(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 545 356**

(51) Int. CI.:

H04Q 9/00 (2006.01)
G01D 4/00 (2006.01)
H04L 9/00 (2006.01)
G06Q 50/06 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.12.2011 E 11793789 (6)**

(97) Fecha y número de publicación de la concesión europea: **17.06.2015 EP 2656631**

(54) Título: **Módulo de control de medición segura de servicios públicos**

(30) Prioridad:

22.12.2010 US 201061425830 P
18.04.2011 EP 11162894

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.09.2015

(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;
CONUS, JOËL y
WENGER, JOEL

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Módulo de control de medición segura de servicios públicos

Campo de la invención

[0001] Esta invención se refiere al campo de la aseguración del uso de servicios públicos contra varias amenazas de hacking mediante programas adicionales de medidores de lectura.

Fondo técnico

[0002] La desregulación en curso en los mercados de distribución de energía a nivel mundial está impulsando la necesidad de cuadros de distribución de servicios inteligentes y contadores inteligentes, permitiendo a ambos proveedores de servicios y consumidores controlar el consumo detallado de un usuario final en cualquier momento a través de redes de comunicación abiertas. El mercado de la energía está particularmente afectado hoy en día pero las salidas relacionadas son también pertinentes para otros mercados de servicios públicos tales como agua o gas.

[0003] Mientras varios contadores existentes ya implementan algunos protocolos de lectura automatizada punto a punto utilizando por ejemplo óptico estándar o interfaces de módem, no son capaces de interactuar con los dispositivos de red de área de hogar del usuario final o el uso de instalaciones remotas de control de servicios públicos usando redes de comunicación inalámbricas o por tendido eléctrico. La respuesta de la industria para este requisito regulador en la siguiente década consistirá por lo tanto en sustituir los contadores existentes por los denominados contadores inteligentes, lo que aumenta costes formidables para los vendedores de servicios públicos y los consumidores al fin y al cabo.

[0004] Además, la dependencia resultante de la funcionalidad de medida básica en los mensajes de comunicación remota alza intereses significativos en la robustez eficaz en defectos de software al igual que amenazas emergentes tales como gusanos de red inteligentes y virus aprovechándose de defectos de diseño de seguridad del contador inteligente que pueden no conocerse en el momento de su uso, pero pueden volverse críticos más tarde. Esto es particularmente evidente en el caso de la característica remota de desconexión, como objetivos serios para el ciber-terrorismo pero también un posible punto de entrada para ladrones locales como una vía para desconectar algunas alarmas de hogar de su fuente de energía.

[0005] En la práctica, los diseños de seguridad de hoy en día para cuadros inteligentes y contadores inteligentes están en gran medida inspirados por la industria de la telecomunicación y una gran parte de estos están sujetos a una emergente estandarización por comités internacionales tales como ANSI o IEC. No obstante los requisitos son muy diferentes, puesto que dispositivos finales de telecomunicación tales como teléfonos móviles, decodificadores o incluso receptores de televisión raramente exceden una vida operativa de 10 a 20 años. En cambio, el equipamiento de medición es típicamente instalado en el momento de construcción de una casa y destinado a durar al menos 20 años, si no 50 a 100 años.

[0006] Una vez que las especificaciones estándar son definidas, ya no es posible actualizar el diseño (por ejemplo, algoritmos criptográficos, longitudes de clave y sistemas de gestión de clave) sin romper el acuerdo, que es un tema importante en mercados desregulados donde cualquier modelo del dispositivo de medición de cualquier fabricante necesita operar con cualquier infraestructura proveedora de servicios y esto posiblemente para los siguientes 50 a 100 años.

[0007] Hay por lo tanto una necesidad de soluciones alternativas para separar claramente la funcionalidad avanzada pero compleja y la funcionalidad de control sensible de seguridad de la entrega de servicios básica pero probada y funcionalidad de medición de consumo. En este método, los contadores existentes completamente operativos no necesitan ser mejorados, lo que también ayuda al ahorro de costes de mejora y energía de fabricación de contadores inteligentes.

[0008] La separación de la funcionalidad de control remoto de la funcionalidad de medida ligada básica requiere típicamente un dispositivo de control separable, incluyendo al menos:

- una interfaz de lectura por sensor para ser conectado a la pantalla del contador existente o interfaz de lectura eléctrica (en serie, óptica etc).
- una memoria para el almacenamiento de información de uso de servicios antes de informar sobre esta.
- una o más interfaces de comunicación de red para informar de los datos tanto a la red de servicios y/o a la red de área de hogar del usuario final, conforme a reglamentos existentes y estándares técnicos pertinentes.
- un procesador a cargo del control de la lectura, almacenamiento y reporte de operaciones.

[0009] Tales soluciones de control separables y sistemas de gestión de datos asociados ya han sido descritos, por ejemplo en WO07134397 o GB 2460517. Algunos dispositivos relacionados son también ahora comercializados por ejemplo por PilotSystems (http://www.pilotsystems.com) y Xemtec (http://www.xemtec.ch), pero ninguno con este estado de la técnica se dirige a la funcionalidad de ejecución de seguridad.

