(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 453 515**

(51) Int. CI.:

G07B 15/00 (2011.01)
G01D 4/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.01.2004 E 04001333 (6)**

(97) Fecha y número de publicación de la concesión europea: **25.12.2013 EP 1453272**

(54) Título: **Disposición y método para la detección y el almacenamiento asegurado de valores de detección**

(30) Prioridad:

22.01.2003 DE 10302449

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2014

(73) Titular/es:

FRANCOTYP-POSTALIA GMBH (33.3%)
Triftweg 21-26
16547 Birkenwerder, DE;
FLEXSECURE GMBH (33.3%) y
CONSENS MANAGEMENT GMBH (33.3%)

(72) Inventor/es:

KAMPERT, WERNER;
STALLENBERGER, ERWIN;
GARRELTS, ECKHARD;
KNEE-FORREST, PAUL, DR.;
KESSELBERG, ULRICH y
LIPPEL, MARK

(74) Agente/Representante:

VEIGA SERRANO, Mikel

DESCRIPCIÓN

Disposición y método para la detección y el almacenamiento asegurado de valores de detección

Sector de la técnica

La presente invención se refiere a una disposición para la detección y el almacenamiento asegurado de al menos un primer valor de detección de al menos una primera magnitud de detección según el preámbulo de la reivindicación 1.

Estado de la técnica

Un primer valor de detección de este tipo de una primera magnitud de detección puede ser, por ejemplo, el primer valor de consumo de un primer bien de consumo, por ejemplo de un portador de energía. En relación con la medición del consumo de portadores de energía habituales se conocen una serie de disposiciones. Estas se usan por regla general para registrar y almacenar en hogares particulares u en otros establecimientos determinados consumos de energía. La medición del consumo, es decir la detección de la primera magnitud de detección, se realiza de forma continua, es decir, en el sentido de la presente invención de forma permanente o en intervalos de tiempo predeterminados.

Por el documento US 6.088.659 se conoce por ejemplo una disposición en la que se detecta y almacena el consumo de corriente en un contador correspondiente, además de transmitirse a continuación mediante una comunicación por radio para el procesamiento posterior a un centro de datos. El aseguramiento del valor de consumo almacenado contra accesos no autorizados se realiza habitualmente mediante una carcasa correspondientemente asegurada del contador, que está provista de sensores correspondientes, que detectan una entrada no autorizada.

Las disposiciones conocidas presentan, no obstante, el inconveniente de que mediante la interfaz en principio prevista para la lectura de los valores de consumo, se abre la posibilidad del acceso al dispositivo de seguridad y, por lo tanto, la posibilidad de una manipulación del contador, en particular del valor de consumo almacenado.

Por el documento US 5.828.751 se conoce una disposición en la que los valores de medición de un dispositivo de medición se almacenan de forma criptográficamente asegurada.

Objeto de la invención

Por lo tanto, la presente invención tiene el objetivo de indicar una disposición del tipo indicado al principio que no presente los inconveniente arriba indicados o al menos en un grado inferior y que garantice, en particular, una mayor protección contra una manipulación no detectada, no autorizada de los valores de detección almacenados, permitiendo un cambio sencillo del proveedor del bien de consumo.

La presente invención consigue este objetivo partiendo de una disposición según el preámbulo de la reivindicación 1 mediante las características indicadas en la parte caracterizadora de la reivindicación 1. Además, consigue este objetivo partiendo de un procedimiento según el preámbulo de la reivindicación 17 mediante las características indicadas en la parte caracterizadora de la reivindicación 17.

La presente invención se basa en la doctrina técnica de que se consigue una mayor protección contra una manipulación no descubierta no autorizada de los valores de detección almacenados si la unidad de procesamiento está realizada para la comprobación de la autorización de acceso a al menos una parte del dispositivo de seguridad. La comprobación puede estar limitada a distintas áreas correspondientemente relevantes para la seguridad del dispositivo de seguridad. No obstante, también puede extenderse a la comprobación de la autorización de acceso para todas las áreas del dispositivo de seguridad.

Preferiblemente se comprueba ya la autorización de acceso a la primera memoria, para impedir accesos no autorizados al primer valor de detección almacenado. No obstante, se entiende que en determinadas variantes de la disposición según la invención puede estar admitido el acceso a la primera memoria, incluso sin una autorización de acceso especial, si el primer valor de detección está almacenado de tal forma que puedan detectarse manipulaciones no autorizadas en los valores de detección almacenados. El valor de detección puede almacenarse por ejemplo junto con una información de autentificación generada usándose el valor de detección, como por ejemplo un llamado MAC (Message Authentification Code), una firma digital o algo similar, que se genera en un área del dispositivo de seguridad para la cual se comprueba la autorización de acceso, en caso de que realmente sea posible el acceso.

Gracias a las medidas según la invención se consigue de forma ventajosa que no sea posible de ninguna manera una manipulación no autorizada del primer valor de detección almacenado, por un lado, por falta de acceso al valor de detección almacenado o porque al menos no quede sin detectar en caso de una comprobación.

El dispositivo de interfaz puede ser una interfaz a elegir libremente, mediante la cual sea posible una comunicación

con la unidad de procesamiento y, por lo tanto, un acceso a los datos del dispositivo de seguridad. Se entiende que en determinadas variantes de la disposición según la invención también pueden estar previstos varios dispositivos de interfaz de este tipo. En caso de que sea posible la comunicación con áreas relevantes para la seguridad del dispositivo de seguridad, dado el caso, se produce para cada uno de estos dispositivos de interfaz una comprobación según la invención de la autorización de acceso.

La comprobación de la autorización de acceso puede realizarse en principio de cualquier forma adecuada. Por ejemplo, es posible implementar un sistema con contraseña o algo similar. Preferiblemente está previsto que la unidad de procesamiento esté realizada para la comprobación de la autorización de acceso mediante el uso de medios criptográficos. Pueden aplicarse, por ejemplo, firmas digitales y certificados criptográficos. Esto es especialmente ventajoso, puesto que los procedimientos criptográficos garantizan un estándar de seguridad especialmente elevado.

En variantes especialmente ventajosas de la disposición según la invención están previstos al menos dos niveles de autorización de acceso diferentes, que están vinculados a distintos derechos de acceso al dispositivo de seguridad. Puede implementarse de forma sencilla, por un lado, una estructura jerárquica con derechos de acceso de niveles distintos. Al usuario de la disposición que tiene el nivel de derecho de acceso más bajo puede estar permitido, por ejemplo, como única acción de acceso leer el valor de detección almacenado de la primera memoria, mientras que un administrador de un nivel de autorización de acceso más elevado, además de leer el valor de detección de la primera memoria también puede realizar la modificación de otros componentes del dispositivo de seguridad etc.

Por otro lado, mediante los niveles de autorización de acceso en el mismo nivel de jerarquía también puede controlarse el acceso a distintas áreas del dispositivo de seguridad. El número de niveles o clases de autorización de acceso depende del uso correspondiente de la disposición y de la complejidad de las aplicaciones que pueden realizarse con la disposición según la invención.

En configuraciones preferibles de la disposición según la invención, la unidad de procesamiento para el almacenamiento del primer valor de detección en la primera memoria está realizada de forma vinculada a un identificador del tiempo de detección característico para el tiempo de detección del primer valor de detección. Gracias a esta vinculación del primer valor de detección almacenado con el tiempo de su detección, que se denomina en muchos casos también cronomarcador, se facilita en gran medida el procesamiento posterior del valor de detección, por ejemplo para fines de facturación pero también para fines estadísticos, etc. Esto es especialmente válido cuando deben procesarse varios primeros valores de detección detectados en tiempos distintos.

No obstante, se entiende que en otras variantes de la invención sin cronomarcadores de este tipo también puede bastar con asegurar sólo mediante medidas adecuadas que sea reproducible la cronología de la detección de los primeros valores de detección. Por ejemplo, es posible asignar números correlativos a los primeros valores de detección para conseguir este objetivo.

La detección del tiempo de detección puede realizarse de cualquier forma adecuada. Es especialmente preferible que el dispositivo de seguridad comprenda un módulo de detección de tiempo conectado con la unidad de procesamiento para determinar el identificador del tiempo de detección. Puede ser un reloj en tiempo real integrado, conectado con la unidad de procesamiento o un módulo que consulta el tiempo real mediante una conexión de comunicación adecuada con una instancia correspondiente. El reloj en tiempo real integrado puede sincronizarse, dado el caso, de vez en cuando con una fuente de tiempo correspondientemente exacta.

En variantes preferibles de la disposición según la invención está previsto que la unidad de procesamiento esté realizada para el aseguramiento del primer valor de detección almacenado y de forma adicional o alternativa del identificador del tiempo de detección mediante medios criptográficos. De este modo puede asegurarse que puedan detectarse en una comprobación posterior manipulaciones no autorizadas en los datos así asegurados. Para el aseguramiento pueden aplicarse a su vez procedimientos criptográficos conocidos a elegir libremente. También aquí es especialmente adecuada la aplicación de firmas digitales, que se generan usándose los datos a asegurar.

En configuraciones especialmente ventajosas de la disposición según la invención, el dispositivo de seguridad está realizado para almacenar una pluralidad de primeros valores de detección de la primera magnitud de detección. De este modo pueden realizarse una serie de comprobaciones y de evaluaciones estadísticas en el procesamiento posterior de los valores de detección medidos, en particular si estos primeros valores de detección están provistos de un cronomarcador correspondiente, es decir de un identificador del tiempo de detección. En particular, de este modo también puede realizarse una comprobación de plausibilidad para la detección de determinados o varios valores de detección, también con ayuda de datos estadísticos determinados en el pasado. Esta comprobación de plausibilidad puede usarse tanto para el control del funcionamiento de la unidad de detección, por ejemplo de un dispositivo de medición, como para la detección de intentos de fraude o similares.

En particular, puede garantizarse mediante medidas adecuadas que pueda comprobarse la continuidad de los valores de detección, es decir, que pueda determinarse si existe una serie ininterrumpida de los valores de detección o si faltan determinados valores de detección, ya sea por un funcionamiento incorrecto o por un intento de fraude.

Esto puede estar realizado de forma sencilla, p.ej. porque se asignan números correlativos a los valores de detección, que están asegurados preferiblemente también a su vez de forma correspondiente mediante medios criptográficos. En caso de que la detección de los valores de detección se realice en intervalos de tiempo predeterminados, para ello también puede bastar por ejemplo el cronomarcador.

En variantes especialmente favorables de la disposición según la invención está previsto al menos un segundo dispositivo de detección para la detección de al menos un segundo valor de detección de la primera magnitud. El dispositivo de seguridad está realizado en este caso para el almacenamiento del segundo valor de detección en la primera memoria, pudiendo tomarse las medidas de seguridad arriba descritas, de modo que respecto al almacenamiento asegurado contra accesos no autorizados se remite a las explicaciones anteriormente expuestas. Con estas variantes es posible hacer funcionar también sistemas más grandes con varios lugares de detección de la magnitud de detección, por ejemplo varios puntos de medición para el consumo de un bien de consumo, con un número reducido de dispositivos de seguridad, dado el caso incluso con un solo dispositivo de seguridad. Puede detectarse por ejemplo el consumo de energía en una casa grande con varias viviendas, es decir, unidades de consumo a detectar por separado mediante un número correspondiente de dispositivos de detección descentralizados que están conectados todos con un solo dispositivo de seguridad.

