(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 542 087**

(51) Int. CI.:

B60L 11/18 (2006.01)
G07F 15/00 (2006.01)
G06Q 20/38 (2012.01)
H04L 29/06 (2006.01)
G06Q 20/32 (2012.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.06.2012 E 12731320 (3)**

(97) Fecha y número de publicación de la concesión europea: **22.04.2015 EP 2755846**

(54) Título: **Procedimiento y dispositivo para asignar un valor de medición registrado por una estación de carga a una transacción**

(30) Prioridad:

15.09.2011 DE 102011113354

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.07.2015

(73) Titular/es:

RWE AG (100.0%)
Opernplatz 1
45128 Essen, DE

(72) Inventor/es:

GAUL, ARMIN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Procedimiento y dispositivo para asignar un valor de medición registrado por una estación de carga a una transacción

El objeto se refiere a un procedimiento y a un dispositivo para asignar un valor de medición registrado por una estación de carga a un identificador de transacción.

Probablemente, la distribución de vehículos de accionamiento eléctrico aumentará rápidamente en el futuro próximo. Sin embargo, con la distribución de vehículos eléctricos que se accionan con un motor eléctrico se debería asegurar que éstos se pueden alimentar de la manera más sencilla con energía. Para ello se debería proporcionar una infraestructura que funcione.

En particular se debería proporcionar la posibilidad de recibir energía para vehículos eléctricos en zonas públicas. En el caso de los alcances disponibles hasta el momento de vehículos eléctricos de entre 50 y algunos 100 km es conveniente que también fuera del entorno doméstico sea posible una carga de los vehículos. Para ello se deberían proporcionar estaciones de carga en zonas públicas para proporcionar una disponibilidad constante de energía para vehículos eléctricos mediante una red de alimentación. Esta disponibilidad de energía eléctrica o de estaciones de carga es un criterio significativo de la aceptación de vehículos eléctricos.

Sin embargo, en el caso de estaciones de carga instaladas en zonas públicas se debe asegurar que el cliente paga energía recibida. También se debería asegurar que el cliente conoce los costes esperados antes de recibir energía eléctrica. De manera correspondiente al proceso de repostaje convencional, el cliente debería saber directamente antes de la carga de la batería qué costes le están esperando. Así, por ejemplo, el cliente debería conocer el precio de un kilovatio-hora. Además, debería estar asegurado que se le factura al cliente realmente sólo la cantidad de energía que haya recibido. Finalmente, debe estar asegurado que el cliente sólo paga por procesos de repostaje que realmente haya efectuado. Se debe evitar de manera segura que datos de medición de procesos de repostaje individuales se facturen de manera paralela a varios clientes.

En particular, en el caso de la movilidad eléctrica se realizan procesos de carga por los clientes más diversos en la misma estación de carga. Los procesos de carga no están controlados permanentemente ni por el operador del punto de medición ni por el cliente de modo que se debe asegurar que los valores de medición registrados por la estación de carga o por el aparato de medición en la estación de carga se transmiten a una centralita de contabilización sin falsificar y de forma que se pueden asignar de forma unívoca a un cliente.

Por tanto, cabe tener en cuenta especialmente la integridad, la autenticidad, la comprobabilidad y la posibilidad de asignación de los datos de contabilización transmitidos entre el vehículo y la estación de carga y/o entre la estación de carga y la centralita de contabilización. Por un lado, es necesario que los datos con respecto a la cantidad de energía permanezcan sin falsificar. Por otro lado, para fines de contabilización, una transmisión de datos de medición (datos de contabilización) de la estación de carga a un sistema de contabilización se debe proteger frente a manipulaciones. El usuario debe poder asegurar y comprobar que sólo se le factura la energía que haya recibido.

Sin embargo, esto resulta difícil en el caso de una contabilización anónima sin ninguna permanencia de contrato como, por ejemplo, en el caso de la gasolinera clásica. Por un lado, se debe asegurar que un usuario paga la energía recibida, por otro lado, tanto el usuario como el proveedor de energía se deben proteger frente a manipulaciones.

En Alemania, la comprobabilidad de valores de medición para estas contabilizaciones independientemente del procedimiento elegido está sujeta al derecho de calibración que protege tanto a consumidores como a comerciantes frente a estafadores al proporcionar bases de contabilización correctas.