[0010] Para abordar completamente la amenaza de hacking de consumo de uso de servicios públicos, es importante prevenir el hacking en todos los componentes individuales en la cadena de comunicación de extremo a extremo. A diferencia de los contadores inteligentes, los contadores existentes LM como el primer componente en la cadena de comunicación de extremo a extremo no tienen interfaces para abrir redes, por lo tanto su hacking requiere una operación mecánica local con cierta preocupación por la seguridad y evidencia de alteración, ya que los contadores están típicamente sellados por los vendedores de servicios públicos en todas partes del mundo. En el otro extremo de la cadena, el estado del diseño criptográfico de la técnica se aplica para comunicaciones entre el módulo de control y la infraestructura de servicios públicos sobre redes abiertas, pero esta seguridad es tan segura como la clandestinidad de claves subyacentes. Un diseño a prueba de manipulaciones en el lado del dispositivo de módulo de control es por lo tanto de importancia fundamental.

Resumen de la invención

[0011] El objetivo de la invención es por lo tanto eliminar los inconvenientes de la técnica anterior y proporcionar un dispositivo de control seguro de servicios públicos separable para ser anexado a un equipo de medida de servicios para controlar al menos un consumo de uso de servicios.

[0012] Esto se consigue gracias a un dispositivo de control de medición separable para ser conectado con un contador de servicios para controlar al menos un consumo de servicios medido por dicho contador de servicios, comprendiendo:

- una interfaz de lectura de uso para adquirir un valor de consumo de servicios públicos medido por dicho contador de servicios,

- una primera memoria segura para almacenar al menos un identificador único ID y una clave personal, ambos pertenecientes a dicho dispositivo,

- un procesador cripto para generar un criptograma de datos informativos que comprenda al menos el valor de consumo de servicios, dicho criptograma siendo encriptado con dicha clave personal,

- un generador de mensajes para generar un mensaje informativo que incluya al menos dicho criptograma y el identificador único ID,

- una unidad de envío para mandar el mensaje informativo a un centro de gestión remoto.

[0013] El equipo contador de servicios permanentemente (o periódicamente) mide el consumo de uso de servicios mientras el dispositivo de control de medida separable lee el consumo de uso de servicios de dicho equipo sobre una base regular con una interfaz de lectura de uso o cualquier medio para adquirir al menos un consumo de servicios medido por el equipo contador de servicios. El dispositivo de control de medición separable puede almacenar el consumo de servicios y es capaz de informar a una infraestructura de control de uso de servicios a través de una interfaz de comunicación, en particular a un centro de gestión remoto mediante una unidad de envío. El dispositivo de control de medición separable está por lo tanto provisto de una primera memoria segura para almacenar al menos un identificador único ID y una clave personal; este identificador único y esta clave privada pertenecientes a este dispositivo. El dispositivo de control de medición separable dispone de un procesador cripto para generar un criptograma a partir de datos informativos que comprende al menos el valor de consumo de servicios; estando este criptograma encriptado con la clave personal del dispositivo de control de medición separable. Este dispositivo también comprende un generador de mensajes o cualquiera de los otros medios para generar un mensaje informativo incluyendo al menos el criptograma y el identificador único ID. Este mensaje informativo se puede enviar al centro de gestión remoto usando la unidad de envío de la interfaz de comunicación.

[0014] El dispositivo podría además comprender un módulo de seguridad encargado de manipular los datos sensibles a la seguridad, tratamiento de seguridad y mensajería de seguridad asociada a dicho informe de dicha infraestructura de control de uso de servicios.

[0015] Otras formas de realización de la presente invención se describen en la siguiente descripción detallada.

Breve descripción de los dibujos

[0016]

La Figura 1 muestra un contador existente LM y un dispositivo de control separable DM que puede ser anexado al

contador existente.

La Figura 2 muestra el contador existente LM de Fig. 1 extendido con el dispositivo de control separable DM operacionalmente conectado a la pantalla de medida de uso DISP del contador existente.

La Figura 3 muestra el contador existente LM de Fig. 1 extendido con el dispositivo de control separable DM operacionalmente conectado al conector de lectura eléctrica de medida de uso opcional RD del contador existente.

La Figura 4 muestra un dispositivo de control separable DM con sus componentes principales e interfaces.

La Figura 5 muestra el dispositivo de control separable DM de Fig. 4 que incluye un procesador cripto en conexión con una memoria segura SMEM.

La Figura 6 muestra un dispositivo de control separable DM operacionalmente conectado a un contador existente LM, donde el dispositivo de control separable DM incluye además una interfaz de módulo de seguridad SM.

La Figura 7 muestra el dispositivo de control separable DM de Fig. 4 junto con un módulo de seguridad SM conectado a través de unas interfaces dedicadas SEC.

Descripción detallada

[0017] En referencia a Fig. 1, un dispositivo seguro de control de servicios separable DM se muestra como conectado de una manera separable a un contador existente LM, también referido como contador de servicios, para controlar el consumo de uso de servicios públicos, tales como el consumo de energía eléctrica, agua o gas. El contador existente ilustrado implementa la pantalla DISP de uso convencional de medición al igual que un conector de lectura eléctrica de medida de uso opcional RD. El contador existente o el equipo contador de servicios permanentemente mide al menos el consumo de uso de un servicio mientras el dispositivo de control de medición separable DM lee este consumo de uso del servicio, sobre una base regular. Con este fin y según una forma de realización, el contador existente LM se puede extender con un dispositivo de control separable DM conectado de forma operacional a la pantalla de uso de medición como se muestra en Fig. 2. El dispositivo de control separable ilustrado aquí incluye una interfaz de lectura OCR y comunica la pantalla del contador existente sobre su propia pantalla para permitir además la lectura manual del valor de medida.