Para asegurar la separación de los primeros y segundos valores de detección puede estar previsto que los primeros y segundos valores de detección se depositen en distintas áreas de memoria de la primera memoria. Aquí pueden estar definidas en particular distintas autorizaciones de acceso para las distintas áreas de memoria, para asegurar que sólo puedan acceder al área de memoria correspondiente las personas u organismos respectivamente autorizados.

No obstante, es especialmente ventajoso que la unidad de procesamiento esté realizada para almacenar el primer valor de detección vinculado al primer identificador de dispositivo de detección característico para el primer dispositivo de detección y para almacenar el segundo valor de detección vinculado a un segundo identificador del dispositivo de detección característico para el segundo dispositivo de detección. Con esta asignación unívoca entre el dispositivo de detección y el valor de detección detectado por el mismo es posible una separación especialmente sencilla y fiable, que facilita considerablemente el procesamiento posterior.

Para evitar aquí accesos no autorizados a los valores de detección correspondientes por parte de personas u organismos que en principio están autorizados para el acceso a la primera memoria, para los primeros y segundos valores de detección puede estar previsto que estén almacenados de forma codificada de distintas maneras. La descodificación sólo puede ser realizada respectivamente por la persona o el organismo correspondientemente autorizado, que tiene por ejemplo la clave de descodificación correspondiente.

Se entiende que también aquí puede estar previsto a su vez un aseguramiento criptográfico de los datos almacenados, como ya se ha descrito anteriormente, para evitar eficazmente la manipulación no descubierta de estos datos.

En otras configuraciones favorables de la disposición según la invención está previsto que el primer dispositivo de detección esté realizado para la detección de al menos un tercer valor de detección de una segunda magnitud de detección. Como alternativa, puede estar previsto un tercer dispositivo de detección para la detección de al menos un tercer valor de detección de una segunda magnitud de detección. En los dos casos, el dispositivo de seguridad está realizado para el almacenamiento asegurado contra accesos no autorizados del tercer valor de detección en la primera memoria, pudiendo tomarse también en este caso preferiblemente las medidas de seguridad arriba descritas.

De este modo es posible realizar con un solo dispositivo de seguridad la detección y el almacenamiento asegurado de los valores de detección para distintas magnitudes de detección en forma de distintos bienes de consumo. Para una unidad de consumo como una vivienda o similares puede detectarse por ejemplo mediante distintos dispositivos de detección el consumo de distintos portadores de energía, como corriente, gas, agua y puede ser almacenado de forma asegurada mediante un único dispositivo de seguridad pudiendo ponerse a disposición para el procesamiento posterior autorizado.

Para asegurar la separación de los primeros y terceros valores de detección, también aquí puede estar previsto que los primeros y terceros valores de detección se depositen en distintas áreas de memoria de la primera memoria. No obstante, también aquí es especialmente ventajoso que la unidad de procesamiento esté realizada para almacenar el primer valor de detección vinculado al primer identificador de magnitud de detección característico para la primera magnitud de detección y para almacenar el tercer valor de detección vinculado al segundo identificador de magnitud de detección característico para la segunda magnitud de detección. Con esta asignación unívoca entre el dispositivo de detección y la magnitud de detección detectada por el mismo es posible una separación especialmente sencilla y fiable, que facilita considerablemente el procesamiento posterior de los datos almacenados. También aquí pueden volver a tomarse naturalmente las medidas anteriormente descritas para evitar accesos no autorizados a los primeros y terceros valores de detección.

Por lo demás, se entiende que también aquí puede estar previsto a su vez un aseguramiento criptográfico de los datos almacenados, como ya se ha descrito anteriormente, para evitar eficazmente la manipulación no descubierta de estos datos.

En variantes especialmente preferibles de la disposición según la invención, la unidad de procesamiento presenta al menos un primer modo de servicio y un segundo modo de servicio. Además, está realizada para conmutar entre el primero y el segundo modo de servicio, realizándose esta conmutación en respuesta a un comando de conmutación. Preferiblemente, la unidad de procesamiento está realizada para la comprobación de un criterio de conmutación y para la generación del comando de conmutación en función del resultado de la comprobación del criterio de conmutación. El criterio de conmutación está almacenado aquí en una segunda memoria conectada con la unidad de procesamiento.

De este modo pueden realizarse de forma sencilla escenarios de aplicación, en los que la disposición realiza distintas funciones en función de si llegan a cumplirse unas condiciones predeterminadas o que pueden ser predeterminadas. Al llegar a cumplirse por ejemplo condiciones predeterminadas o que pueden ser predeterminadas puede iniciarse una rutina de notificación, con la que se informan personas u organismos correspondientes de que ha llegado a cumplirse la condición. Por ejemplo, en caso de la detección del consumo, el consumidor del bien de consumo, el proveedor del bien de consumo o un tercero pueden ser informados de que ha llegado a cumplirse la condición. Esto puede realizarse mediante medios de notificación a elegir libremente, como indicaciones ópticas o acústicas, correo electrónico, fax, SMS etc. De este modo, el consumidor puede ser informado por ejemplo de un consumo inusitadamente elevado o de un consumo que difiere del perfil de consumo normal o de que se ha sobrepasado un límite de consumo definido por él mismo.

En otras variantes preferibles de la disposición según la invención está previsto que esté previsto un dispositivo de influencia para influir en la primera magnitud de detección que está conectado con la unidad de procesamiento y que al menos en el segundo modo de servicio está mandado por la unidad de procesamiento. De este modo, en caso de una detección del consumo puede estar previsto un dispositivo de influencia en el consumo para la influencia en el consumo del primer bien de consumo. Gracias a este dispositivo de influencia en el consumo puede procederse a un bloqueo del consumo, por ejemplo, en el caso de llegar a cumplirse determinadas condiciones, por ejemplo quedarse por debajo de un saldo determinado, sobrepasar un marco de crédito determinado o sobrepasar un valor de consumo determinado. Dado el caso, puede iniciarse a tiempo antes de llegar a cumplirse esta condición una de las rutinas de notificación arriba descritas, para informar al consumidor por ejemplo del bloqueo inminente.

En otras variantes, en las que se realiza la detección de un parámetro de servicio de un dispositivo como magnitud de detección, puede estar prevista una influencia en el parámetro de servicio. Por ejemplo, al llegar a cumplirse determinadas condiciones, por ejemplo quedarse por debajo o por encima de un valor límite determinado para el parámetro de servicio, puede realizarse o iniciarse una contramedida correspondiente, que debe hacer pasar el parámetro de servicio nuevamente a un intervalo predeterminado. Dado el caso, puede iniciarse a tiempo antes de llegar a cumplirse la condición indicada una de las rutinas de notificación arriba descritas, para informar a las personas o los organismos correspondientes de que es inminente el cumplimiento de la condición.

El criterio de conmutación puede ser predeterminado preferiblemente mediante acceso mediante el primer dispositivo de interfaz a la segunda memoria o puede ser modificado de forma adicional o alternativa para poder influir de forma ventajosa en el criterio de conmutación o para poder reaccionar a circunstancias cambiadas.

En variantes especialmente ventajosas de la disposición según la invención, el dispositivo de seguridad comprende un módulo de acuse de recibo conectado con la unidad de procesamiento con una tercera memoria. Además, la unidad de procesamiento está realizada para generar un acuse de recibo para un acceso al dispositivo de seguridad, en particular para un acceso a la primera memoria, y para el almacenamiento del primer acuse de recibo en la tercera memoria. De este modo es posible de forma ventajosa documentar el acceso al dispositivo de seguridad y evaluarlo, dado el caso, en un momento posterior.

Se entiende que también aquí puede volver a estar previsto un almacenamiento asegurado contra accesos no autorizados del acuse de recibo, así como el aseguramiento del acuse de recibo mediante medios criptográficos, como ya se han descrito detalladamente antes, de modo que en este lugar sólo se remite a las explicaciones anteriores.

Preferiblemente está previsto que la unidad de procesamiento esté realizada para almacenar el acuse de recibo en la segunda memoria vinculado al identificador de acceso característico para el usuario que accede. Este identificador del usuario que accede es preferiblemente una segunda firma digital del usuario que accede, que se genera preferiblemente usándose la información del acuse de recibo. De este modo es posible de forma sencilla asignar las modificaciones de la disposición realizadas en el marco de accesos de este tipo, en particular del dispositivo de seguridad, a distintos usuarios que acceden. Esto es especialmente ventajoso por los aspectos de la responsabilidad.

Además, el acuse de recibo es provisto preferiblemente de un cronomarcador. Para ello, la unidad de procesamiento está realizada preferiblemente para almacenar el acuse de recibo en la segunda memoria vinculado al identificador del tiempo de acceso característico para el tiempo del acceso. Se entiende que también aquí pueden volver a tomarse las mismas medidas, en particular las mismas medidas de seguridad como se han descrito ya anteriormente en relación con el identificador del tiempo de detección.
En particular, el dispositivo de seguridad para determinar el identificador del tiempo de acceso comprende preferiblemente un módulo de detección de tiempo conectado con la unidad de procesamiento. También es preferible que la unidad de procesamiento esté realizada para asegurar el acuse de recibo almacenado y de forma adicional o alternativa el identificador del usuario que accede así como de forma adicional o alternativa el identificador del tiempo de acceso mediante medios criptográficos. Aquí puede realizarse en particular nuevamente un aseguramiento mediante una tercera firma digital, que se genera preferiblemente usándose los datos a asegurar.

Según la invención, el dispositivo de seguridad presenta para la selección de un proveedor de un primer bien de consumo un módulo de selección conectado con la unidad de procesamiento. El consumo del primer bien de consumo representa aquí la primera magnitud de detección. Además, la unidad de procesamiento está realizada para almacenar el primer valor de consumo como primer valor de detección en la primera memoria vinculado al identificador de proveedor característico para el proveedor seleccionado del primer bien de consumo. De este modo es posible de forma sencilla seleccionar un proveedor determinado según unos criterios determinados y asignar a este proveedor los valores de consumo determinados, para facturarlos por ejemplo posteriormente a nombre de este proveedor.

Por ejemplo, puede estar previsto que un consumidor seleccione a través de una interfaz determinada del dispositivo de seguridad a libre elección un proveedor del bien de consumo, por ejemplo un determinado proveedor de corriente, al que se asignan los valores de consumo detectados tras la selección de la forma descrita. Aquí, naturalmente es posible definir determinadas especificaciones o límites respecto a la frecuencia de los cambios del proveedor etc.

También aquí, preferiblemente está previsto que la unidad de procesamiento esté realizada para asegurar el identificador del proveedor mediante medios criptográficos, como ya se ha descrito detalladamente más arriba con ayuda de otros identificadores. Aquí, el aseguramiento puede realizarse, en particular, nuevamente mediante una cuarta firma digital.

