.
Esta clave se puede usar para el encriptado de mensajes 8 que se deben enviar al centro de gestión de servicios remotos 20.

[0032] En otra forma de realización, para otros fines de equilibrio de carga de mensajería, el tiempo de comunicación aguas arriba por un medidor de servicios al centro de gestión de servicios remotos se programa por el medidor de servicios según la programación de instrucciones recibidas desde el centro de gestión de servicios remotos o desencadenadas por eventos determinados en el medidor de servicios como se han preprogramado en dicho microprograma del dispositivo o directamente desencadenados por mensajes de solicitud recibidos desde el centro de gestión de servicios remotos a través de la red de comunicación.

[0033] En otra forma de realización, el medidor de servicios 10 comprende una clave secreta Kt (es decir, una clave personal que pertenece a este medidor de servicios 10) que se puede almacenar en la memoria 13 o en otros medios de almacenamiento, preferiblemente en un área fijada.
Según esta forma de realización, la memoria 13 también comprende un valor de inicialización I0 que puede ser preferiblemente recibido por el medidor de servicios 10 dentro de un mensaje de inicialización.
Este medidor de servicios 10 está también provisto de un módulo criptográfico 17 como está ilustrado en la figura 1.
Este módulo criptográfico integra una función para generar una clave compartida Ks tomando la clave secreta Kt como una primera entrada y el valor de inicialización I0 como una segunda entrada, como se muestra en la figura 3.
La clave compartida Ks se puede considerar como una especie de clave de sesión con una vida más larga.

[0034] En otra forma de realización, el medidor de servicios 10 preferiblemente comprende una unidad de desencriptación 14' para la desencriptación de mensajes recibidos por la unidad de comunicación 12.
La unidad de desencriptación y la unidad de encriptación puede ser parte de la misma unidad, es decir, una unidad de codificación/descodificación.
Gracias a la unidad de desencriptación 14', el medidor de servicios puede recibir mensajes encriptados, tales como mensajes de control encriptado, de todo el centro de gestión 20 de servicios remotos al que es asignada.
Dentro de un esquema de encriptación simétrica, estos mensajes de control podrían ser encriptados por la clave compartida Ks, mientras que dentro de un esquema de encriptación asimétrica, estos mensajes de control son encriptados con una clave privada, que pertenece al centro de gestión de servicios remotos y se pueden descifrar por el medidor de servicios usando la clave pública del centro de gestión de servicios remotos 20 que han sido previamente almacenados en la memoria 13 del medidor de servicios.

[0035] Según otra forma de realización, el mensaje de inicialización que comprende el valor de inicialización I0 se encripta con una clave de sesión de inicialización Ki.
Esta clave de sesión de inicialización Ki se almacena en la memoria 13 del medidor de servicios y se usa mediante la unidad de desencriptación 14' para la desencriptación del mensaje de inicialización cuando lo recibe la unidad de comunicación 12.

[0036] En otra forma de realización, el mensaje de inicialización comprende una firma S para su autentificación.
Por lo tanto, el medidor de servicios 10 comprende una unidad de autentificación 18 para la verificación de la autentificación de la firma S. Esta unidad de autentificación permite la carga del valor de inicialización I0 en el módulo criptográfico 17 solo tras una autentificación exitosa.
Así, la generación de la clave compartida Ks no se puede manipular introduciendo un valor de inicialización falso I0

en el módulo criptográfico 17 al recibimiento de un mensaje de inicialización hackeado.

[0037] El organigrama de la figura 4 ilustra una implementación de ejemplo de una forma de realización donde las operaciones siguientes son ejecutadas:

- El medidor de servicios 10 adquiere datos de monitorización para ser proporcionados al centro de gestión 20 de servicios.
  Tales datos de supervisión pueden comprender por ejemplo información de supervisión de uso, información de pago, registro de eventos de operación de medidor, información de supervisión de seguridad.
- El medidor de servicios formatea los datos de supervisión en un mensaje de carga útil conforme a especificaciones estándar tal como tablas de datos ANSI C12,19 o IEC 62056/COSEM.
  Alternativamente, el formato de carga útil se puede definir en una especificación privada, pero es preferiblemente en un formato que es comprensible por todos los centros de gestión de servicios conectados A, B y C.
  En aplicaciones determinadas, también se puede utilizar una mezcla de especificación estándar y de formato privado.
- El medidor de servicios 10 genera una clave de carga útil Kp, la encripta y la transmite como información de control (o mensaje de control) al centro de gestión de servicios 20 conforme a los protocolos de comunicación segura en su lugar entre el centro de gestión de servicios y el dispositivo de supervisión de servicios.
  Preferiblemente, esta comunicación segura usa estrategias compartidas punto a punto tal como una sesión de canal autentificado seguro Ks juntamente computarizada por el centro de gestión de servicios previstos y el dispositivo de supervisión de servicios.
  Tales protocolos de seguridad punto a punto se definen por ejemplo en las especificaciones estándar ANSI C12.22 o IEC 62056/COSEM.
  La generación, encriptación y proceso de transmisión de la clave de carga útil Kp se pueden ejecutar sincrónicamente o asíncronamente con la operación de formación de carga útil, pero preferiblemente en un modo asincrónico.
  En particular, es posible generar la clave de carga útil Kp solo de vez en cuando para reducir los mensajes de control de unidifusión necesarios necesitados para transmitir esta clave de carga útil compartida Ks individualmente para cada centro de gestión de servicios A, B y C.
  De esta manera, también contribuye a la optimización de comunicaciones aguas arriba.
- El medidor de servicios protege la supervisión de datos de carga útil mediante la clave de carga útil Kp.
  Dependiendo de los modelos de amenaza y estándar elegidos o protocolos de criptografía privada, esta operación de protección puede comprender uno o más pasos de encriptación y/o autentificar y/o firmar partes de datos de carga útil utilizando la clave de carga útil Kp, por ejemplo conforme a las especificaciones de seguridad ANSI C12.22 o IEC 62056/COSEM.
  Preferiblemente, se usa un cifrado del estado de la técnica eficaz simple, tal como AES con una clave de carga útil de bit Kp 128.
  Alternativamente, la clave de carga útil Kp también se puede combinar con otras llaves privadas y/o públicas y/o valores de clasificación, que se pueden almacenar en el dispositivo de supervisión al tiempo de fabricación, generados localmente por el dispositivo de supervisión o se transmiten previamente desde el centro de gestión de servicios bien directamente o como parte de un microprograma del dispositivo de supervisión mejorado por cualquier medio de comunicación remoto o local.
  En casos específicos, algoritmos de criptografía adaptados pueden ser aplicados, en particular, en manipulación de datos de supervisión de seguridad sensibles.
- En el momento de la comunicación de nuevo al centro de gestión de servicios remotos, en la implementación del ejemplo de la figura 4, el medidor de servicios 10 formatea el mensaje de carga útil compartida 8 y lo transmite a los centros de gestión de servicios 20 en modo unidifusión, multidifusión o difusión.