[0018] Alternativamente y como se muestra en Fig. 3, el contador existente LM se puede extender con un dispositivo de control separable DM conectado de forma operacional al conector de lectura eléctrica de medida de uso opcional RD. El dispositivo de control separable ilustrado aquí cumple con el estándar industrial pertinente de comunicación de medición de uso tal como IEC1107 o IEC61107, FLAG, ANSI C12.18 para puertos ópticos o ANSI C12.21 para puertos de módem.

[0019] El dispositivo de control separable DM mostrado en la Fig. 4 comprende una interfaz de lectura de uso READ para adquirir un valor de consumo de servicios medido por el contador existente LM conforme a cualquier forma descrita anteriormente, un búfer de memoria de uso MEM para almacenar al menos temporalmente valores de consumo de servicios leídos por la interfaz de lectura de uso READ, una interfaz de control de servicios remota GRID para reportar al menos estos valores de consumo de servicios a un centro de gestión remoto, una interfaz de red de área de hogar opcional HAN para conectar opcionalmente un dispositivo HAN que procese al menos una parte de la lectura de datos por la interfaz de lectura, una pantalla visual opcional DISP y un procesador central CTRL encargado del control los componentes anteriores.

[0020] En referencia a Fig. 5, el último muestra el dispositivo de control separable DM de Fig. 4 que comprende además un procesador cripto CRYPTO que provee funcionalidades criptográficas sostenido por el procesador central CTRL. El procesador cripto CRYPTO puede generar un criptograma de datos informativos que comprende al menos el valor de consumo de servicios. Según la forma de realización preferida, este criptograma es encriptado con una clave personal del dispositivo de control de medición separable DM. Debido al procesador cripto, el valor de consumo de servicios leído por la interfaz de lectura de uso READ puede introducirse en una función criptográfica para obtener unos datos encriptados que no sean legibles sin saber información secreta. Por esta razón, el procesador cripto está en relación con una memoria segura SMEM para almacenar información sensible tales como claves criptográficas secretas y un identificador único ID perteneciente al dispositivo de control de medición separable DM (o al contador de servicios LM). El procesador cripto implementa varios algoritmos criptográficos tales como por ejemplo, pero no limitados a, AES, NXT, RSA, SHA-256, ECC, etc. El procesador cripto es también el componente único capaz de interactuar con la memoria segura tanto en lectura como escritura. El dispositivo de control separable DM también comprende un generador de mensaje MGEN para generar mensajes informativos que deben ser enviados al centro de gestión remoto mediante la interfaz de red de comunicación GRID. Estos mensajes enviados comprenden, en particular, mensajes informativos que incluyen al menos el criptograma y el identificador único ID anteriormente mencionado.

[0021] El búfer de memoria de uso MEM es capaz de almacenar los valores de consumo de servicios para reportar

éstos a una infraestructura de control de uso de servicios (como a un centro de gestión remoto) a través de una interfaz de comunicación.

[0022] Los datos informativos usados como entrada para generar el criptograma pueden comprender además unos datos complementarios predefinidos, por ejemplo una constante. Los datos informativos pueden comprender además el identificador único ID del dispositivo de control de medición separable. Los mensajes informativos enviados por este dispositivo pueden comprender además cualquier información acerca de este dispositivo, por ejemplo su estado o información acerca de la versión de este dispositivo, en particular la versión de su firmware. Podría ser también posible enviar información acerca del consumo de servicios, por ejemplo en vista a recopilar datos estadísticos o para cualquier otro propósito.

[0023] El criptograma mencionado arriba podría ser un resultado de la función hash (o una función XOR) en los datos informativos. En este caso, el mensaje informativo incluye además el valor de consumo de servicios.

[0024] La clave personal perteneciente al dispositivo de la presente invención puede ser además una clave asimétrica en un esquema de encriptación público/privado, teniendo el centro de gestión remoto la clave asimétrica correspondiente. Por tanto, la clave privada y la clave pública forman juntas un par de claves que se usan para encriptar y desencriptar los mensajes intercambiados.

[0025] El dispositivo de control separable DM es anexo al contador existente mostrado en la figura 1 mediante una interfaz de medición, en particular la interfaz de lectura de uso READ que puede coger varias formas para adaptarse a la tecnología del contador: lectura OCR para contadores existentes más antiguos, óptico estándar o lectura de interfaz de módem para medidores existentes más recientes, y comunicaciones inalámbricas o por tendido eléctrico basadas en estándares de medida inteligentes para permitir la renovación de la seguridad de contadores inteligentes futuros. El dispositivo de control puede implementar cualquiera, un subconjunto o todas las interfaces últimas posibles como dictado por factores de coste, cuestiones de implementación (por ejemplo vida de la batería) y necesidades de mercado.

[0026] Para mantener contadores existentes viejos sin interfaz de lectura eléctrica solo se puede leer visualmente, el dispositivo de control separable DM de Figura 2 se conecta a la pantalla del contador existente LM y los medios para adquirir el valor de consumo de servicios del dispositivo de control comprende una interfaz de lectura OCR para leer este consumo de servicios. El dispositivo también informa a la pantalla del contador existente sobre su propia pantalla para permitir además la lectura manual del valor de medida.