En variantes especialmente ventajosas de la disposición según la invención está prevista que la unidad de procesamiento esté realizada para la comprobación de un criterio de selección y para la selección del proveedor en función del resultado de la comprobación del criterio de selección, estando almacenado el criterio de selección en una cuarta memoria conectada con la unidad de procesamiento. De este modo, p.ej., es posible minimizar de forma sencilla los costes de consumo, seleccionándose mediante una comparación de las tablas de tasas de distintos proveedores aquél que ofrezca el bien de consumo en el momento actual al precio más favorable. Esta consulta puede realizarse en intervalos predeterminados. Además, puede estar prevista tanto una actualización de las tablas de tasas iniciada regularmente por la unidad de procesamiento como una actualización regular por parte de los proveedores, que llegan mediante una conexión de comunicación correspondiente a la unidad de procesamiento.

Como ya se ha mencionado anteriormente, puede estar prevista una selección libre por parte del consumidor. Para ello, está previsto preferiblemente un dispositivo de entrada de selección conectado con la unidad de procesamiento, pudiendo ser predeterminado el criterio de selección por un usuario mediante el dispositivo de entrada de selección mediante acceso a la cuarta memoria, y de forma adicional o alternativa pudiendo ser modificado.

Para poder entender también en un momento posterior la selección, en variantes preferibles de la disposición según la invención está previsto que la unidad de procesamiento esté realizada para almacenar el primer valor de consumo en la primera memoria vinculado al identificador de usuario característico para el usuario que selecciona. También aquí pueden volver a usarse los mecanismos de aseguramiento arriba descritos. Por lo tanto, la unidad de procesamiento está realizada preferiblemente para asegurar el identificador del usuario mediante medios criptográficos, en particular mediante una quinta firma digital.

En realizaciones preferibles de la disposición según la invención, el dispositivo de seguridad comprende un módulo criptográfico conectado con la unidad de procesamiento, que está realizado para poner a disposición de la unidad de procesamiento medios criptográficos para al menos una aplicación de seguridad usándose al menos primeros datos criptográficos, estando almacenados los primeros datos criptográficos en una quinta memoria del módulo criptográfico y comprendiendo al menos un primer algoritmo criptográfico. De este modo es posible de forma sencilla un aseguramiento correspondientemente fiable, tanto de los datos a almacenar como de los datos a transmitir. Usándose el módulo criptográfico, posteriormente pueden ponerse a disposición los medios criptográficos descritos para los distintos módulos (módulo de detección de tiempo, módulo de acuse de recibo etc.) y funciones del dispositivo de seguridad.

El módulo criptográfico puede usarse, por un lado, para la codificación de los datos a almacenar y, por otro lado, también para la codificación de los datos a enviar. Por ejemplo, pueden codificarse los datos que se leen o

transmiten mediante la primera interfaz mediante un procedimiento criptográfico correspondiente con un algoritmo criptográfico correspondiente. Se entiende que según la aplicación, es decir, por ejemplo en función de si deben enviarse o almacenarse datos, también pueden usarse distintos procedimientos criptográficos.

Además del algoritmo criptográfico y de una o varias claves criptográficas, los datos criptográficos comprenden preferiblemente otros datos, como por ejemplo uno o varios certificados criptográficos de instancias de certificación correspondientes, así como dado el caso uno o varios certificados criptográficos propios del dispositivo de seguridad.

En variantes preferibles de la disposición según la invención, el dispositivo de seguridad está realizado para el intercambio de al menos una parte de los primeros datos criptográficos para garantizar de forma ventajosa un aseguramiento sencillo y fiable a largo plazo de los datos. Aquí puede estar previsto, en particular, que además de las claves criptográficas y certificados criptográficos también pueda intercambiarse el algoritmo criptográfico respectivamente usado, para poder adaptar el sistema de forma sencilla a requisitos de seguridad modificados.

La implementación y el intercambio de los datos criptográficos se realizan usándose el primer dispositivo de interfaz u otro dispositivo de interfaz, preferiblemente en el marco de una llamada infraestructura de clave pública (en inglés Public Key Infrastructure (PKI)), como es sobradamente conocida y no se describirá más detalladamente aquí. En particular, se entiende que está prevista una rutina correspondiente para la comprobación de la validez de los certificados criptográficos usados. Las rutinas de comprobación de este tipo también son sobradamente conocidas, por lo que no se describirán aquí en detalle.

En variantes preferibles de la disposición según la invención, el primer dispositivo de detección y el dispositivo de seguridad están dispuestos en un entorno seguro protegido contra accesos no autorizados, para impedir eficazmente de forma ventajosa accesos no autorizados no sólo a los datos del dispositivo de seguridad sino también a los datos que se suministran de y al primer dispositivo de detección.

El entorno seguro puede estar realizado, por un lado, de forma física mediante una o varias carcasas correspondientemente aseguradas. Estas carcasas están provistas preferiblemente de medios correspondientes, sobradamente conocidos, para la detección de manipulaciones en la carcasa. No obstante, el aseguramiento se realiza preferiblemente también de forma lógica mediante un protocolo de comunicación correspondientemente asegurado entre el primer dispositivo de detección y el dispositivo de seguridad. Por ejemplo, puede estar previsto que en cada comunicación entre el primer dispositivo de detección y el dispositivo de seguridad se establezca un canal de comunicación asegurado mediante una autentificación mutua correspondientemente fuerte. Se entiende que el primer dispositivo de detección dispone en este caso de medios de comunicación correspondientes, que ponen a disposición la funcionalidad de seguridad descrita.

También se entiende que mediante los mecanismos de seguridad lógicos de este tipo, el entorno seguro puede extenderse a un espacio de un tamaño a elegir libremente. En las realizaciones de este tipo, el primer dispositivo de detección y el dispositivo de seguridad pueden estar dispuestos a grandes distancias unos de otros dentro del entorno seguro. También se entiende que mediante los mecanismos de seguridad lógicos de este tipo, el entorno seguro también puede ampliarse a otros componentes, por ejemplo un centro de datos o similares, del que se leen los datos de la primera memoria para el procesamiento posterior.

Por lo tanto, el primer dispositivo de detección está dispuesto preferiblemente en una primera carcasa segura y el dispositivo de seguridad en una segunda carcasa segura, estando realizada la comunicación entre el primer dispositivo de detección y el dispositivo de seguridad para generar el entorno seguro como conexión asegurada por medios criptográficos.

Se entiende que todos los módulos y funciones anteriormente descritos del dispositivo de seguridad pueden estar realizados mediante módulos hardware correspondientemente configurados. No obstante, están configurados al menos en parte como módulos software, a los que accede la unidad de procesamiento para realizar la función correspondiente. Además, se entiende que las distintas memorias no tienen que estar realizadas en forma de módulos de memoria separados. Por lo contrario, se trata preferiblemente de áreas de memoria correspondientemente separadas de forma lógica de una sola memoria, por ejemplo de un solo módulo de memoria.

La presente invención se refiere además a un sistema con una disposición según la invención, cuyo dispositivo de seguridad presenta al menos un primer dispositivo de interfaz conectado con la unidad de procesamiento para acceder al dispositivo de seguridad, que está realizado como primer dispositivo de comunicación. Además, está previsto un centro de datos remoto del dispositivo de seguridad con un segundo dispositivo de comunicación. El primer dispositivo de comunicación y el segundo dispositivo de comunicación están realizados para establecer una primera conexión de comunicación entre el dispositivo de seguridad y el centro de datos.

De este modo es posible acceder desde el centro de datos remoto a la disposición, en particular al dispositivo de seguridad de la misma y de leer por ejemplo los valores de detección almacenados y procesarlos posteriormente. Por lo tanto, el centro de datos está realizado preferiblemente para leer los contenidos de memoria de la primera

memoria mediante la primera conexión de comunicación. En caso de una autorización de acceso correspondiente, naturalmente también es posible influir mediante el centro de datos en el comportamiento de la disposición, como ya se ha descrito anteriormente.

El centro de datos almacena los datos de detección leídos y los tiene preparados para el procesamiento posterior. Se entiende que los datos de detección se tienen preparados, dado el caso, de una forma correspondientemente anonimizados, para cumplir con los requisitos de la protección de datos.

El procesamiento posterior puede realizarse en otro centro de datos remoto, por ejemplo del proveedor del bien de consumo correspondiente, al que se transmiten en este caso los datos de detección. El centro de datos procesa preferiblemente estos datos de detección leídos ya al menos hasta cierto grado.

En particular, en el caso de valores de consumo como valores de detección puede estar previsto que la facturación del consumo se realiza a través del centro de datos. Por lo tanto, el centro de datos está realizado preferiblemente para generar una información de facturación en función de los contenidos de memoria de la primera memoria. Para ello, el centro de datos puede ser operado por el proveedor del bien de consumo correspondiente. No obstante, se entiende que el centro de datos también puede ser operado por un tercero, que pone a disposición estos servicios.

Como ya se ha mencionado anteriormente, en caso de una autorización de acceso correspondiente puede estar previsto que mediante el centro de datos se influya en el comportamiento de la disposición. Por lo tanto, el centro de datos está realizado para la especificación y de forma adicional o alternativa para la modificación del criterio de conmutación arriba descrito.

En particular, puede estar previsto que al llegar a cumplirse determinadas condiciones, el centro de datos influya en la magnitud de detección, como ya se ha descrito anteriormente, por ejemplo impidiendo el centro de datos el consumo del bien de consumo. En particular, esto puede ser el caso en los llamados sistemas de prepago o sistemas prepaid, cuando el saldo se queda por debajo de un saldo mínimo determinado. Para ello puede estar previsto en combinación con las disposiciones arriba descritas con al menos dos modos de servicio que el consumo del primer bien de consumo quede bloqueado en el segundo modo de servicio siendo el criterio de conmutación cuando se constata que el saldo actual, almacenado en la segunda memoria, queda por debajo de un límite de saldo almacenado en la segunda memoria.

Aquí, el usuario tiene preferiblemente una posibilidad para evitar o impedir de forma sencilla y rápida el bloqueo. El centro de datos presenta para ello preferiblemente un tercer dispositivo de comunicación, mediante el cual puede establecerse una segunda conexión de comunicación para cambiar el saldo actual almacenado en la segunda memoria. Puede estar previsto, por ejemplo, un pago exprés por móvil mediante servicios correspondientes o algo similar.

Por lo demás, se entiende que el sistema según la invención también puede comprender varias disposiciones según la invención, así como de forma adicional o alternativa también varios centros de datos. Esto puede ser el caso, en particular, cuando se detectan mediante uno o varios dispositivos de seguridad distintas magnitudes de detección, en particular los consumos de distintos bienes de consumo de distintos proveedores. Estos pueden ser distribuidos a continuación para el procesamiento posterior a distintos centros de datos.