[0038] Como se ilustra en la figura 4, el procesamiento de datos de carga útil compartida y las operaciones de protección se pueden ejecutar de antemano al tiempo de transmisión.
En este caso, los datos de carga útil compartidos protegidos se almacenan en un búfer de memoria o registro del medidor de servicios.
En el momento de la transmisión, el medidor de servicios lee los datos de carga útil compartidos protegidos desde el registro para formatear y transmitir el mensaje de carga útil compartida 8 al centro de gestión de servicios remotos 20 objetivo.
Proceder de esta manera ahorra potencia y memoria informática en el medidor de servicios, ya que la protección de carga útil mediante algoritmos criptográficos necesita hacerse solo una vez y puede hacerse de antemano.
Además, la transmisión a cada centro de gestión de servicios remotos A, B o C puede tener lugar en un tiempo diferente.

[0039] La Figura 5 ilustra las operaciones inversas que tienen lugar en el centro de gestión de servicios remotos que serán ahora descritas:

- El centro de gestión 20 de servicios remotos recibe un mensaje de control 8 y extrae la información de control de este mensaje de control.
- El centro de gestión de servicios remotos desencripta y verifica la información de control para derivar la clave de

carga útil Kp conforme a los protocolos de comunicación segura en su lugar entre el centro de gestión de servicios y el dispositivo de supervisión de servicios.
Preferiblemente, esta comunicación segura usa estrategias compartidas punto a punto tales como una clave compartida de canal autentificado seguro Ks conjuntamente computarizada por el centro de gestión de servicios y el dispositivo de supervisión de servicios.
Tales protocolos de seguridad punto a punto se definen por ejemplo en las especificaciones estándar ANSI C12.22 o IEC 62056/COSEM.

- El centro de gestión de servicios recibe un mensaje de carga útil compartida 8 y extrae la carga útil protegida de mensaje de carga útil compartida.
- El centro de gestión de servicios deriva la carga útil clara desde la carga útil protegida mediante la clave de carga útil computarizada anteriormente Kp.
  Esta operación puede comprender uno o más pasos de desencriptación y/o verificación de las partes de datos de carga útil protegida que utilizan la clave de carga útil Kp, conforme al método de protección aplicado por el dispositivo de supervisión de servicios.

[0040] También son posibles otras variantes del sistema y método representados en la figura 4 y la figura 5.

[0041] Para el caso de la encriptación y las operaciones de formación de mensaje se pueden ejecutar en un orden diferente del medidor de servicios 10.

[0042] El mensaje de carga útil 8 también se puede pre-procesar y almacenar en los tampones de memoria 13 o registrar por el medidor de servicios.

[0043] El medidor de servicios 10 y el centro de gestión de servicios remotos 20 puede intercambiar otros mensajes 8 para sincronizar los intercambios de mensajes de control o la actualización Ks de clave compartida.

[0044] Más allá de los mensajes puramente de carga útil de supervisión funcional, un número de mensajes necesitan ser enviados aguas arriba por el medidor de servicios al centro de gestión de servicios remotos, en particular, en el caso de credenciales de seguridad y actualizaciones de microprograma de seguridad requieren una recepción segura y ejecución de confirmación de mensaje de vuelta al servicio que inicia la mejora.
Para cuestiones prácticas, los mensajes de mejora pueden ser de difusión o de multidifusión aguas abajo, lo que significa que todos los medidores de servicios 10 previstos los recibirán y manejarán al mismo tiempo, y consecuentemente enviarán la confirmación de mensaje de vuelta aguas abajo al mismo tiempo, dando así como resultado una congestión posible del tráfico de red y salidas de escalabilidad de tratamiento de valor máximo en el centro de gestión de servicios remotos.

[0045] Para un mejor equilibrio de la carga aguas arriba entre los medidores de servicios 10 conectados múltiples, el registro de medidor de servicios de amortiguación se puede programar para durar más o menos dependiendo de parámetros determinados, tales como el identificador único de medidor de servicios ID (número de serie), el número de versión de microprograma de medidor de servicios, la suscripción de índice de servicio del medidor de servicios o información de consumo, o un comando explícito para ser enviado individualmente al medidor de servicios por el servicio en un mensaje de unidifusión aguas abajo.

[0046] También es posible insertar las órdenes explícitas en el microprograma de mejora de difusiones o mensajes de multidifusión, en particular, si el protocolo de mensajería de medida inteligente permite definir grupos de medidores de servicios propuestos: cada grupo puede luego compartir un comando explícito y el microprograma de mejora de carga útil será anexo con una concatenación de órdenes explícitos, uno para cada grupo objetivo.
En ese escenario, idealmente el vendedor de servicios definirá el miembro de grupo basado en información geográfica/de localización, si está disponible, de modo que la carga aguas arriba también sea equilibrada a nivel de red local.

[0047] El medidor de servicios podría también comprender una unidad de validez 19 (Fig. 1) para dar con mensajes de renovación enviados por el centro de gestión de servicios remotos.
Alternativamente, la unidad de validez 19 podría ser usada para controlar la validez de un sello de tiempo T incluido en un mensaje entrante (por ejemplo, un mensaje de inicialización, un mensaje de control o cualquier mensaje de datos) enviado por el centro de gestión de servicios remoto o cualquier otro centro.

[0048] El medidor de servicios podría también comprender una unidad de control de transmisión encargada de la verificación, por ejemplo, si un mensaje de reconocimiento ha sido debidamente recibido desde el centro de gestión remoto en respuesta a un mensaje de informe.
En el evento positivo, la unidad de control de transmisión entrega una señal positiva, mientras que el evento negativo puede entregar una señal negativa.

[0049] El medidor de servicios podría también comprender un contador de validez para incrementar o deducir un valor de validez y un interruptor para la conmutación del operativo del medidor de servicios a partir de un modo operativo normal (modo estándar) a un modo operativo interrumpido.