[0027] Alternativamente, en el contador existente LM más reciente de Figura 3 el dispositivo de control separable DM puede ser conectado de forma operacional al conector de lectura eléctrica de medida de uso RD. Por tanto, medios para adquirir el valor de consumo de servicios, tal como la interfaz de lectura de uso READ en el dispositivo de la presente invención, podría comprender una conexión eléctrica proporcionada por el contador de servicios para transmitir el valor de consumo de servicios públicos.

[0028] El dispositivo de control separable DM se fija al contador existente por cualquier medio con elementos fijadores mecánicos como tornillos, o elementos fijadores químicos como pegamento, o imanes. Además, es deseable que el dispositivo de control separable DM sea posteriormente unido al contador existente mediante un sello para fines de sellado de garantía, de modo que solo personal autorizado puede conectar/desconectar el dispositivo de control separable DM a/del contador existente LM.

[0029] Tanto el procesador cripto CRYPTO como la memoria segura SMEM deben estar hechos a prueba de manipulación contra varios tipos de ataque. Con este fin, el procesador cripto y la memoria segura se pueden implementar como un circuito de silicio destinado o integrado en el hardware del dispositivo de control bajo cuidadoso aislamiento de las instalaciones de procesamiento principal y comunicación como se muestra en Fig. 5. El procesador cripto puede incluir bloques de lógica de criptografía adaptada. También es posible emular la funcionalidad del módulo de seguridad SM en un componente de software aislado mediante ofuscación y tecnologías de seguridad de software de criptografía de caja blanca.

[0030] Para facilitar el procesador cripto y la implementación de memoria segura, la segmentación de diseño de seguridad y personalización de acuerdo con prácticas y procesos industriales del estado de la técnica, en otra forma de realización, la funcionalidad de seguridad correspondiente está físicamente aislada por la implementación de esta en un módulo de seguridad separado.

[0031] En una forma de realización mostrada en Fig. 6, el contador existente LM se extiende con un dispositivo de control separable DM conectado a este de forma operacional y el dispositivo de control separable DM incluye además una interfaz de módulo de seguridad SM adecuado por ejemplo para albergar una tarjeta inteligente, posiblemente en el factor de forma de la tarjeta SIM.

[0032] De acuerdo con otra forma de realización, Fig. 7 muestra un dispositivo de control separable DM, similar al de Fig. 4, donde el procesador central CTRL también interactúa con un módulo de seguridad SM aunque una interfaz

dedicada SEC. El módulo de seguridad SM implementa la funcionalidad del procesador cripto CRYPTO en relación con la memoria segura SMEM para memorizar información sensible tales como claves criptográficas secretas al menos.

[0033] Más allá de su diseño de seguridad y ventajas de fabricación, este módulo de seguridad separado permite separar la renovación de seguridad de la lectura y reportar la funcionalidad de control y la renovación del dispositivo de comunicación. Como una tarjeta inteligente o factor de forma de tarjeta SIM es lo suficientemente fina como para ser transmitida al usuario final por correo ordinario al mismo coste de una simple carta, y el módulo de seguridad puede ser renovado por el usuario final sin intervención alguna en el contador mismo, es decir sin preocupaciones de seguridad , y además sin requerir intervención in situ del personal de servicio para abrir y renovar el dispositivo de control separable en caso de que este esté sellado.

[0034] Además, para los mercados de servicios públicos que requieren un soporte de modelo de negocio de prepago, el dispositivo de control separable DM puede incorporar una funcionalidad de control de prepago conectada a intervalos regulares al sistema de autorización de abonado de servidor de servicio remoto a través del procesador central CTRL y la interfaz de red de comunicación GRID o una interfaz SEC basada en contacto estándar o sin contacto a una tarjeta inteligente de prepago SM, en varios factores de forma posible tales como, pero no limitado a, ISO7816, SIM, SD, µSD, MMC.

[0035] En otra forma de realización, el módulo de seguridad se puede combinar con una interfaz de red de área interna HAN para, leer, grabar y reportar de forma segura los datos de otros dispositivos HAN a otro Sistema de Manipulación de Datos de Medidor. Esta interfaz es preferiblemente de naturaleza de consumo inalámbrico y de baja potencia tal como Zigbee.

[0036] En otra forma de realización, para administrar datos varios y consultas de control con modelos de negocio de medida posiblemente compleja de forma segura mientras se apoya la optimización de mensajería de difusión, el módulo de seguridad implementa preferiblemente una base de datos relacional.

[0037] En otra forma de realización, para asegurar el mantenimiento de seguridad y renovación con el paso del tiempo, el dispositivo de control separable DM implementa un mecanismo de ataque seguro para su procesador de controlador CTRL bajo un estrecho control por el módulo de seguridad SM. En ausencia o malfuncionamiento del módulo de seguridad SM, la funcionalidad de comunicación nula o limitada es soportada de modo que se origina una alarma en el lado de la infraestructura del servicio.

[0038] Otra ventaja del dispositivo de la presente invención es proporcionar una gestión mejorada del consumo ya que permite la gestión de más de un contador activado según un horario temporal o por recepción de mensajes de comando.

[0039] Otra ventaja del dispositivo de medición separable de la presente invención es proporcionar gestión mejorada del consumo que permite diferenciar el consumo del servicio medido bajo tarifas diferentes y totalizar cada uno de estos consumos del servicio. Este fin se puede alcanzar por ejemplo usando una pluralidad de contadores de tarifas, cada uno de éstos siendo usado para medir el consumo del servicio bajo una tarifa predeterminada. El dispositivo puede tener estados diferentes (por ejemplo un estado o modo de ejecución normal, un estado de ejecución mínimo, un estado de ejecución interrumpido, etc ...) que puede corresponder a la pluralidad de tarifas aplicables. La asignación de una tarifa predeterminada por una unidad de selección SELECT puede depender de un planificador temporal, de la recepción de un mensaje de comando del centro de gestión remoto o puede ser una acción resultante de una conmutación del modo operativo del dispositivo de medición separable.