En principio, las magnitudes de detección pueden ser magnitudes correspondientemente detectables a elegir libremente. Pueden detectarse en principio parámetros de estado o parámetros de servicio a elegir libremente de dispositivos a elegir libremente. Además, puede detectarse como magnitud de detección si se producen o no determinados eventos. Según la invención, se detecta el consumo de un bien de consumo.

En principio pueden ser bienes de consumo bienes o prestaciones a elegir libremente, en particular servicios, que pueden detectarse mediante una medición de consumo correspondiente. Como ejemplos pueden indicarse aquí portadores de energía como corriente, combustibles, agua, etc. No obstante, también puede detectarse el uso sujeto a pago de dispositivos a elegir libremente. Aquí pueden indicarse como ejemplos dispositivos de telecomunicación, determinados aparatos, como por ejemplo maquinaria de construcción o vehículos, pero también dispositivos de juegos o similares. En particular, para el uso de un aparato, en particular de un vehículo, en cuyo caso la facturación se realiza en función de una distancia recorrida o de la permanencia en una posición determinada o en una zona geográfica determinada, es posible usar como valor de consumo o uno de los valores de consumo a detectar también la posición, que puede detectarse mediante un módulo correspondiente para la detección de la posición, por ejemplo un módulo GPS.

En relación con la medición del consumo también puede detectarse, en particular, la prestación de determinados servicios. Por ejemplo puede detectarse la duración de la presencia de un empleado o de un mandatario en un lugar de trabajo determinado mediante unidades de detección correspondientes, para que el empleador o mandante pueda detectar el consumo de la prestación de trabajo del empleado o contratista. Naturalmente, lo mismo es válido para la presencia de determinados aparatos o dispositivos en determinados lugares de empleo, en los que puede conseguirse adicionalmente mediante la detección de determinados parámetros de servicio también una información

acerca del uso real del aparato o del dispositivo durante la presencia en el lugar de empleo.

La presente invención se refiere además a un procedimiento para la detección y el almacenamiento asegurado de al menos un primer valor de detección de al menos una primera magnitud de detección según la reivindicación 17, en el que se detecta la primera magnitud de detección de forma sustancialmente continua y se almacena el primer valor de detección en un dispositivo de seguridad. El primer valor de detección se almacena de forma asegurada contra accesos no autorizados en una primera memoria del dispositivo de seguridad. Según la invención está previsto que en caso de un acceso al dispositivo de seguridad mediante un primer dispositivo de interfaz, en particular, en caso de un acceso para leer el primer valor de detección de la primera memoria tiene lugar una comprobación de la autorización de acceso al dispositivo de seguridad. En particular, se realiza una comprobación de la autorización de acceso a la primera memoria.

Con el procedimiento según la invención pueden conseguirse las ventajas y funciones ya anteriormente descritas de la disposición según la invención con el alcance que se ha descrito anteriormente en detalle, de modo que a este respecto sólo se remite a las explicaciones anteriormente expuestas. También respecto a las variantes preferibles del procedimiento según la invención se remite aquí sólo al funcionamiento de las configuraciones de la disposición según la invención que se ha descrito anteriormente en detalle.

Descripción de las figuras

Otras configuraciones preferibles de la invención resultan de las reivindicaciones dependientes o de la descripción expuesta a continuación de ejemplos de realización preferibles, que hace referencia a los dibujos adjuntos. Muestran:

La Figura 1 un diagrama de bloques de una forma de realización preferible de la disposición según la invención para la realización del procedimiento según la invención.

La Figura 2 un diagrama de bloques de una forma de realización preferible del sistema según la invención con la disposición según la invención de la Figura 1.

La Figura 3 un diagrama de bloques de otra forma de realización preferible del sistema según la invención.

La Figura 4 un diagrama de bloques de una forma de realización preferible del sistema según la invención.

La Figura 5 un diagrama de bloques de otra forma de realización preferible del sistema según la invención.

Descripción detallada de la invención

La Figura 1 muestra una forma de realización preferible de la disposición 1 según la invención para la realización del procedimiento según la invención. La disposición 1 sirve para la detección y el almacenamiento asegurado de un primer valor de consumo del consumo de un primer bien de consumo. El primer valor de consumo representa el primer valor de detección, mientras que el consumo de primer bien de consumo representa la primera magnitud de detección. En el presente caso se trata del consumo de corriente, que se detecta en una línea eléctrica 2.

La disposición 1 comprende un primer dispositivo de detección 3 para la detección del primer valor de consumo y un dispositivo de seguridad en forma de un módulo de seguridad 4 conectado con el primer dispositivo de detección 3. El primer dispositivo de detección 3 comprende una unidad de detección en forma de un dispositivo de medición 3.1 conectado con el módulo de seguridad 4, que está realizado de forma conocida para la medición sustancialmente continua del consumo de corriente.

El módulo de seguridad 4 comprende a su vez una unidad de procesamiento 5, una primera memoria 6 conectada con ésta, así como un primer dispositivo de interfaz 7 conectado con la unidad de procesamiento 5. Los valores de consumo detectados por el dispositivo de detección 3 se transmiten a la unidad de procesamiento 5, que los deposita a continuación en la primera memoria 6. En la primera memoria se almacenan varios primeros valores de consumos detectados sucesivamente. Mediante el primer dispositivo de interfaz 7 puede accederse al módulo de seguridad, en particular a la primera memoria, para leer en particular los primeros valores de consumo de la primera memoria 6.

El módulo de seguridad 4 está realizado para el almacenamiento asegurado contra accesos no autorizados del primer valor de consumo en la primera memoria 6. Para ello, presenta, por un lado, una carcasa que está físicamente asegurada de una forma correspondiente y, por otro lado, la unidad de procesamiento también realiza una comprobación de la autorización de acceso al módulo de seguridad 4. La comprobación puede limitarse a determinadas áreas correspondientemente relevantes para la seguridad del módulo de seguridad 4. En el presente caso, la comprobación se extiende, no obstante, también a la comprobación de la autorización de acceso a todas las áreas del módulo de seguridad 4. De este modo se consigue una mayor protección contra una manipulación no autorizada no descubierta de los valores de consumo almacenados.

Para conseguir otro aseguramiento de los valores de consumo almacenados, los primeros valores de consumo se almacenan de tal forma que puedan detectarse manipulaciones no autorizadas en los valores de consumo almacenados. El valor de consumo puede almacenarse por ejemplo junto con una información de autentificación generada usándose el valor de consumo, como por ejemplo un llamado MAC (Message Authentification Code), una firma digital o algo similar, que se genera en un área del módulo de seguridad 4, para el que se comprueba la autorización de acceso. De este modo se consigue que no sea posible de ninguna manera una manipulación no autorizada de los valores de consumo almacenados por falta de acceso o que al menos no quede sin descubrir en caso de una comprobación.

La comprobación de la autorización de acceso mediante la unidad de procesamiento 5 se realiza mediante el uso de medios criptográficos. Aquí, en el marco de una autentificación mutua de los participantes de la comunicación se realiza una comprobación de firmas digitales usándose certificados criptográficos correspondientes. Esto es especialmente ventajoso, puesto que los procedimientos criptográficos de este tipo garantizan un estándar de seguridad especialmente elevado.

Para ello está previsto un módulo criptográfico 8 conectado con la unidad de procesamiento 5, que está realizado para poner a disposición de la unidad de procesamiento medios criptográficos para al menos una aplicación de seguridad usándose al menos primeros datos criptográficos. Los primeros datos criptográficos están almacenados en una quinta memoria 8.1 del módulo criptográfico 8. Los primeros datos criptográficos comprenden un primer algoritmo criptográfico y una o varias clave criptográficas, así como uno o varios certificados criptográficos de instancias de certificación correspondientes, así como uno o varios certificados criptográficos propios del módulo de seguridad 4.

El módulo criptográfico 8 puede usarse, por un lado, para la codificación de los datos a almacenar y, por otro lado, también para la codificación de los datos a enviar. Por ejemplo, pueden codificarse los datos que se leen o transmiten mediante la primera interfaz 7 mediante un procedimiento criptográfico correspondiente con el algoritmo criptográfico almacenado. Se entiende que según la aplicación, es decir, por ejemplo en función de si deben enviarse o almacenarse datos, también pueden usarse distintos procedimientos criptográficos.

El módulo de seguridad 4 está realizado para el intercambio de al menos una parte de los primeros datos criptográficos, para garantizar mediante actualizaciones correspondientes un aseguramiento sencillo y fiable a largo plazo de los datos. Aquí, en particular, es posible que además de las claves criptográficas y certificados criptográficos almacenados en la quinta memoria 8.1, también pueda intercambiarse el algoritmo criptográfico respectivamente usado, para poder adaptar el sistema a requisitos de seguridad modificados.

La implementación y el intercambio de los datos criptográficos se realizan usándose el primer dispositivo de interfaz 7 en el marco de una llamada infraestructura de clave pública (en inglés Public Key Infrastructure (PKI)). Además, está prevista una rutina correspondiente para la comprobación de la validez de los certificados criptográficos usados mediante rutinas de comprobación adecuadas.

Para la disposición 1 están previstos dos niveles de autorización de acceso diferentes, que están vinculadas a distintos derechos de acceso al módulo de seguridad 4 para implementar una estructura jerárquica con derechos de acceso de niveles distintos. El usuario de la disposición 1, es decir, el consumidor, en el nivel de derecho de acceso más bajo tiene permitido como única acción de acceso leer el valor de consumo almacenado mediante una interfaz 9 local de la primera memoria 6, mientras que un administrador de un nivel de autorización de acceso más elevado, además de leer el valor de consumo de la primera memoria 6, también puede realizar la modificación de otros componentes del módulo de seguridad 4.

La unidad de procesamiento 5 está realizada además para el almacenamiento del primer valor de consumo en la primera memoria 6 de forma vinculada a un identificador del tiempo de detección característico para el tiempo de detección del primer valor de consumo. Gracias a esta vinculación del primer valor de consumo almacenado con el tiempo de su detección, que se denomina en muchos casos también cronomarcador, se facilita claramente el procesamiento posterior del valor de consumo, por ejemplo para fines de facturación, pero también para fines estadísticos etc.

Para determinar el tiempo de detección, el módulo de seguridad 4 comprende un módulo de detección de tiempo 10 conectado con la unidad de procesamiento 5. Es un reloj en tiempo real integrado, que se sincroniza en intervalos regulares, por ejemplo al establecer contacto con un centro de datos externo, con una fuente de tiempo correspondientemente exacta.

Tanto el primer valor de consumo almacenado como el identificador del tiempo de detección son asegurados por la unidad de procesamiento 5 accediéndose al módulo criptográfico 8. Esto se realiza porque se genera una firma digital en el valor de consumo y en el identificador del tiempo de detección correspondiente. De este modo queda asegurado que puedan constatarse en una comprobación posterior manipulaciones no autorizadas en los datos así asegurados.

La unidad de procesamiento 5 presenta un primer modo de servicio y un segundo modo de servicio, entre los que puede conmutarse mediante un comando de conmutación. La unidad de procesamiento 5 está realizada para la comprobación de un criterio de conmutación y para la generación del comando de conmutación en función del resultado de la comprobación del criterio de conmutación. El criterio de conmutación está almacenado en una segunda memoria 11 conectada con la unidad de procesamiento.