[0050] Como la clave secreta Kt del medidor de servicios 10 debe permanecer en secreto y es a priori desconocida desde los centros de gestión de servicios 20 remotos (proveedores de servicios), la presente invención también sugiere la implementación de un método que implica una tercera entidad remota, nombrada como centro de supervisión 30, como se muestra esquemáticamente en las Figuras 6a, 6b y 6c.
El objetivo de este método es administrar una comunicación entre un medidor de servicios 10, usado para la medida de al menos un consumo de servicios y al menos un centro de gestión de servicios remotos 20 encargado del tratamiento de al menos una parte de este consumo de servicios; esta comunicación está supervisada por al menos un centro de supervisión 30, por ejemplo, a través de la misma la red de comunicación 5 como se usa entre el medidor de servicios 10 y el centro de gestión de servicios remotos 20.
Con este fin y como ya se ha mostrado en la Fig. 1, el medidor de servicios comprende:

- una unidad de medida 11 para la medida de al menos un valor de consumo de servicio V,
- una unidad de comunicación 12 para el envío/recepción de mensajes 8 a/de al menos el centro de gestión de servicios remotos 20, teniendo en cuenta que este también puede recibir mensajes desde el centro de supervisión 30 (Fig. 6b),
- una memoria 13 para depositar un identificador único ID pertenece al medidor de servicios 10 y una primera clave K1 requerida para la codificación/descodificación de mensajes 8 que se deben enviar/recibir por la unidad de comunicación 12,
- una unidad de encriptación 14 para el encriptado de dicho valor de consumo de servicios V como un primer criptograma C1, en particular, el primer criptograma C1 resultará de la encriptación del valor de consumo de servicios V por la primera clave K1,
- un generador de mensaje 16 para generar un mensaje de servicio 8 que contiene dicho primer criptograma C1 que tiene que ser enviado al centro de gestión de servicios remotos 20.

[0051] Este método comprende los pasos de:

- solicitud al centro de supervisión 30 por el centro de gestión de servicios remotos 20, la asignación (es decir, la asociación) de este centro de gestión de servicios remotos 20 con un medidor de servicios 10 específicos mediante una solicitud (por ejemplo, un mensaje) que comprende al menos el identificador único ID de dicho medidor de servicios 10; esta solicitud se puede considerar como una solicitud de inscripción enviada por el medidor de servicios por lo menos a un centro de gestión de servicios remotos de su elección; luego el centro de gestión de servicios remotos 20 contacta con el centro de supervisión 30 (por ejemplo, por el envío de la solicitud) en vistas de realización de esta solicitud,
- transmisión por el centro de supervisión 30 de unos denominados datos clave (es decir, datos acerca de una clave) al centro de gestión de servicios remotos 20; dichos datos clave son solicitados para la desencriptación/encriptación de mensajes 8,
- lectura, por el medidor de servicios 10, el valor de consumo de servicios V medido por la unidad de medida 11,
- generación, por el medidor de servicios 10, del mensaje de servicio 8 que incluye el primer criptograma C1,
- envío, por el medidor de servicios 10, del mensaje de servicio 8 al centro de gestión de servicios remotos 20 en vistas de este tratamiento por este centro de gestión de servicios remotos.

[0052] Según una vía posible, el centro de supervisión 30 podría pertenecer al fabricante de los medidores de servicios.
Ventajosamente en este caso, ya sabe los datos personales del medidor de servicios, en particular, el identificador único ID y la clave privada Kt de cada medidor de servicios 10.
Alternativamente, el centro de supervisión puede ser cualquier tercera autoridad que es independiente de cualquier centro de gestión de servicios remotos y que se autoriza para tratar la clave secreta Kt de medidores de servicios.

[0053] Alternativamente, la solicitud enviada al centro de supervisión 30, en vistas de registrar la asociación de un centro de gestión de servicios remotos 20 con un medidor de servicios particular 10, podría realizarse también por el medidor de servicios en vez del centro de gestión de uservicios remotos.
En este caso, esta solicitud debería comprender además el identificador único de este centro de gestión de servicios remotos 20.

[0054] Según una forma de realización, los datos de clave transmitidos por el centro de supervisión 30 al centro de gestión de servicios remotos 20 es la primera clave K1 que ya es almacenada en la memoria 13 del medidor de servicios 10 y que se usa como clave compartida Ks.
Esta forma de realización se representa en la figura 6a.
Ya que todas las entidades 10, 20, 30 tienen la clave compartida Ks, por lo tanto, pueden comunicarse entre sí bajo condiciones seguras.

[0055] La figura 6b muestra una forma de realización alterna donde la primera clave K1, almacenada en la memoria 13, es una clave secreta Kt que pertenece al medidor de servicios 10.
Según esta forma de realización, la clave secreta Kt también se conoce por el centro de supervisión que mantiene esta clave como datos confidenciales debido a su estado de entidad de confianza.
Con este fin, el centro de supervisión dispone de una base de datos fijada que comprende, para cada medidor de

servicios del sistema, un registro que incluye al menos su único identificador ID junto con su clave secreta Kt.
Preferiblemente, cada registro comprende además el identificador único del centro de gestión de servicios remotos y, opcionalmente, la clave compartida actual Ks.
En esta forma de realización, el centro de supervisión 30 y el medidor de servicios 10 comprenden cada uno un módulo criptográfico 17 como se muestra en la Fig. 3.
Así, cada uno es capaz de generar una clave compartida Ks tomando la clave secreta Kt como una primera entrada y un valor de inicialización I0 como una segunda entrada.
Con este fin, el valor de inicialización requerido I0 se genera (por ejemplo, de forma aleatoria) por el centro de supervisión 30 y los datos de clave (mencionados arriba) son la clave compartida Ks proporcionada por el módulo criptográfico 17 del centro de supervisión.
El método comprende además los pasos de:

- generación de la clave compartida Ks por el centro de supervisión 30 usando su módulo criptográfico 17,
- transmisión del valor de inicialización I0, desde el centro de supervisión 30 al medidor de servicios 10, dentro de un mensaje de inicialización,
- carga del valor de inicialización I0 y la clave secreta Kt en el módulo criptográfico del medidor de servicios, para obtener la clave compartida requerida Ks que tiene que ser usada para la encriptación/desencriptación de mensajes, según un esquema de encriptación simétrica, cuando se intercambian comunicaciones entre el medidor de servicios 10 y el centro de gestión de servicios remotos 20.

[0056] Una vez calculada por el medidor de servicios, la clave compartida Ks se puede almacenar en la memoria 13 del medidor de servicios.
Alternativamente, el valor de inicialización I0 se puede almacenar en esta memoria en vez de la clave compartida KS que se puede calcular cada vez unos mensajes deben ser encriptados/desencriptados.

[0057] De esta manera, se evita cualquier divulgación de la clave secreta Kt del medidor de servicios.
Cuando, un nuevo propietario de un medidor de servicios quiere los servicios proporcionados por un centro de gestión de servicios remotos de su elección, el centro de gestión de servicios remotos manda una solicitud de registro al centro de supervisión.
Luego, este centro de supervisión actualizará su base de datos registrando un par nuevo entre el medidor de servicios 10 de este nuevo cliente y este centro de gestión de servicios remotos.