[0040] Según una forma de realización preferida, el dispositivo de medición separable DM comprende una memoria actualizada a la última para almacenar el valor de consumo de servicios mientras al menos una memoria de una tarifa es actualizada. La unidad de selección SELECT o cualquier medio de selección se usa para definir el uso de una tarifa actual predeterminada entre tarifas predeterminadas diferentes. Esta unidad de selección puede cambiarse de una tarifa predeterminada a otra. Con este fin, el dispositivo de control de medición separable DM comprende una pluralidad de memorias de tarifas TMEM para almacenar el consumo de servicios según diferentes estados del dispositivo DM, donde se asigna una tarifa predeterminada a cada estado. En particular, este dispositivo comprende al menos dos memorias de tarifas para memorizar sumas (es decir valores acumulados) de consumo del servicio medido bajo estas tarifas predeterminadas diferentes; siendo asignada cada memoria de tarifa para contar el consumo de servicios bajo una tarifa predeterminada. Finalmente, este dispositivo comprende unos calculadores de consumo CALC o cualquier medio en primer lugar para calcular un valor de consumo actual de la última memoria actualizada y el valor de consumo del servicio adquirido leído por la interfaz de lectura de uso READ. Con este fin, el calculador de consumo CALC substrae el valor de consumo del servicio almacenado en la última memoria actualizada del valor de consumo del servicio adquirido. Luego, una unidad de actualización de memoria UPMEM actualiza el valor almacenado en la memoria de las tarifas TMEM que corresponde con la tarifa actual predeterminada (es decir seleccionando la unidad de selección SELECT) añadiendo este valor de consumo actual. Luego, la unidad de actualización de memoria UPMEM recarga la última memoria actualizada con el valor medido durante dicho paso de adquisición. Preferiblemente, la unidad de actualización de memoria UPMEM comprende una

unidad de procesamiento para leer la memoria de la tarifa seleccionada, para añadir el valor de consumo actual a la memoria de la tarifa seleccionada y escribir dicha suma en la memoria de la tarifa seleccionada.

[0041] Los valores almacenados en las memorias de las tarifas correspondientes TMEM relacionadas con el consumo realizado bajo tarifas predeterminadas pueden ser parte de los datos informativos usados para generar el criptograma incluido en el mensaje informativo enviado al centro de gestión remoto.

[0042] Según otra forma de realización, el dispositivo DM de la presente invención, en particular la interfaz de red de comunicación GRID, comprende además una unidad de recepción RECEIV o cualquier medio para recibir al menos un mensaje enviado por el centro de gestión remoto y una unidad de autenticación AUTH o cualquier medio para autenticar este mensaje usando la clave personal de este dispositivo DM. En caso de autentificación exitosa, estos medios pueden ser capaces de ejecutar órdenes incluidas en este mensaje. Si la autentificación fallara, el mensaje podría ser meramente ignorado u otra acción podría desencadenarse. Por ejemplo, el mensaje recibido por la unidad de recepción RECEIV del dispositivo DM del centro de gestión podría ser un mensaje de comando pidiendo medios para definir el uso de la tarifa actual predeterminada para usar una tarifa más alta que la actual, por ejemplo la tarifa máxima disponible. Alternativamente, el mensaje de comando podría pedir medios para definir el uso de la tarifa actual predeterminada para cambiar las tarifas conforme a un horario temporal. Tal horario temporal podría ser almacenado, por ejemplo, en la primera memoria segura del dispositivo de control de medición separable y podrían ser actualizadas a través de un mensaje enviado por el centro de gestión.

[0043] Según otra forma de realización, el dispositivo de la presente invención comprende además un contador de validez VCOUNT o cualquier medio para incrementar/disminuir un valor de validez según el consumo del servicio o un tiempo (por ejemplo duración), una unidad de restablecimiento RESET o cualquier medio para actualizar o sustituir el valor del contador de validez por un valor de validez nuevo, y un interruptor SWIT o cualquier medio para cambiar el funcionamiento del dispositivo DM de un modo operativo normal a un modo operativo interrumpido, dependiendo de si el valor del contador de validez alcanza al menos un valor de umbral predeterminado.

[0044] El modo operativo interrumpido podría forzar medios para definir el uso de una tarifa actual predeterminada para usar una tarifa superior a la tarifa actual predeterminada, por ejemplo la tarifa máxima .

[0045] El contador de validez VCOUNT podría ser un contador temporal o un contador de control de impulsos, incrementado según un reloj interno. En otra forma de realización, el contador de validez podría ser incrementado según el consumo de servicios de modo que el contador de validez podría estar basado en contar el consumo de servicios (por ejemplo KW/h para el consumo de energía eléctrica o m^3 para el consumo de gas o agua).

[0046] Además, la clave personal usada para autenticar el mensaje de renovación podría ser una clave privada perteneciente al dispositivo de control de medición separable y, en este caso, el mensaje de renovación sería encriptado con una clave pública correspondiente a este dispositivo.