De este modo pueden realizarse de forma sencilla escenarios de aplicación, en los que la disposición realiza distintas funciones en función de si llegan a cumplirse unas condiciones predeterminadas o que pueden ser predeterminadas. Al llegar a cumplirse por ejemplo condiciones predeterminadas o que pueden ser predeterminadas, puede iniciarse una rutina de notificación, con la que se informa al consumidor del bien de consumo o a un tercero de que ha llegado a cumplirse la condición. Esto puede realizarse mediante medios de notificación a elegir libremente, como indicaciones ópticas o acústicas, correo electrónico, fax, SMS. De este modo, el consumidor puede ser informado, por ejemplo, de un consumo inusitadamente elevado o que difiere del perfil de consumo habitual o de que se ha sobrepasado un límite de consumo definido por él mismo.

En el presente ejemplo está previsto un dispositivo de influencia en el consumo, conectado con la unidad de procesamiento, y que al menos en el segundo modo de servicio está mandado por la unidad de procesamiento, estando realizado el mismo en forma de un interruptor 3.2 para influir en el consumo del primer bien de consumo mediante bloqueo del consumo. Mediante este interruptor 3.2 puede procederse al bloqueo del consumo al llegar a cumplirse determinadas condiciones, por ejemplo quedarse por debajo de un saldo determinado, sobrepasar un marco de crédito determinado o sobrepasar un valor de consumo determinado. Está previsto que se inicie a tiempo, antes de llegar a cumplirse esta condición, una de las rutinas de notificación arriba descritas, para informar al consumidor del bloqueo inminente.

El criterio de conmutación puede ser predeterminado o modificado mediante acceso mediante el primer dispositivo de interfaz 7 a la segunda memoria 11, para poder influir en el criterio de conmutación o para poder reaccionar a circunstancias cambiadas.

El módulo de seguridad 4 comprende además un módulo de acuse de recibo 12 conectado con la unidad de procesamiento 5 con una tercera memoria 12.1. La unidad de procesamiento 5 crea un primer acuse de recibo para cada acceso al módulo de seguridad 4 accediendo al módulo de acuse de recibo 12. En particular, se crea un acuse de recibo para cada acceso a la primera memoria 6. La unidad de procesamiento 5 almacena el primer acuse de recibo posteriormente en la tercera memoria 12.1. De este modo se documenta el acceso al módulo de seguridad 4 y puede ser evaluado, dado el caso, en un momento posterior.

También aquí se realiza nuevamente un almacenamiento asegurado contra accesos no autorizados del acuse de recibo, así como el aseguramiento del acuse de recibo mediante medios criptográficos, como ya se han descrito anteriormente en detalle, de modo que aquí sólo se remite a las explicaciones anteriormente descritas.

La unidad de procesamiento almacena el acuse de recibo en la segunda memoria 12.1 de forma vinculada a un identificador de acceso característico para el usuario que accede. Este identificador del usuario que accede es una segunda firma digital del usuario que accede que se genera en la información del acuse de recibo. De este modo pueden asignarse las modificaciones realizadas en el marco de accesos de este tipo en la disposición 1, en particular en el módulo de seguridad 4 a distintos usuarios que acceden.

El acuse de recibo es provisto además de un cronomarcador y se almacena. Para ello, la unidad de procesamiento accede al módulo de detección de tiempo 10 y genera un identificador del tiempo de acceso característico para el tiempo del acceso que se vincula al acuse de recibo. También aquí vuelven a tomarse las mismas medidas, en particular las mismas medidas de seguridad como se han descrito ya anteriormente en relación con el identificador del tiempo de detección. De este modo, el identificador del tiempo de detección se integra en la segunda firma digital.

El módulo de seguridad 4 presenta para la selección de un proveedor del primer bien de consumo un módulo de selección 13 conectado con la unidad de procesamiento 5. La unidad de procesamiento 5 almacena el primer valor de consumo en la primera memoria 6, en este caso vinculado al identificador de proveedor característico para el proveedor seleccionado del primer bien de consumo. De este modo es posible seleccionar un proveedor determinado según unos criterios determinados y asignar a este proveedor los valores de consumo determinados, para facturarlos por ejemplo posteriormente a nombre de este proveedor.

El consumidor puede seleccionar mediante la segunda interfaz 9 a elección un proveedor de corriente determinado, al que se asignan de la forma descrita los valores de consumo detectados tras la selección. También aquí está nuevamente previsto que la unidad de procesamiento 5 asegure el identificador del proveedor integrándolo en la primera firma digital en el valor de consumo correspondiente. Como alternativa puede realizarse una cuarta firma digital separada en el identificador del proveedor.

Para la selección, la unidad de procesamiento 5 comprueba un criterio de selección y selecciona un proveedor en función del resultado de esta comprobación, estando almacenado el criterio de selección en una cuarta memoria 13.1 del módulo de selección 13. Como se ha mencionado anteriormente, este criterio de selección puede ser predeterminado por un usuario mediante la selección de un procedimiento. Como alternativa, el consumidor también puede seleccionar un modo con el que se minimizan los costes de consumo. Aquí se selecciona mediante comparación de tablas de tasas almacenadas en la cuarta memoria 13.1 de distintos proveedores aquel proveedor que ofrece el bien de consumo en el momento actual al precio más favorable. Esta consulta puede realizarse en intervalos predeterminados. Además, puede estar prevista tanto una actualización de las tablas de tasas iniciada regularmente por la unidad de procesamiento 5 como una actualización regular por parte de los proveedores, que llegan mediante una conexión de comunicación correspondiente a la unidad de procesamiento 5.

Para poder entender también en un momento posterior la selección por parte del consumidor, está previsto que la unidad de procesamiento 5 deposite el primer valor de consumo en la primera memoria 6 vinculado al identificador de usuario característico para el usuario que selecciona. También aquí pueden volver a usarse los mecanismos de aseguramiento arriba descritos. También aquí vuelve a estar previsto que la unidad de procesamiento 5 asegure el identificador del usuario integrándolo en la primera firma digital en el valor de consumo correspondiente. Como alternativa puede realizarse una quinta firma digital separada en el identificador del usuario.

El primer dispositivo de detección 3 y el módulo de seguridad 4 están dispuestos en un entorno seguro 14 protegido contra accesos no autorizados, para impedir eficazmente accesos no autorizados no sólo a los datos del módulo de seguridad 4 sino también a los datos que se suministran de y al primer dispositivo de detección 3.

El entorno seguro 14 está realizado, por un lado, de forma física mediante carcasas seguras del primer dispositivo de detección 3 y del módulo de seguridad 4, que están provistos de medios sobradamente conocidos para la detección de manipulaciones en la carcasa. Por otro lado, se realiza de forma lógica mediante un protocolo de comunicación correspondientemente asegurado entre el primer dispositivo de detección 3 y el módulo de seguridad 4. Así, en cada comunicación entre el primer dispositivo de detección 3 y el módulo de seguridad 4 se establece un canal de comunicación asegurado mediante un autentificación mutua correspondientemente fuerte. Se entiende que el primer dispositivo de detección 3 dispone para ello de medios de comunicación correspondientes, que ponen a disposición las funcionalidades de seguridad descritas.

La Figura 2 muestra un diagrama de bloques de una forma de realización preferible del sistema según la invención con la disposición 1 según la invención de la Figura 1 y un centro de datos 15 remoto.

El primer dispositivo de interfaz 7 del módulo de seguridad 4 está realizado como primer dispositivo de comunicación. Además, el centro de datos 15 presenta un segundo dispositivo de comunicación 16. Mediante el primer dispositivo de comunicación 7 y el segundo dispositivo de comunicación 16 puede establecerse una primera conexión de comunicación entre el módulo de seguridad 4 y el centro de datos 15. De este modo es posible acceder desde el centro de datos remoto a la disposición 1, en particular al módulo de seguridad 4, leer los primeros valores de consumo almacenados y procesarlos en el centro de datos 15. Con una autorización de acceso correspondiente naturalmente también es posible influir a través del centro de datos 15 en el comportamiento de la disposición 1, como ya se ha descrito anteriormente.

El entorno seguro 14 se ha extendido en el ejemplo mostrado mediante un protocolo de comunicación correspondientemente asegurado entre el primer dispositivo de comunicación 7 y el segundo dispositivo de comunicación 16 al centro de datos 15. Un protocolo de comunicación de este tipo ya se ha descrito anteriormente en relación con la comunicación entre el módulo de seguridad 4 y el dispositivo de detección 3, de modo que aquí sólo se remite a las explicaciones anteriormente expuestas.

El centro de datos 15 almacena los datos de consumo leídos y los tiene preparados para el procesamiento posterior. El procesamiento puede realizarse en otro centro de datos remoto, por ejemplo del proveedor del bien de consumo correspondiente, al que se transmiten a continuación los datos de consumo. En el ejemplo mostrado, el centro de datos 15 procesa por su cuenta estos datos de consumo leídos.

La facturación del consumo se realiza mediante el centro de datos 15. El centro de datos 15 genera en función de los contenidos de memoria de la primera memoria una información de facturación, que se comunica al consumidor de la forma habitual. En el caso de consumidores que participan en un procedimiento de adeudo en cuenta, el centro de datos 15 está conectado directamente con los bancos 17.1 y 17.2 correspondientes de los consumidores correspondientes.

El centro de datos 15 puede ser operado por el proveedor de corriente. No obstante, se entiende que el centro de datos 15 también puede ser operado por un tercero, que pone estos servicios de facturación al servicio del proveedor de corriente.

Como ya se ha mencionado anteriormente, en caso de una autorización de acceso correspondiente, está previsto que mediante el centro de datos 15 se influya en el comportamiento de la disposición 1. El centro de datos especifica

en este caso el criterio de conmutación arriba descrito o lo cambia.

Entre otras cosas está previsto que, al llegar a cumplirse unas condiciones determinadas, el centro de datos 15 impide el consumo de corriente. Al emplearse el sistema en un llamado sistema de prepago o sistema prepaid, esto puede ser el caso cuando el saldo se queda por debajo de un saldo mínimo determinado. Para ello puede estar previsto en combinación con la disposición 1 que el consumo de corriente quede bloqueado mediante el interruptor 3.2.
El criterio de conmutación es cuando se constata que el saldo actual, almacenado en la segunda memoria 12.1, queda por debajo de un límite de saldo almacenado en el centro de datos 15. En cuanto se detecte en el centro de datos 15 que ha llegado a cumplirse esta condición, éste envía un comando de conmutación correspondiente al módulo de seguridad 4.

Como ya se ha descrito anteriormente en relación con la disposición 1, también aquí puede estar implementada una rutina de preaviso correspondiente, que avisa al consumidor a tiempo antes del bloqueo. El consumidor tiene, además, una posibilidad para evitar o impedir de forma sencilla y rápida el bloqueo. El centro de datos presenta para ello un tercer dispositivo de comunicación 18, mediante el cual puede establecerse una segunda conexión de comunicación para cambiar el saldo actual almacenado en la segunda memoria 12.1. Puede estar previsto, por ejemplo, un pago exprés por móvil mediante servicios correspondientes o algo similar.