[0058] La ilustración de la figura 6c sugiere una variante de la forma de realización de la figura 6b.
Como se muestra en la Fig. 6c, la etapa de transmisión del valor de inicialización I0 se realiza desde el centro de supervisión 30, a través del centro de gestión de servicios remotos 20 que transmite el mensaje de inicialización al medidor de servicios 10.
El valor de inicialización I0 y la clave compartida Ks se pueden transmitir por el centro de supervisión en dos mensajes separados o en un mensaje único, por ejemplo, como datos clave.

[0059] Según otra forma de realización, el mensaje de inicialización comprende además una firma S, típicamente un valor de hash que puede ser obtenido aplicando una función de hash sobre el mensaje de inicialización.
Esta firma S puede ser realizada, durante un denominado paso de firma, por el centro de supervisión 30 utilizando una unidad de firma.
Como resultado, el método también comprende un paso de autentificación realizado por el medidor de servicios para verificar la autentificación de esta firma S. Este control se puede conseguir por una unidad de autentificación 18 (Fig. 1).
En caso de autentificación exitosa, se permite la carga del valor de inicialización (I0) en su módulo criptográfico.

[0060] En otra forma de realización, el método comprende además un primer paso de validez, que se realiza por el centro de supervisión para añadir un sello de tiempo T (es decir, unos datos de validez) al mensaje de inicialización.
Este sello de tiempo T se define por el centro de supervisión 30 basándose en un tiempo actual CT.
En esta forma de realización, el método comprende un segundo paso de validez que se realiza por el medidor de servicios 10 antes de cargar el valor de inicialización I0 en su módulo criptográfico 17.
El segundo paso de validez pretende controlar la validez del sello de tiempo T, comparándola con el tiempo actual CT.
En caso de validación exitosa, se permite la carga del valor de inicialización I0.

[0061] Por ejemplo, el sello de tiempo T es una fecha de validez, un tiempo de validez o un intervalo de tiempo de validez definido por ejemplo por dos fechas, una fecha de inicio y una fecha final.
Según una primera vía, el centro de supervisión 30 y el medidor de servicios 10 comprenden cada uno un temporizador (por ejemplo un reloj) que produce un tiempo actual CT y el denominado segundo paso de validez pretende verificar que el tiempo actual CT está dentro de un periodo de validez determinado de dichos datos de validez T.
Los dos temporizadores se deben sincronizar en lo posible.
Según una vía alterna, el tiempo actual CT se puede proporcionar por una señal radiofónica controlada única que se puede recibir por cada temporizador.

[0062] En otra forma de realización, el medidor de servicios 10 comprende un generador de clave 16 para generar una clave de carga útil Kp que tiene que usarse por su unidad de encriptación 14 para el encriptado del valor de consumo de servicios V dentro de un mensaje de carga útil 8.
En esta forma de realización, el método comprende además los pasos de:

- generar una clave de carga útil Kp,
- usar esta clave de carga útil Kp para el encriptado del valor de consumo de servicios V como resultado del primer criptograma C1,
- generar un segundo criptograma C2 como resultado de la encriptación de la clave de carga útil Kp por la primera clave K1, usando la unidad de encriptación 14 del medidor de servicios 10,
- incluir el segundo criptograma C2 en un mensaje de servicio 8 antes de enviarlo al centro de gestión 20 de servicios remotos.

Preferiblemente, el segundo criptograma C2 se envía con el primer criptograma C1, sin embargo, en el mismo mensaje, los primeros y segundos criptogramas también se pueden enviar en dos mensajes separados.
Preferiblemente, este segundo criptograma será incluido al menos una vez en tal mensaje, por ejemplo, al menos durante una fase de inicialización donde el medidor de servicios 10 se asigna al centro de gestión 20 de servicios remotos.
Más preferiblemente, este segundo criptograma C2 será periódicamente incluido en el mensaje 8, al menos cada vez que la clave de carga útil Kp se cambie o renueve.

[0063] Según otra forma de realización, la primera clave K1 del presente método es una denominada clave de gestión remota Km que pertenece al centro de gestión de servicios remotos.

[0064] Según una forma de realización de la invención, el medidor de servicios 10 podría ser monitorizado y gestionado por más de un centro de gestión de servicios remotos 20.
Tal situación puede ocurrir si el medidor de servicios pudiera medir diferentes tipos de servicios al mismo tiempo, por ejemplo, monitorizando la potencia eléctrica y consumos de agua simultáneamente.
Por lo tanto, el sistema mostrado en la Fig. 6a, 6b, 6c obviamente no está limitado a un solo medidor de servicios.
Lo mismo se aplica al centro de gestión de servicios remotos 20 e incluso al centro de supervisión 30.
Alternativamente, el medidor de servicios 10 podría ser capaz de funcionar de acuerdo con un planificador temporal, de modo que la provisión de potencia eléctrica, gas o agua podría realizarse por algunas partes de tiempo por un primer centro de gestión de servicios remotos y para otras partes de tiempo por otro proveedor.

[0065] En la descripción mencionada anteriormente, la terminología que se refiere al dispositivo de supervisión de uso de servicios califica bien un medidor de servicios 10, como se ilustra en la figura 1 o un dispositivo de aparato interno que se puede monitorear remotamente y gestionar desde el centro de gestión de servicios remotos 20 (como mostrado en la figura 1) o a partir de un equipo de concentrador colector.
Además, la terminología que se refiere al centro de gestión de servicios remotos se utiliza para calificar bien un centro de gestión de proveedor de servicios central o un nodo de equipo de concentrador colector intermedio en red eléctrica inteligente, donde el centro de gestión de servicios está bajo control estricto del proveedor de servicios, por ejemplo en una cámara o construcción segura.