[0047] El nuevo valor de validez usado para recargar el contador de validez y/o el valor de umbral que permite la conmutación entre el modo operativo normal y el modo operativo interrumpido se puede incluir en el mensaje de renovación o se puede prealmacenar en la primera memoria segura SMEM del dispositivo de control de medición separable DM.

[0048] El mensaje de renovación puede incluir información de actualización acerca de este dispositivo, por ejemplo información acerca de su firmware.

[0049] Antes de cambiar del modo normal a otro modo, por ejemplo al modo interrumpido, además podría ser posible alertar al consumidor, a través de un mensaje visualizado en la pantalla del dispositivo o a través de cualquier otro medio (sonido, luz, etc ...), de que el contador de validez de su dispositivo ha alcanzado un nivel crítico. Tales medios de alerta o unidad de alerta ALERT serían útiles para advertir al consumidor de cualquier inconveniente, típicamente la interrupción del consumo del servicio o cualquier aumento en la tarifa.

[0050] El servicio medido por el contador de servicios podría ser energía eléctrica, gas o agua. Además, también podría ser posible imaginar que el contador de servicios, al que el dispositivo de la presente invención se une en una manera desmontable, podría ser capaz de medir diferentes consumos de servicios públicos, tales como consumo de energía eléctrica y agua o gas si fuera necesario. En este caso, el dispositivo de la presente invención podría ser adaptado para tratar estos consumos en vez de tener diferentes dispositivos, es decir uno para cada consumo de servicio.

REIVINDICACIONES

1. Dispositivo de control de medición separable (DM) por ser conectado con un contador de servicios (LM) para controlar al menos un consumo de servicios públicos medido por dicho contador de servicios (LM), comprendiendo:

- una interfaz de lectura de uso (READ) para adquirir un valor de consumo de servicios medido por dicho contador de servicios,
- una primera memoria segura (SMEM) para memorizar al menos un identificador único ID y una clave personal, ambos pertenecientes a dicho dispositivo,
- un procesador cripto (CRYPTO) para generar un criptograma a partir de datos informativos que comprende al menos el valor de consumo de servicios, siendo dicho criptograma encriptado con dicha clave personal,
- un generador de mensaje (MGEN) para generar un mensaje informativo que incluya al menos dicho criptograma y el identificador único ID,
- una interfaz de red de comunicación (GRID) que comprenda una unidad de envío para enviar dicho mensaje informativo a un centro de gestión remoto.

2. Dispositivo según la reivindicación 1, donde dichos datos informativos comprendan además unos datos complementarios predefinidos.

3. Dispositivo según la reivindicación 1, donde dichos datos informativos comprenden además el identificador único ID.

4. Dispositivo de cualquiera de las reivindicaciones 1 a 3, donde el criptograma es un resultado de una función hash en los datos informativos, donde dicho mensaje informativo comprende además el valor de consumo de servicios.

5. Dispositivo de cualquiera de las reivindicaciones 1 a 3, donde dicho mensaje informativo incluye además una versión de firmware de dicho dispositivo.

6. Dispositivo de cualquiera de las reivindicaciones 1 a 5, donde la clave personal es una clave asimétrica en un esquema de encriptación público/privado, teniendo el centro de gestión remoto la clave asimétrica correspondiente.

7. Dispositivo de cualquiera de las reivindicaciones 1 a 6, donde la interfaz de lectura de uso (READ) comprende una conexión eléctrica proporcionada por dicho contador de servicios para transmitir el valor de consumo de servicios públicos.

8. Dispositivo de cualquiera de las reivindicaciones 1 a 6, donde la interfaz de lectura de uso (READ) comprende una interfaz de lectura OCR para leer el consumo de servicio medido por dicho contador de servicios.

9. Dispositivo de cualquiera de las reivindicaciones 1 a 8, que comprende además:

- pluralidad de memorias de tarifas para almacenar el consumo de servicios según diferentes estados del dispositivo,
- una memoria actualizada a la última para almacenar el valor de consumo de servicios mientras se actualiza al menos una memoria de tarifa,
- una unidad de selección para seleccionar una de las memorias de tarifa según el estado actual,
- un calculador de consumo para calcular un valor de consumo actual de la última memoria actualizada y el valor de consumo del servicio adquirido,
- una unidad de actualización de memoria para aplicar el valor de consumo calculado actual a la memoria de tarifa seleccionada por la unidad de selección y para actualizar la última memoria actualizada con el valor de consumo del servicio adquirido.

10. Dispositivo según la reivindicación 9, donde la unidad de selección que selecciona el estado del dispositivo y la memoria de tarifa se conducen por un planificador temporal.

11. Dispositivo según la reivindicación 9, donde la interfaz de red de comunicación (GRID) comprende una unidad de recepción y donde la unidad de selección, para seleccionar una de las memorias de tarifas y el estado del dispositivo, se conduce por la recepción de un mensaje del centro de gestión remoto.

12. Dispositivo de cualquiera de las reivindicaciones 9 a 11, donde la unidad de actualización de memoria comprende una unidad de procesamiento para leer la memoria de la tarifa seleccionada, para añadir el valor de consumo actual a la memoria de la tarifa seleccionada y para escribir dicha suma en la memoria de la tarifa seleccionada.

13. Dispositivo de cualquiera de las reivindicaciones 9 a 12, donde dicho mensaje informativo comprende además los valores de los memorias de las tarifas.