En el centro de datos 15 se almacenan y procesan además de los valores de consumo entre otros también todos los demás datos generados en el módulo de seguridad 4. En particular, se almacenan para posteriores pruebas para la selección de un proveedor los identificadores de selección y los identificadores de usuarios vinculados a la selección y, dado el caso, se procesan posteriormente.

En caso de un fallo de larga duración de la conexión de comunicación entre uno de los centros de datos 15, 19 y el módulo de seguridad 4, los datos almacenados en la primera memoria también pueden ser leídos localmente. Para ello puede conectarse un aparato lector 26 mediante una interfaz correspondiente con el módulo de seguridad 4. También aquí se realiza naturalmente de nuevo una comprobación correspondiente de la autorización de acceso.

La Figura 3 muestra un diagrama de bloques de otra forma de realización preferible del sistema según la invención con la disposición 1 según la invención, cuyo módulo de seguridad 4 está conectado con dos centros de datos 15 y 19 remotas.

La disposición 1 sólo se ha ampliado con un segundo dispositivo de detección 20 conectado con el módulo de seguridad 4 y un tercer dispositivo de detección 21 también conectado con el módulo de seguridad 4, que están dispuestos ambos en el entorno seguro 14. El primer dispositivo de detección 3 y el segundo dispositivo de detección 20 detectan el consumo de corriente en viviendas separadas de una casa, mientras que el tercer dispositivo de detección 21 detecta de forma central el consumo de gas de una calefacción central de la casa.

Los valores de consumo detectados se almacenan en la primera memoria 6 del módulo de seguridad 4. A los valores de consumo se vinculan entre otras cosas un identificador del dispositivo de detección para el dispositivo de detección en cuestión, es decir, el consumidor correspondiente y se vincula un identificador del bien de consumo para el bien de consumo correspondiente. Estos datos se aseguran además de forma criptográfica del modo ya anteriormente descrito mediante la integración en una primera firma digital en estos datos.

Los valores de consumo de corriente de las dos viviendas se transmiten al primer centro de datos 15 y se procesan y facturan allí de la forma anteriormente descrita. Los valores de consumo de gas se transmiten al segundo centro de datos 19, se procesan allí y se envían a un tercer centro de datos 22 del proveedor de gas, que factura a continuación el consumo, estando conectado el tercer centro de datos 22 dado el caso directamente con un banco 23 del consumidor.

El módulo de seguridad 4 y el primer centro de datos 15 se encuentran en un entorno seguro 24, que se ha creado entre otras cosas mediante un protocolo de comunicación correspondientemente seguro entre el módulo de seguridad 4 y el primer centro de datos 15. La comunicación se realiza en este caso mediante una línea fija 24.1.

El módulo de seguridad 4 y el segundo centro de datos 19 se encuentran también en un entorno seguro 25, que se ha creado también aquí entre otras cosas mediante un protocolo de comunicación correspondientemente seguro entre el módulo de seguridad 4 y el segundo centro de datos 19. La comunicación se realiza en este caso mediante una comunicación por radio 25.1

La Figura 4 muestra un diagrama de bloque de otra forma de realización preferible del sistema según la invención con una disposición 1' según la invención, cuyo módulo de seguridad 4' está conectado con un centro de datos 15' remoto. La estructura básica y el funcionamiento del sistema corresponden al de la Figura 2, de modo que aquí se hablará sólo de las diferencias.

Una diferencia está en que el valor de consumo a detectar es una información de lugar. El dispositivo de medición

del dispositivo de detección 3' móvil es, por lo tanto, un módulo GPS 3.1', que asume al mismo tiempo la función de un módulo de detección de tiempo y que suministra al módulo de seguridad 4 datos de posición acoplados a un tiempo de detección. El módulo de seguridad 4' procesa estos datos de la forma anteriormente descrita y los suministra al centro de datos 15', que realiza la facturación.

Gracias a un protocolo de comunicación correspondientemente asegurado, el dispositivo de detección 3' y el módulo de seguridad 4' están dispuestos en un entorno seguro 14'. Lo mismo es válido para el módulo de seguridad 4' y el centro de datos 15', que están dispuestos en un entorno seguro 24'.

En el ejemplo mostrado, también el módulo de seguridad 4' está realizado de forma móvil, por lo que está prevista una línea de datos fija 14.1' entre el módulo de seguridad 4' y el módulo GPS 3.1', mientras que la comunicación entre el módulo de seguridad 4' y el centro de datos 15' se realiza mediante una comunicación por radio 24.1'. No obstante, se entiende que en otras variantes de la invención también puede estar previsto un módulo de seguridad estacionario, que comunica en este caso mediante una comunicación por radio correspondiente con el dispositivo de detección móvil, como se indica en la Figura 4 mediante la flecha 14.2' de trazo interrumpido.

Con un dispositivo de este tipo pueden facturarse, por ejemplo, los kilómetros recorridos de un coche de alquiler o similares. También pueden facturarse con el mismo los peajes para carreteras de peaje etc.

La Figura 5 muestra un diagrama de bloques de otra forma de realización preferible del sistema según la invención con una disposición 1" según la invención y un centro de datos 15" remoto. El sistema se emplea en el marco del control de calidad en un supermercado.

La disposición 1" comprende un módulo de seguridad 4", que está conectado con un primer dispositivo de detección 3" y un segundo dispositivo de detección 20". El primer dispositivo de detección 3" detecta como primera magnitud de detección un primer parámetro de servicio de un primer dispositivo de servicio en forma de un arcón congelador 27 en la sala de venta de un supermercado. El primer parámetro de servicio es la temperatura en el interior del arcón congelador 27. El segundo dispositivo de detección 20" detecta como segunda magnitud de detección un segundo parámetro de servicio de un segundo dispositivo de servicio en forma de unas estanterías refrigeradas 28 en la sala de venta del supermercado. El primer parámetro de servicio es la temperatura en el interior de las estanterías refrigeradas 28.

El módulo de seguridad 4", el primer dispositivo de detección 3", el segundo dispositivo de detección 20" y el centro de datos 15" están dispuestos a su vez en un entorno seguro 14", que están realizados además de carcasas correspondientemente seguras de los distintos componentes mediante un protocolo de comunicación correspondientemente seguro entre los distintos componentes.

Los primeros y segundos parámetros de servicio detectados se almacenan en la primera memoria 6" del módulo de seguridad 4". A los parámetros de servicio se vincula entre otras cosas un identificador del dispositivo de detección para el dispositivo de detección en cuestión, es decir, el dispositivo de servicio correspondiente, y un identificador de la magnitud de detección para la magnitud de detección correspondiente, es decir, el parámetro de servicio. Estos datos se aseguran además del modo anteriormente descrito de forma criptográfica mediante integración en una primera firma digital en estos datos.

Los valores de detección de los dos dispositivos de servicio se transmiten al centro de datos 15" y se almacenan o procesan allí. Por ejemplo, pueden ser usados posteriormente para probar que la temperatura en el interior del arcón congelador 27 o de las estanterías refrigeradas 28 estaban siempre por debajo de las temperaturas legalmente prescritas.

El módulo de seguridad 4" comprueba además continuamente si los valores de temperatura detectados están situados por debajo de unos valores límite predeterminados. A tiempo antes de quedar la temperatura por encima de los valores límite correspondientes, se inicia una rutina de notificación correspondiente, que avisa por ejemplo al personal del supermercado de que la temperatura está por encima de los valores límite. Además, está previsto que en este caso se influya mediante un dispositivo de influencia correspondiente del dispositivo de detección en cuestión en los parámetros de servicio, iniciándose por ejemplo mediante una conexión correspondiente con el grupo frigorífico del arcón congelador 27 o de las estanterías refrigeradas 28 un aumento de la potencia frigorífica.

REIVINDICACIONES

1. Disposición para la detección y el almacenamiento asegurado de al menos un primer valor de detección de al menos una primera magnitud de detección con

- al menos un primer dispositivo de detección (3; 3'; 3") para la detección del primer valor de detección y
- un dispositivo de seguridad (4; 4'; 4") conectado con el primer dispositivo de detección (3; 3'; 3"), que comprende una unidad de procesamiento (5), una primera memoria (6; 6") conectada con la misma, así como un primer dispositivo de interfaz (7) conectado con la unidad de procesamiento (5),
- estando realizado el dispositivo de seguridad (4, 4'; 4") para el almacenamiento asegurado contra accesos no autorizados del primer valor de detección en la primera memoria (6; 6"),
- estando realizado el primer dispositivo de interfaz (7) para acceder al dispositivo de seguridad (4; 4'; 4"),
- comprendiendo el primer dispositivo de detección (3; 3'; 3") una unidad de detección (3.1; 3.1') conectada con el dispositivo de seguridad (4; 4'; 4") que está realizado para la detección continua de la primera magnitud de detección, y
- estando realizada la unidad de procesamiento (5) para la comprobación de la autorización de acceso al dispositivo de seguridad (4; 4'; 4"),

caracterizada porque

- el primer dispositivo de detección (3; 3'; 3") es un dispositivo de medición de consumo, la primera magnitud de detección es el consumo de un primer bien de consumo en forma de un primer portador de energía, así como el primer valor de detección es un primer valor de consumo del primer portador de energía y
- el dispositivo de seguridad (4) presenta un módulo de selección (13) conectado con la unidad de procesamiento (5), que está realizado para la comprobación de un criterio de selección y para la selección de un proveedor del primer bien de consumo de una pluralidad de proveedores en función del resultado de la comprobación del criterio de selección, y
- la unidad de procesamiento (5) está realizada para el almacenamiento del primer valor de consumo en la primera memoria (6) vinculado al identificador de proveedor característico para el proveedor seleccionado del primer bien de consumo.

2. Disposición de acuerdo con la reivindicación 1, **caracterizada porque** la unidad de procesamiento (5) está realizada para la comprobación de la autorización de acceso mediante del uso de medios criptográficos.

3. Disposición de acuerdo con la reivindicación 1 o 2, **caracterizada porque** la unidad de procesamiento (5) está realizada para el almacenamiento del primer valor de detección en la primera memoria (6; 6") vinculado a un identificador del tiempo de detección característico para el tiempo de detección del primer valor de detección.

4. Disposición de acuerdo con una de las reivindicaciones anteriores, **caracterizada porque**

- está previsto al menos un segundo dispositivo de detección (20; 20") diferente del primer dispositivo de detección (3; 3'; 3") en forma de un dispositivo de medición de consumo para la detección de al menos un segundo valor de detección de la primera magnitud de detección diferente del primer valor de detección y
- el dispositivo de seguridad (4; 4") está realizado para el almacenamiento asegurado contra accesos no autorizados del segundo valor de detección en la primera memoria (6; 6").