**REIVINDICACIONES**

1. Medidor de servicios (10) para la medida de al menos un consumo de servicios y para optimizar el tráfico de mensajes intercambiados por una pluralidad de centros de gestión de servicios remotos (20), que comprende:
- una unidad de medida (11) para la medida de al menos un valor de consumo de servicio (V),
- una unidad de comunicación (12) para el envío de mensajes (8) a dichos centros de gestión de servicios remotos (20) asignados al medidor de servicios (10) para el tratamiento de dicho valor de consumo de servicios (V) por dichos centros de gestión de servicios remotos (20),
- una memoria (13) para depositar un identificador único (ID) que pertenece al medidor de servicios (10) y una primera clave (K1) para el encriptado de mensajes (8) que van a ser enviados por la unidad de comunicación (12),
- una unidad de encriptación (14) para el encriptado de dicho valor de consumo de servicios (V) como un primer criptograma (C1),
- un generador de mensaje (15) para generar un mensaje de servicio (8) que contiene dicho primer criptograma (C1) que va a ser enviado a los centros de gestión de servicios (20) remotos,
**caracterizado por el hecho de que** dicha unidad de comunicación (12) es además capaz de recibir mensajes (8) de dichos centros de gestión de servicios remotos (20) y donde dicho medidor de servicios (10) comprende además:
un generador de clave (16) para generar una clave de carga útil (Kp) destinada a ser compartida por dicha pluralidad de centros de gestión de servicios (20) remotos, dicha clave de carga útil (Kp) es usada por dicha unidad de encriptación (14) para el encriptado del valor de consumo de servicios (V), para formar un mensaje de carga útil compartida (8) adecuada para ser enviada a dicha pluralidad de centros de gestión de servicios remotos (20),
y donde la unidad de encriptación (14) es capaz de generar un segundo criptograma (C2), para cada uno de dichos centros de gestión de servicios remotos (20), por el encriptado de dicha clave de carga útil (Kp) con dicha primera clave (K1), dicho segundo criptograma (C2) está destinado a ser incluido, por el generador de mensaje (15), en un mensaje de control (8) para ser enviado a un centro de gestión de servicios remotos dedicado (20).

2. Medidor de servicios, según la reivindicación 1, donde dicha primera clave (K1) es una clave pública de centro de gestión que pertenece a dicho centro de gestión de servicios remotos.

3. Medidor de servicios (10), según la reivindicación 1, donde este comprende una clave secreta (Kt) que pertenece al medidor de servicios (10), un valor de inicialización (I0) recibido dentro de un mensaje de inicialización por la unidad de comunicación (12) y almacenado en la memoria (13), y un módulo criptográfico (17) que integra una función para generar una clave compartida (Ks) tomando dicha clave secreta (Kt) como una primera entrada y dicho valor de inicialización (I0) como una segunda entrada, dicha clave compartida (Ks) se usa como clave simétrica entre el medidor de servicios y uno de dichos centros de gestión de servicios remotos (20), al menos para el encriptado de mensajes (8) en vez de la primera clave (K1).

4. Medidor de servicios (10), según la reivindicación 3, donde este comprende una unidad de desencriptación (14') para la desencriptación de mensajes recibidos por la unidad de comunicación (12).

5. Medidor de servicios (10), según la reivindicación 4, donde dicha memoria (13) almacena además una clave de sesión de inicialización (Ki), dicho mensaje de inicialización se encripta con la clave de sesión de inicialización (Ki) y la unidad de desencriptación (14') es capaz de desencriptar dicho mensaje de inicialización usando la clave de sesión de inicialización (Ki).

6. Medidor de servicios (10), según la reivindicación 4 o 5, donde el mensaje de inicialización comprende una firma (S) para su autentificación, dicho medidor de servicios comprende además una unidad de autentificación (18) para la verificación de la autentificación de la firma (S) y permitir la carga del valor de inicialización (I0) en el módulo criptográfico (17) en caso de autentificación exitosa.

7. Método para administrar una comunicación entre un medidor de servicios (10), usado para la medida de al menos un consumo de servicios y al menos un centro de gestión de servicios remotos (20) a cargo del tratamiento de dicho consumo de servicios, dicha comunicación está supervisada por al menos un centro de supervisión (30), dicho medidor de servicios (10) comprende:
- una unidad de medición (11) para la medida de al menos un valor de consumo de servicios (V),
- una unidad de comunicación (12) para el envío de mensajes (8) a dicho centro de gestión de servicios remotos (20),
- una memoria (13) para depositar un identificador único (ID) que pertenece al medidor de servicios (10) y una primera clave (K1) requerida para la encriptación/desencriptación de mensajes (8) para ser enviados por la unidad de comunicación (12),
- una unidad de encriptación (14) para el encriptado de dicho valor de consumo de servicios (V) como un primer criptograma (C1),
- un generador de mensaje (15) para generar un mensaje de servicio (8) que contiene dicho primer criptograma (C1) para ser enviado al centro de gestión de servicios remotos (20),
dicho método incluye los pasos de:

- lectura por el medidor de servicios (10) del valor de consumo de servicios (V) medido por la unidad de medida (11),
- generación por el medidor de servicios (10) del mensaje de servicio (8) que comprende dicho primer criptograma (C1),
- envío por el medidor de servicios (10) del mensaje de servicio (8) al centro de gestión de servicios remotos (20) con vistas a su tratamiento por este último,

**caracterizado por el hecho de que:**

dicha comunicación se establece entre dicho medidor de servicios (10) y una pluralidad de centros de gestión de servicios remotos (20) encargados del tratamiento de al menos una parte de dicho consumo de servicios, y dicha comunicación se supervisa por al menos un centro de supervisión (30),

dicha unidad de comunicación (12) es además capaz de recibir un mensaje (8) de dichos centros de gestión de servicios remotos (20) y

dicho método comprende además los pasos de:

- para cada uno de dichos centros de gestión de servicios remotos (20), el envío de una solicitud al centro de supervisión (30) preguntando por la asignación de dicho medidor de servicios (10) a dicho centro de gestión de servicios remotos (20), dicha solicitud comprende al menos el identificador único (ID) de dicho medidor de servicios (10),
- transmisión por el centro de supervisión (30) de los datos de clave al centro de gestión de servicios remotos (20); dichos datos de clave son usados como datos de entrada solicitados de una operación criptográfica para la desencriptación/encriptación de dichos mensajes (8).

8. Método, según la reivindicación 7, donde los datos de clave son la primera clave (K1) almacenada en la memoria (13) del medidor de servicios (10) como una clave compartida (Ks).

9. Método, según la reivindicación 7, donde la primera clave (K1) depositada en la memoria (13) del medidor de servicios (10) es una clave secreta (Kt) del medidor de servicios, dicha clave secreta (Kt) se conoce por el centro de supervisión (30) como datos confidenciales, el centro de supervisión (30) y el medidor de servicios (10) comprende cada uno un módulo criptográfico (17) que integra una función para generar una clave compartida (Ks) tomando dicha clave secreta (Kt) como una primera entrada y un valor de inicialización (I0) generado por el centro de supervisión (30) como una segunda entrada, el dato de clave es la clave compartida (Ks) proporcionada por el módulo criptográfico (17) del centro de supervisión (30), el método comprende además los pasos de:

- generación de la clave compartida (Ks) por el centro de supervisión (30) usando su módulo criptográfico (17),
- transmisión de dicho valor de inicialización (I0), desde el centro de supervisión (30) al medidor de servicios (10), dentro de un mensaje de inicialización,
- carga del valor de inicialización (I0) y la clave secreta (Kt) en el módulo criptográfico (17) del medidor de servicios (10) para obtener dicha clave compartida (Ks) para ser usada para la encriptación/desencriptación de mensajes (8), según un esquema de encriptación simétrica.