14. Dispositivo de cualquiera de las reivindicaciones 1 o 13, donde el dispositivo comprende además:

- una unidad de autenticación para autenticar mensajes recibidos del centro de gestión remoto a través de la unidad de recepción usando dicha clave personal y, en caso de autentificación exitosa, para ejecutar este mensaje.

15. Dispositivo de cualquiera de las reivindicaciones 1 a 14, donde dicho mensaje es un mensaje de renovación y dicho dispositivo comprende además:

- un contador de validez para incrementar/disminuir un valor de validez según el consumo del servicio o un tiempo,
- una unidad de restablecimiento para sustituir un valor del contador de validez por un valor nuevo,
- un interruptor para intercambiar el funcionamiento del dispositivo de un modo de funcionamiento estándar a un modo de funcionamiento interrumpido, dependiendo de si el valor del contador de validez alcanza al menos un valor umbral predeterminado.

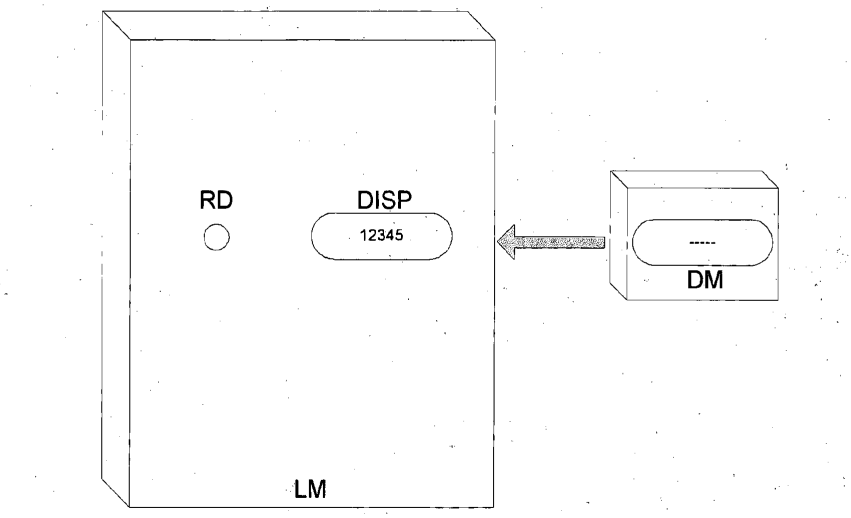

Figura 1

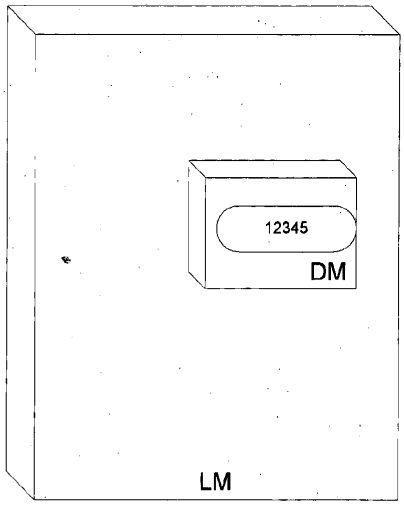

Figura 2

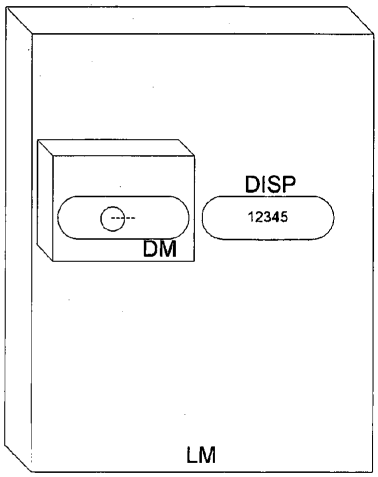

Figura 3

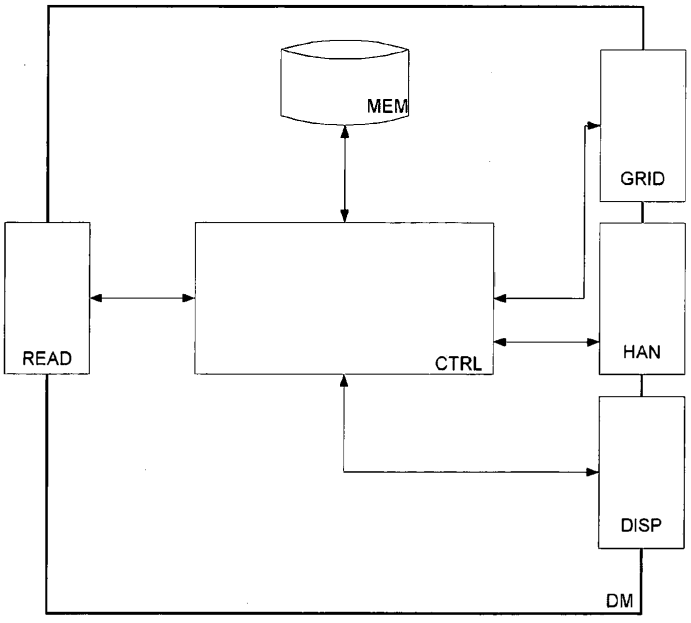

Figura 4

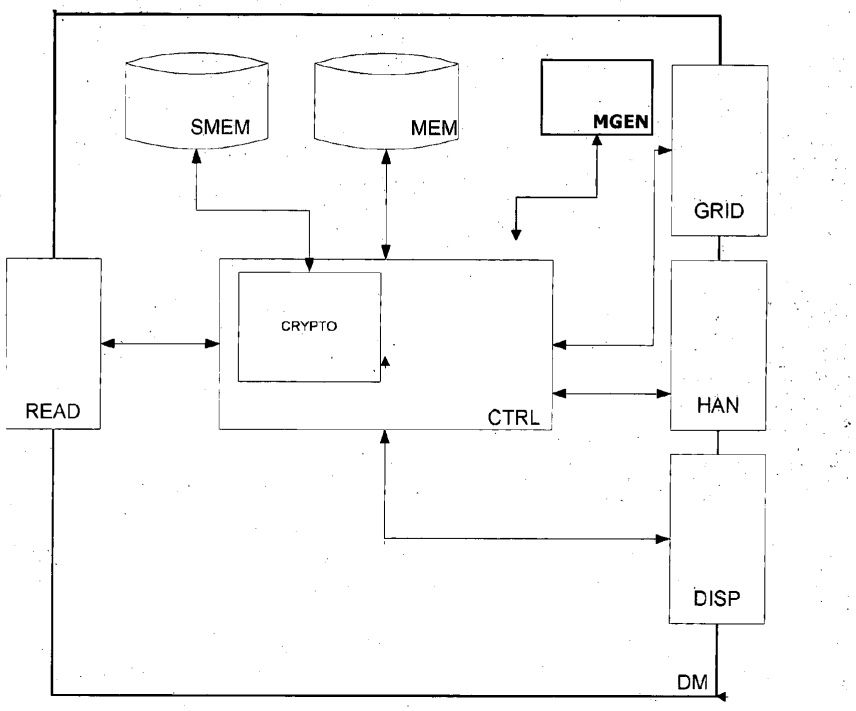

Figura 5

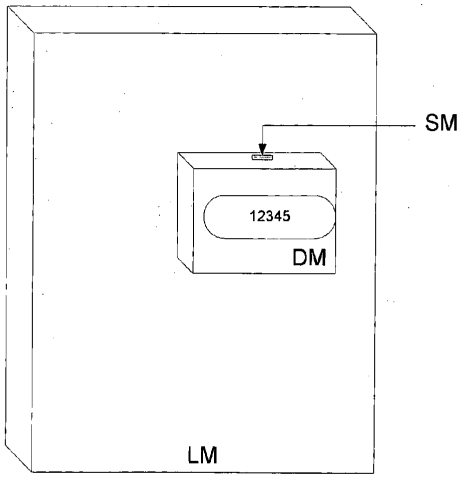

Figura 6

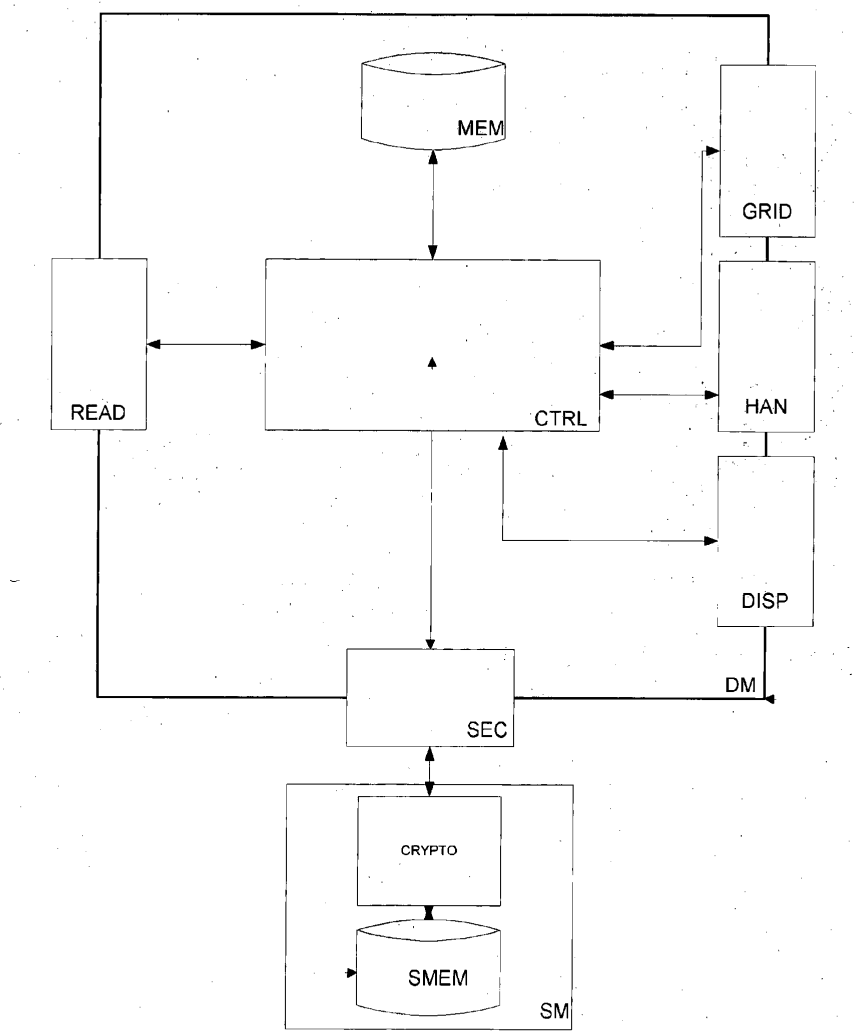

Figura 7