5. Disposición de acuerdo con una de las reivindicaciones anteriores, **caracterizada porque**

- o bien el primer dispositivo de detección está realizado para la detección de al menos un valor de detección de una segunda magnitud de detección
- o bien está previsto al menos un tercer dispositivo de detección (21) para la detección de al menos un valor de detección de una segunda magnitud de detección,
- siendo la segunda magnitud de detección el consumo de un segundo bien de consumo en forma de un segundo portador de energía diferente del primer portador de energía, siendo además el valor de detección de la segunda magnitud de detección un valor de consumo del segundo portador de energía,
- y estando realizado el dispositivo de seguridad (4) para el almacenamiento asegurado contra accesos no autorizados del valor de detección de la segunda magnitud de detección en la primera memoria (6).

6. Disposición de acuerdo con una de las reivindicaciones anteriores, **caracterizada porque** la unidad de procesamiento (5) presenta al menos un primer modo de servicio así como un segundo modo de servicio y está realizada para la conmutación entre el primero y el segundo modo de servicio en respuesta a un comando de conmutación.

7. Disposición de acuerdo con la reivindicación 6, **caracterizada porque** está previsto un dispositivo de influencia (3.2) conectado con la unidad de procesamiento (5) y mandada al menos en el segundo modo de servicio por la unidad de procesamiento (5) para influir en la primera magnitud de detección.

8. Disposición de acuerdo con una de las reivindicaciones anteriores, **caracterizada porque** el dispositivo de seguridad (4) comprende un módulo de acuse de recibo (12) conectado con la unidad de procesamiento con una memoria (12.1) y la unidad de procesamiento (5) está realizada para generar un acuse de recibo para un acceso al dispositivo de seguridad (4) y para almacenar el primer acuse de recibo en la memoria (12.1) del módulo de acuse de recibo (12).

9. Disposición de acuerdo con la reivindicación 8, **caracterizada porque** la unidad de procesamiento (5)

- está realizada para el almacenamiento del acuse de recibo en la memoria (12.1) del módulo de acuse de recibo (12) vinculado al identificador del usuario que accede característico para el usuario que accede

y/o

- está realizada para el almacenamiento del acuse de recibo en la memoria (12.1) del módulo de acuse de recibo (12) vinculado al identificador del tiempo de acceso característico para el tiempo de acceso.

10. Disposición de acuerdo con la reivindicación 8 o 9, **caracterizada porque** la unidad de procesamiento (5) está realizada para asegurar el acuse de recibo almacenado y/o el identificador del usuario que accede y/o el identificador del tiempo de acceso mediante medios criptográficos.

11. Disposición de acuerdo con una de las reivindicaciones anteriores, **caracterizada porque** la unidad de procesamiento (5) está realizada para proteger el identificador del proveedor mediante medios criptográficos.

12. Disposición de acuerdo con la reivindicación 11, **caracterizada porque** la unidad de procesamiento (5) está realizada para el almacenamiento del primer valor de consumo en la primera memoria (6) vinculado al identificador de usuario característico para el usuario que realiza la selección.

13. Disposición de acuerdo con una de las reivindicaciones anteriores, **caracterizada porque** el dispositivo de seguridad (4; 4'; 4") comprende un módulo criptográfico (8) conectado con la unidad de procesamiento (5), que está realizado para poner a disposición de la unidad de procesamiento medios criptográficos para al menos una aplicación de seguridad usándose al menos primeros datos criptográficos, estando almacenados los primeros datos criptográficos en una memoria (8.1) del módulo criptográfico y comprendiendo un primer algoritmo criptográfico.

14. Disposición de acuerdo con una de las reivindicaciones anteriores, **caracterizada porque** el primer dispositivo de detección (3; 3'; 3") y el dispositivo de seguridad (4; 4'; 4") están dispuestos en un entorno seguro (14; 14'; 14") protegido contra accesos no autorizados.

15. Disposición de acuerdo con una de las reivindicaciones anteriores, **caracterizada porque** el dispositivo de seguridad (4; 4'; 4") presenta al menos un primer dispositivo de interfaz (7) conectado con la unidad de procesamiento (5) para acceder al dispositivo de seguridad (4; 4'; 4"), que está realizado como primer dispositivo de comunicación y por que está previsto un centro de datos (15, 19; 15'; 15") remoto del dispositivo de seguridad (4; 4'; 4") con un segundo dispositivo de comunicación (16), estando realizados el primer dispositivo de comunicación (7) y el segundo dispositivo de comunicación (18) para establecer una primera conexión de comunicación entre el dispositivo de seguridad (4; 4'; 4") y el centro de datos (15, 19; 15'; 15").

16. Disposición de acuerdo con la reivindicación 15, **caracterizada porque** el centro de datos (15, 19; 15'; 15")

- está realizado para leer los contenidos de memoria de la primera memoria (6; 6") mediante la primera conexión de comunicación y/o
- para generar la información de facturación en función de los contenidos de memoria de la primera memoria (6; 6") y/o
- para influir en el modo de servicio de la unidad de procesamiento (5).

17. Procedimiento para la detección y el almacenamiento asegurado de al menos un primer valor de detección de al menos una primera magnitud de detección, en el que

- la primera magnitud de detección se detecta de forma continua y el primer valor de detección se almacena en un dispositivo de seguridad (4; 4'; 4"),
- almacenándose el primer valor de detección en una primera memoria (6; 6") del dispositivo de seguridad (4; 4'; 4") de forma asegurada contra accesos no autorizados y
- realizándose en caso de un acceso del dispositivo de seguridad (4; 4'; 4") mediante un primer dispositivo de interfaz (7) una comprobación de la autorización de acceso al dispositivo de seguridad (4; 4'; 4"),

caracterizado porque

- la primera magnitud de detección es el consumo de un primer bien de consumo en forma de un primer portador

de energía y el primer valor de detección es un primer valor de consumo del primer portador de energía,
- se comprueba un criterio de selección y se selecciona en función del resultado de la comprobación del criterio de selección un proveedor del primer bien de consumo de una pluralidad de proveedores y
- el primer valor de consumo se almacena en la primera memoria (6) de forma vinculada a un identificador de proveedor característico para el proveedor seleccionado del primer bien de consumo.

18. Procedimiento de acuerdo con la reivindicación 17, **caracterizado porque** la comprobación de la autorización de acceso se realiza mediante el uso de medios criptográficos.

19. Procedimiento de acuerdo con la reivindicación 17 o 18, **caracterizado porque** el primer valor de detección se almacena en la primera memoria (6; 6”) de forma vinculada a un identificador del tiempo de detección característico para el tiempo de detección del primer valor de detección.

20. Procedimiento de acuerdo con una de las reivindicaciones 17 a 19, **caracterizado porque** se detecta al menos un segundo valor de detección de la primera magnitud de detección diferente del primer valor de detección y se almacena en la primera memoria (6; 6”) de forma asegurada contra accesos no autorizados.

21. Procedimiento de acuerdo con una de las reivindicaciones 17 a 20, **caracterizado porque**

- se detecta al menos un valor de detección de una segunda magnitud de detección y se almacena en la primera memoria (6) de forma asegurada contra accesos no autorizados,
- siendo la segunda magnitud de detección el consumo de un segundo bien de consumo en forma de un segundo portador de energía diferente del primer portador de energía, y siendo el valor de detección de la segunda magnitud de detección un valor de consumo del segundo portador de energía.

22. Procedimiento de acuerdo con una de las reivindicaciones 17 a 21, **caracterizado porque** el dispositivo de seguridad (4; 4’; 4”) presenta al menos un primer modo de servicio, así como un segundo modo de servicio y se conmuta entre el primero y el segundo modo de servicio en respuesta a un comando de conmutación.

23. Procedimiento de acuerdo con una de las reivindicaciones 17 a 22, **caracterizado porque** se genera un acuse de recibo para un acceso al dispositivo de seguridad (4) y se almacena el acuse de recibo en el dispositivo de seguridad (4).

24. Procedimiento de acuerdo con una de las reivindicaciones 17 a 23, **caracterizado porque** el identificador del proveedor se protege mediante medios criptográficos.

25. Procedimiento de acuerdo con la reivindicación 24, **caracterizado porque** el primer valor de consumo se almacena en la primera memoria (6) de forma vinculada a un identificador de usuario característico para el usuario que realiza la selección.

26. Procedimiento de acuerdo con una de las reivindicaciones 17 a 25, **caracterizado porque** entre el dispositivo de seguridad (4; 4’; 4”) y un centro de datos (15, 19; 15’; 15”) remoto del dispositivo de seguridad (4; 4’; 4”) se establece una primera conexión de comunicación y el centro de datos (15, 19; 15’; 15”) lee los contenidos de memoria de la primera memoria (6; 6”) mediante la primera conexión de comunicación.

27. Procedimiento de acuerdo con la reivindicación 26, **caracterizado porque** el centro de datos (15, 19; 15’; 15”)

- genera una información de facturación en función de los contenidos de memoria de la primera memoria (6; 6”) y/o
- influye en el modo de servicio del dispositivo de seguridad (4; 4’; 4”).