10. Método, según la reivindicación 9, donde la etapa de transmisión de dicho valor de inicialización (I0) se realiza a través de dicha gestión de servicios remotos (20) que transmite el mensaje de inicialización al medidor de servicios (10) después de haberlo recibido del centro de supervisión (30).

11. Método, según la reivindicación 9 o 10, donde este comprende:

- un paso de firma realizado por el centro de supervisión (30) para generar una firma (S) por una unidad de firma y añadir esta firma (S) en el mensaje de inicialización para su autentificación,
- un paso de autentificación realizado por el medidor de servicios (10) para verificar la autentificación de dicha firma (S) mediante una unidad de autentificación (18) y permitir la carga del valor de inicialización (I0) en su módulo criptográfico (17) en caso de autentificación exitosa.

12. Método, según cualquiera de las reivindicaciones 9 a 11, donde comprende además:

- un primer paso de validez realizado por el centro de supervisión (30) para añadir un sello de tiempo (T) al mensaje de inicialización, dicho sello de tiempo (T) está definido por el centro de supervisión (30) basándose en un tiempo actual (CT) y,
- un segundo paso de validez realizado por el medidor de servicios (10), antes de cargar el valor de inicialización (I0) en su módulo criptográfico (17), para controlar la validez del sello de tiempo (T) comparando el sello de tiempo (T) con el tiempo actual (CT) y permitiendo esta carga en caso de validación exitosa.

13. Método, según la reivindicación 12, donde dicho sello de tiempo (CT) se proporciona por una señal controlada radiofónica.

14. Método, según cualquiera de las reivindicaciones 7 a 13, donde el medidor de servicios (10) comprende un generador de clave (16) para generar una clave de carga útil (Kp) para ser usada por su unidad de encriptación (14) para el encriptado del valor de consumo de servicios (V), dicho método comprende además los pasos de:

- generación de una clave de carga útil (Kp),
- utilización de dicha clave de carga útil (Kp) para el encriptado del valor de consumo de servicios (V) como resultado del primer criptograma (C1),

- generación de un segundo criptograma (C2) como resultado de la encriptación de dicha clave de carga útil (Kp) por la primera clave (K1) usando la unidad de encriptación (14) del medidor de servicios (10),
- incluisión del segundo criptograma (C2) en el mensaje de servicio (8) antes de enviarlo al centro de gestión de servicios remotos (20).

15. Método, según cualquiera de las reivindicaciones 7 a 14, donde dicha primera clave (K1) es una clave de gestión remota (Km) que pertenece al centro de gestión de servicios remotos (20).

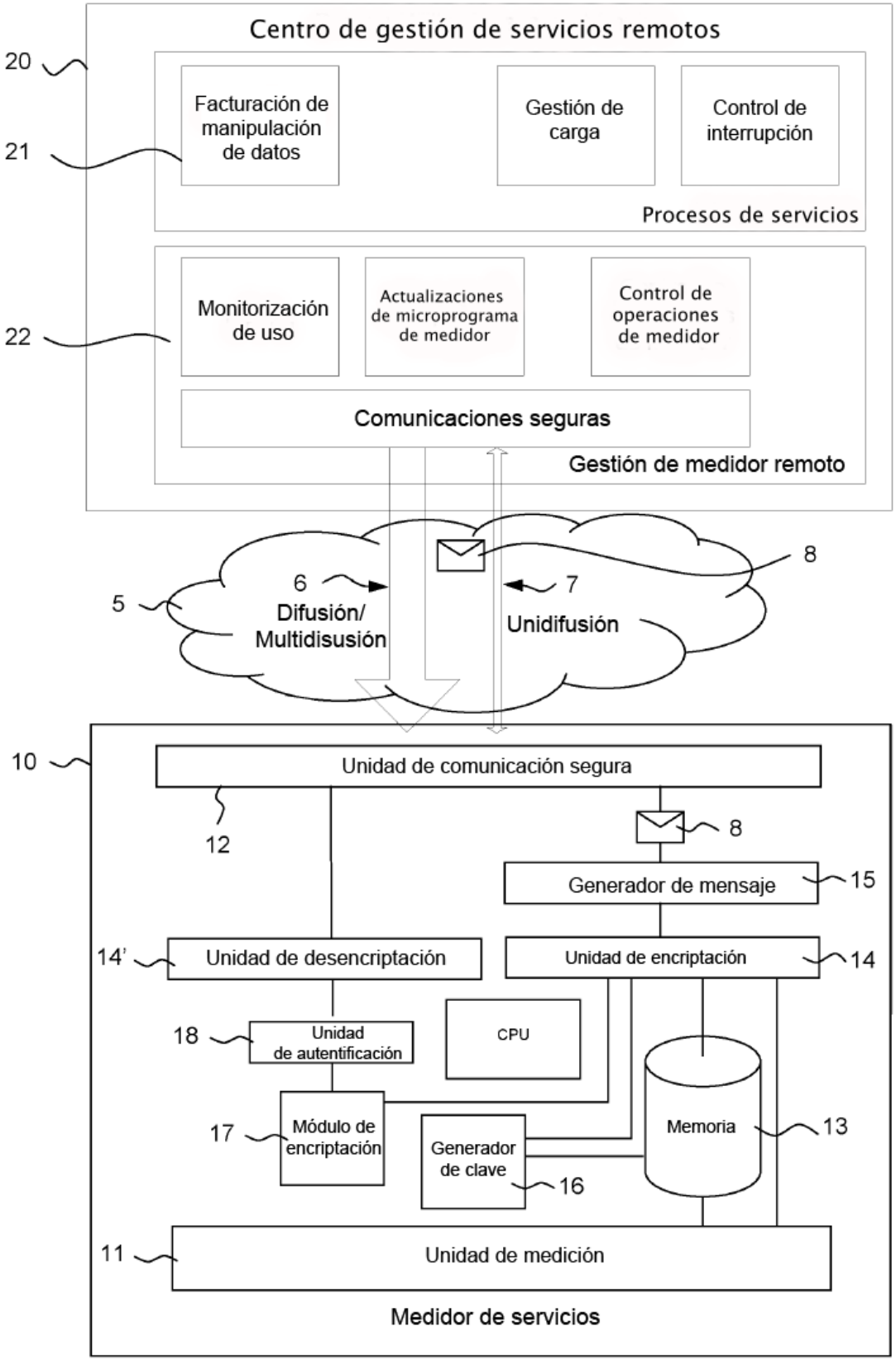
Centro de gestión de servicios remotos
20
21
Facturación de manipulación de datos
Gestión de carga
Control de interrupción
Procesos de servicios
22
Monitorización de uso
Actualizaciones de microprograma de medidor
Control de operaciones de medidor
Comunicaciones seguras
Gestión de medidor remoto
5
6
Difusión/ Multidisusión
7
Unidifusión
8
10
Unidad de comunicación segura
12
8
Generador de mensaje
15
14'
Unidad de desencriptación
Unidad de encriptación
14
18
Unidad de autentificación
CPU
17
Módulo de encriptación
Generador de clave
16
Memoria
13
11
Unidad de medición
Medidor de servicios

**Fig. 1**

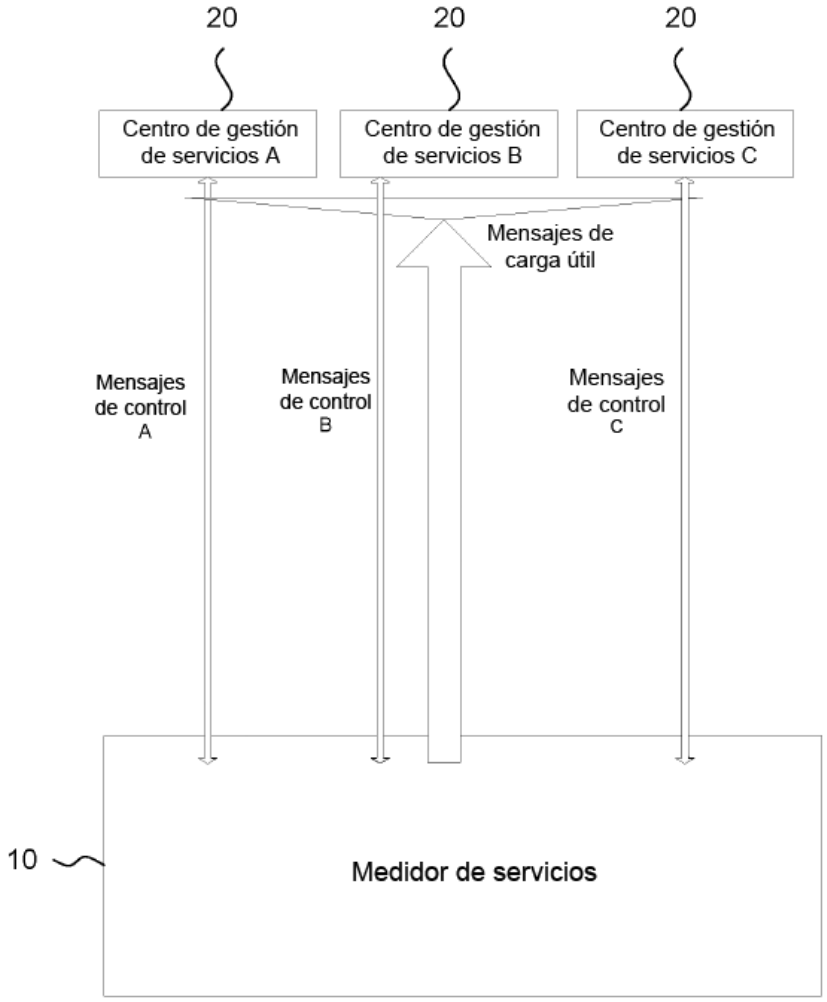
20
20
20
Centro de gestión de servicios A
Centro de gestión de servicios B
Centro de gestión de servicios C
Mensajes de carga útil
Mensajes de control A
Mensajes de control B
Mensajes de control C
10
Medidor de servicios

**Fig. 2**

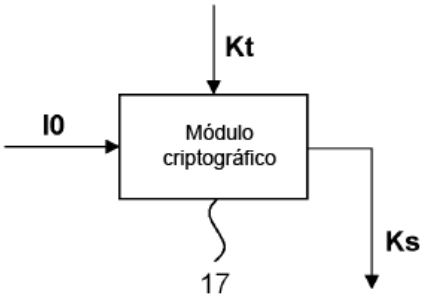
Kt
I0
Módulo criptográfico
Ks
17

**Fig. 3**

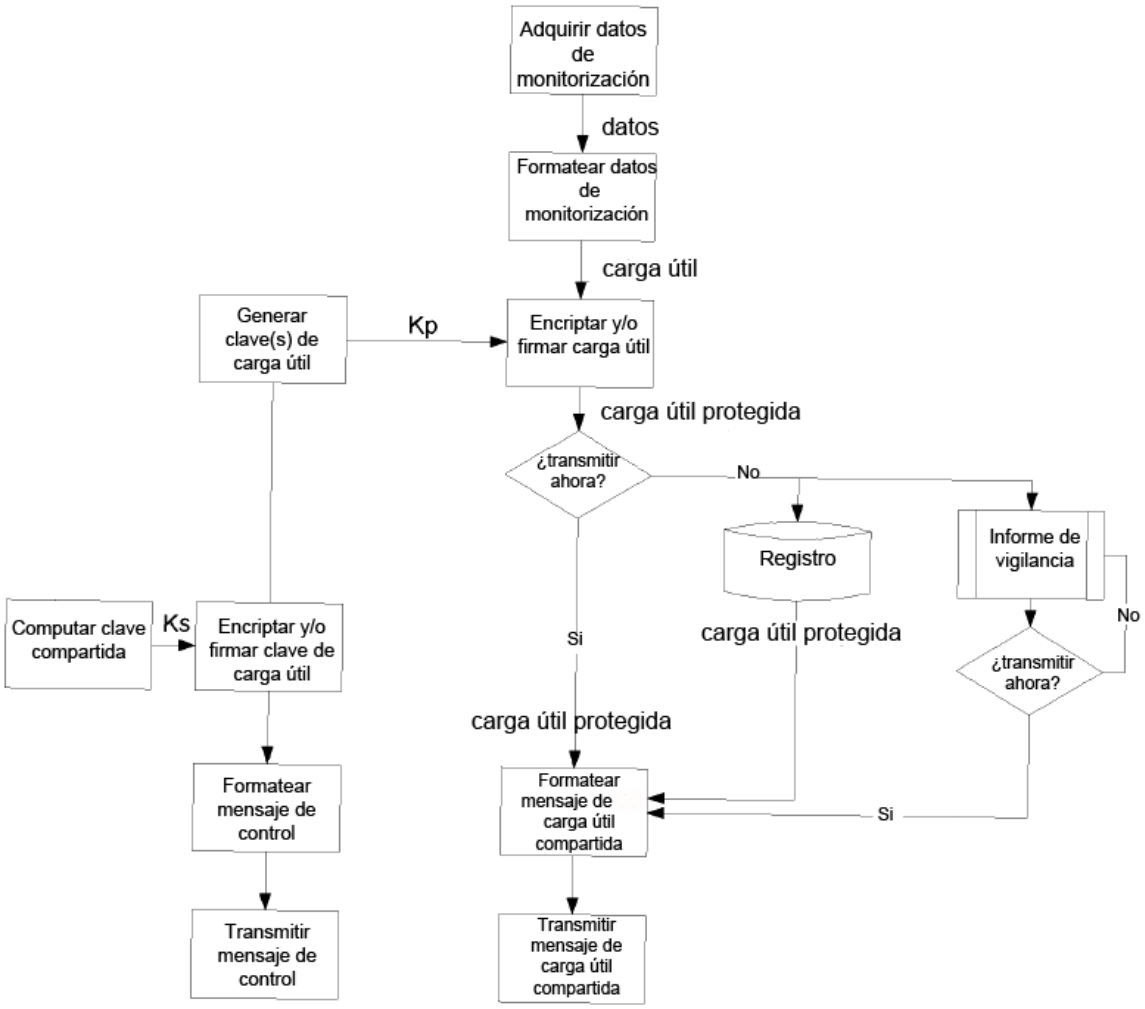
Adquirir datos de monitorización
datos
Formatear datos de monitorización
carga útil
Generar clave(s) de carga útil
Kp
Encriptar y/o firmar carga útil
carga útil protegida
¿transmitir ahora?
No
Registro
Informe de vigilancia
No
Computar clave compartida
Ks
Encriptar y/o firmar clave de carga útil
Si
carga útil protegida
¿transmitir ahora?
carga útil protegida
Formatear mensaje de control
Formatear mensaje de carga útil compartida
Si
Transmitir mensaje de control
Transmitir mensaje de carga útil compartida