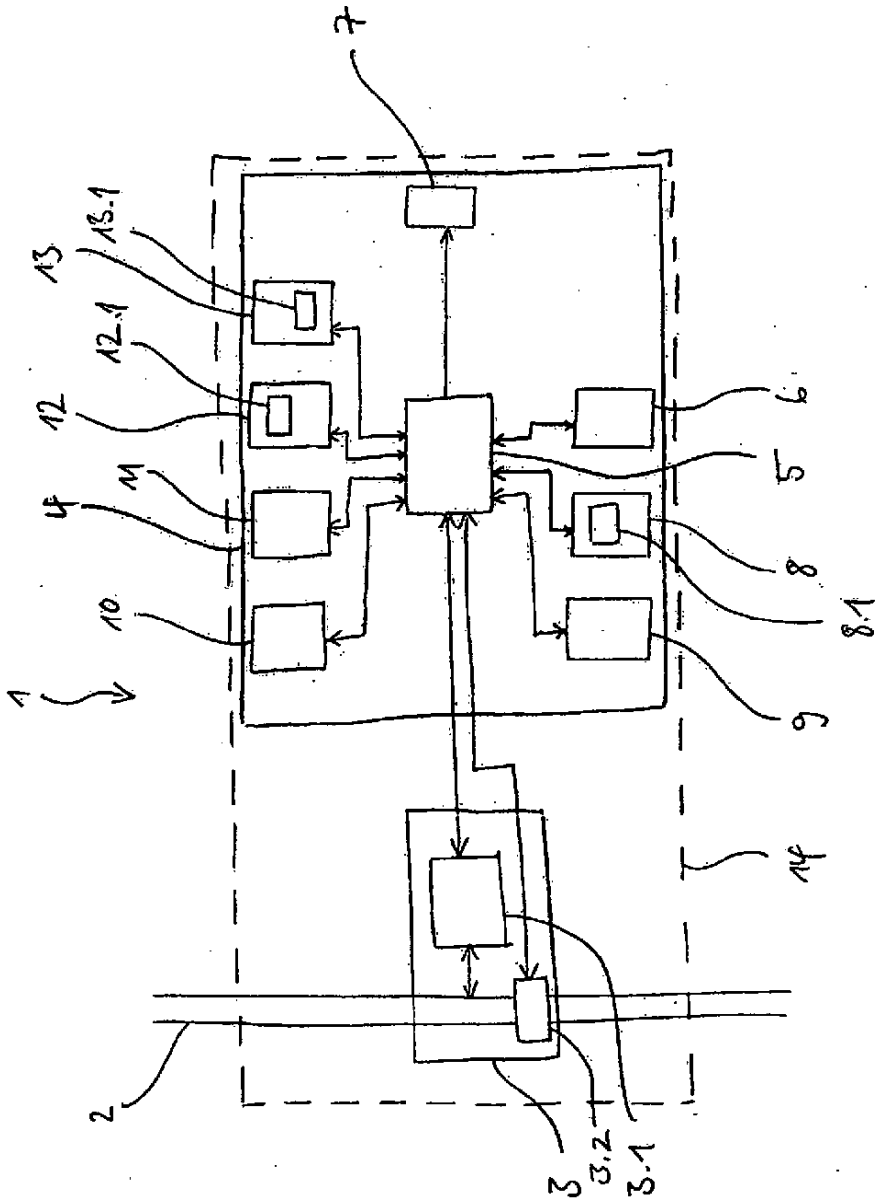

Fig. 1

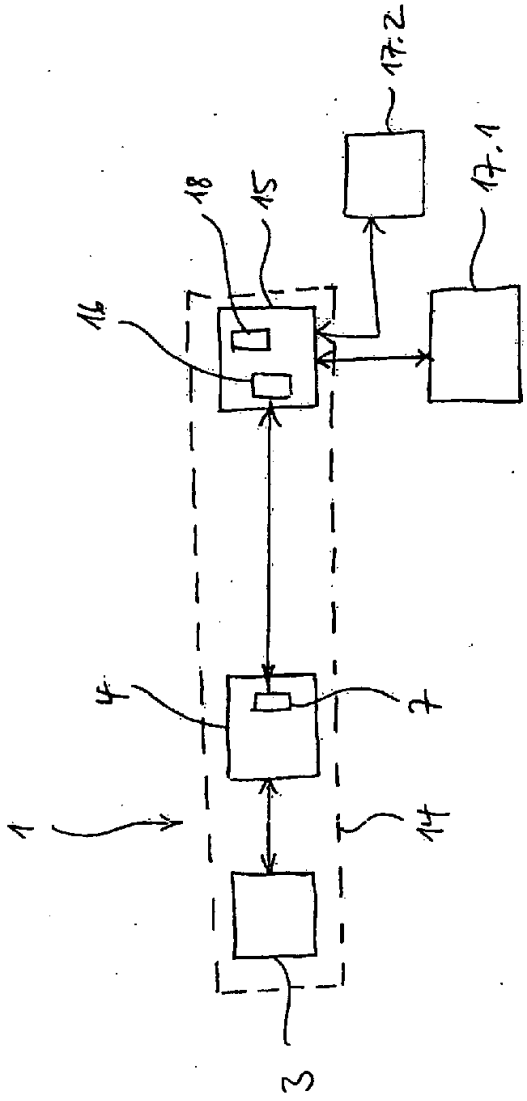

Fig. 2

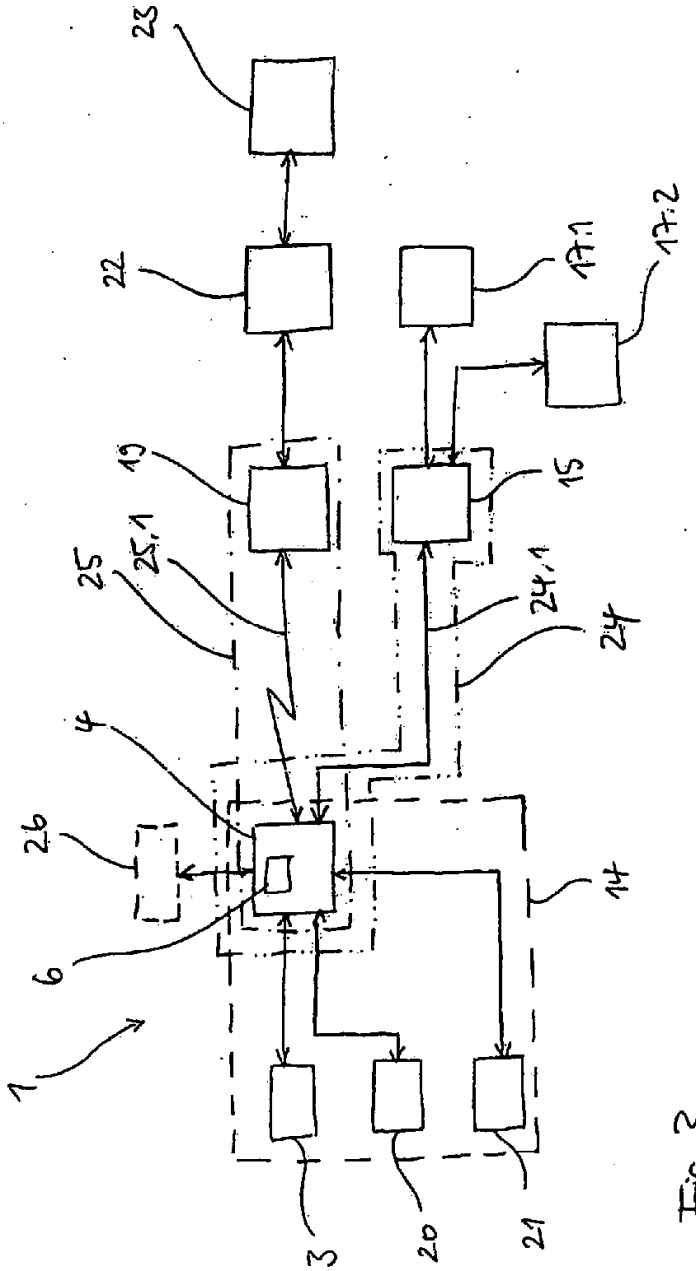

Fig. 3

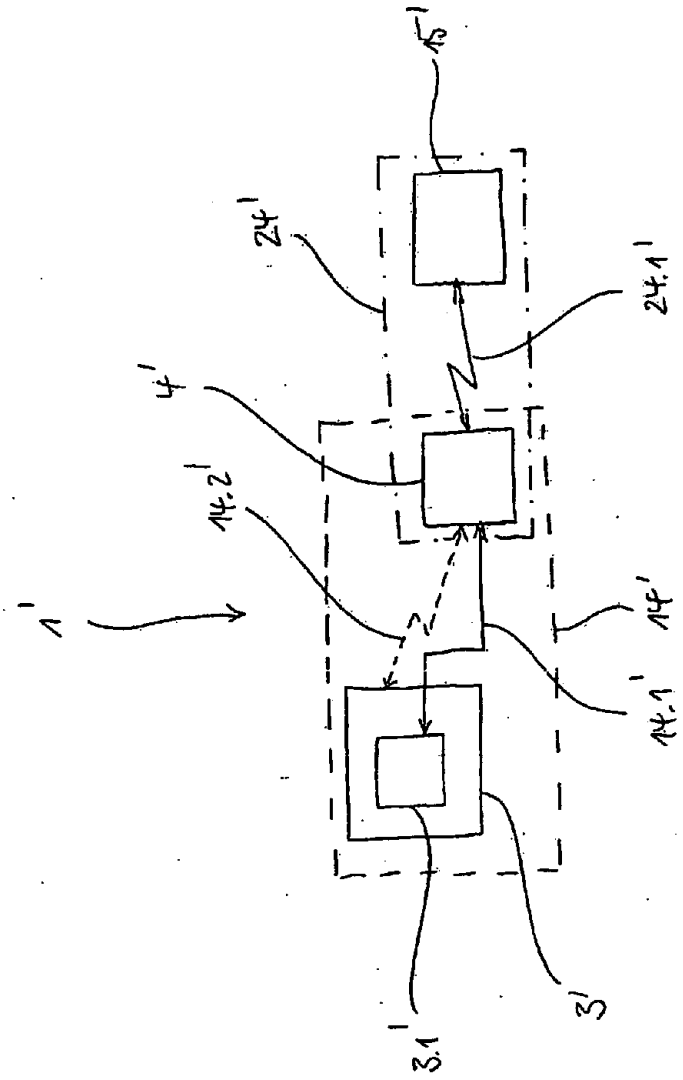

Fig. 4

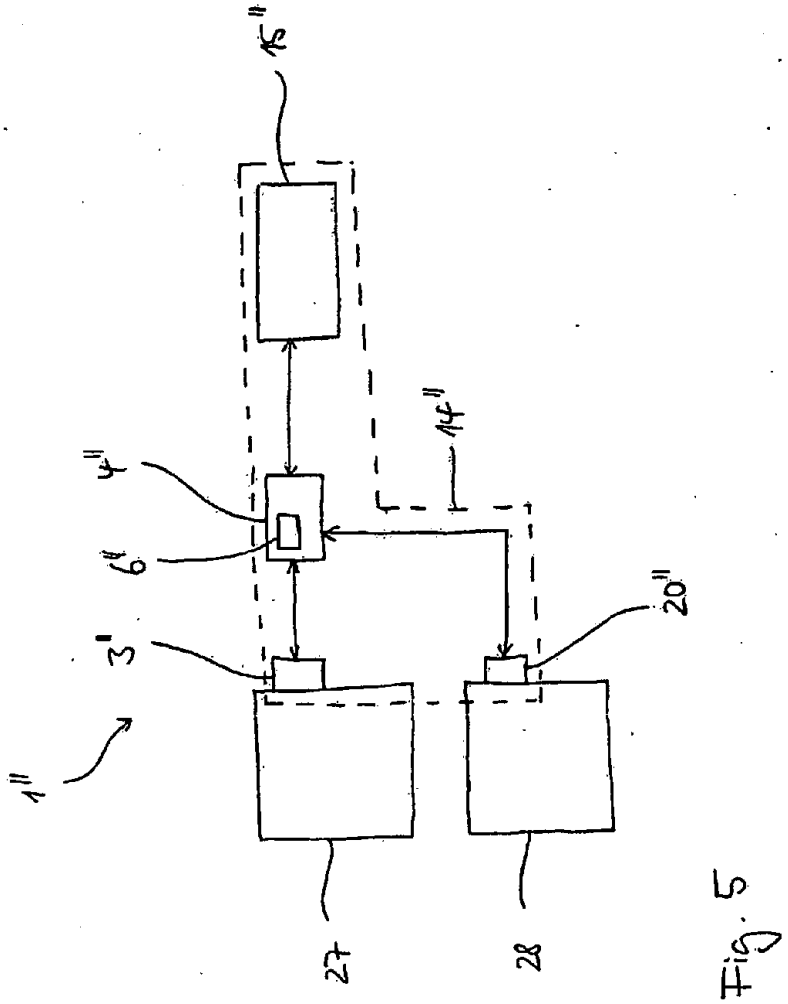

Fig. 5