**Fig. 4**

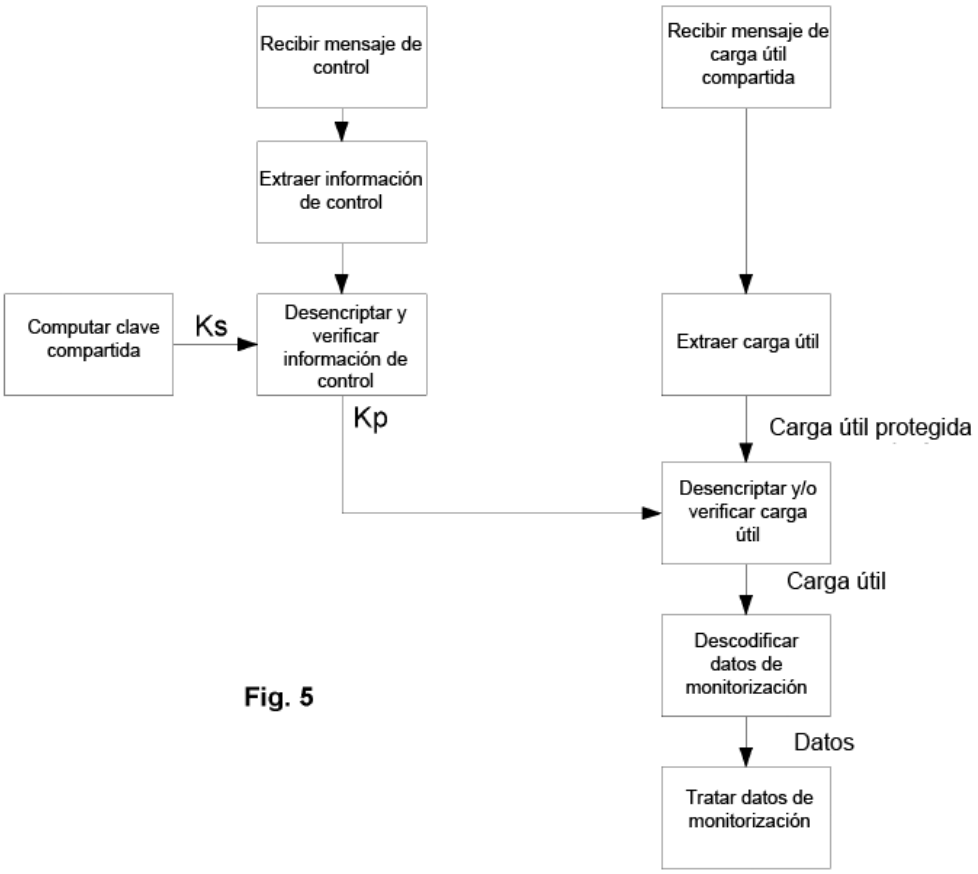


Fig. 5

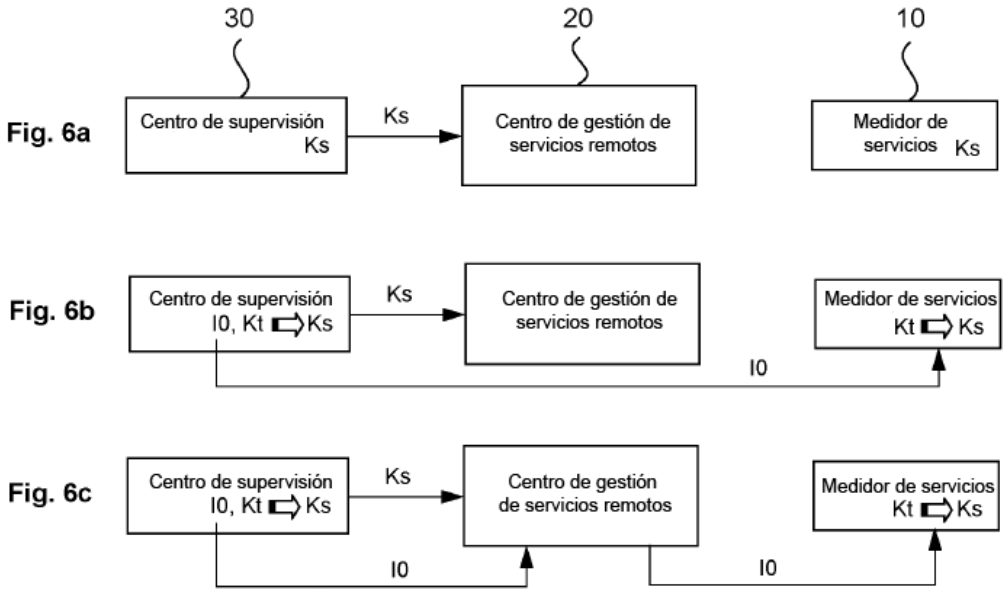


Fig. 6a

Fig. 6b

Fig. 6c