Sin embargo, dado que se exigen tarifas variables en el tiempo para el suministro de corriente para poder acompañar una mayor alimentación desde fuentes regeneradoras con sistemas de incentivos monetarios se debe asegurar que el cliente conoce una tarifa variable.

Una tarifa variable en el tiempo sólo debe existir cuando se pueda representar en la indicación y, entonces, sea además muy fácilmente comprensible para el cliente. Sin embargo, dado que el proceso de carga tiene una duración muy larga, apenas se le puede exigir al cliente que espere en la columna de carga para observar cambios de tarifa. Además, la necesidad de la transparencia no sólo existe para el cliente sino también para el proveedor de energía de modo que, en el sentido del derecho de calibración, también el proveedor de energía tiene que tener una posibilidad de consultar los comprobantes, por lo que el derecho de calibración exige un almacenamiento asegurado según el derecho de calibración de los comprobantes para mediciones en las que no están presentes ambas partes. Los documentos US20100161482 y US 20090313104 dan a conocer procedimientos para la identificación de transacciones en la carga de un vehículo mediante una estación de carga de acuerdo con el estado de la técnica. Paquetes de datos que comprenden datos con respecto a la cantidad de energía alimentada y la identificación de vehículo se transmiten a una centralita de contabilización.

Por tanto, el objeto se basó en el objetivo de proporcionar un procedimiento y un dispositivo que proporcione a un cliente, preferiblemente anónimo, y al proveedor de energía una factura transparente y comprensible por cada proceso de venta, en particular cuando se debe facturar una tarifa variable en el tiempo. Este objetivo se consigue de acuerdo con el objeto mediante un procedimiento de acuerdo con la reivindicación 1 u 8 y un dispositivo de acuerdo con la reivindicación 13 o 14.

En el proceso de carga, el vehículo eléctrico recibe energía eléctrica de la estación de carga. En la estación de carga se mide esta energía eléctrica con ayuda de un aparato de medición (contador). Durante el proceso de carga y también al finalizar el proceso de carga es necesario que la cantidad de energía recibida se registre para fines de contabilización y que el usuario de la estación de carga conozca la cantidad de energía recibida. Por regla general, la medición en sí no se tendrá que reclamar, ya que ésta se realiza mediante un contador calibrado. Por tanto, sólo se tiene que asegurar que los valores de medición se alimentan de forma asegurada a la centralita de contabilización, debiendo estar garantizada una asignación infalsificable unívoca a una transacción. Por otro lado, también tiene que estar asegurado que el usuario también paga la energía recibida.

Se parte de que el cliente ha conocido de manera adecuada la posibilidad de usar una tarifa variable en el tiempo en la columna de carga y ha elegido intencionadamente a ésta.

En este caso, el usuario tiene que señalar su disposición de pago y proporcionar informaciones con respecto a un modo de pago para posibilitar una contabilización.

La disposición de pago se puede indicar, por ejemplo, al indicar el usuario mediante una tarjeta de crédito, una tarjeta de prepago, insertando dinero en la estación de carga, una llamada telefónica o similares que desea pagar la energía. Esta información de pago se puede obtener directamente en la estación de carga, por ejemplo, mediante un lector de tarjetas de crédito, o mediante teléfono, por ejemplo, mediante un número de teléfono o también un mensaje corto en el que, por ejemplo, se indica la IMSI (*International Mobile Subscriber Identification*, identificación de abonado móvil internacional). Mediante esta información que, por ejemplo, es anónima en el caso de una tarjeta de telefonía móvil de prepago, se puede realizar una contabilización, por ejemplo, mediante una factura de teléfono.

Si el usuario revela informaciones de pago en la estación de carga, entonces se pueden transmitir éstas para su comprobación a la centralita de contabilización y, tras la liberación, se puede generar allí un número de transacción, o se puede generar directamente en la estación de carga el identificador de transacción. En este caso, el identificador de transacción se puede indicar por la estación de carga al usuario y se puede transmitir por separado o con la transmisión del valor de medición de energía a la centralita.

También es posible que mediante una tarjeta de saldo se de a conocer un identificador de transacción. Este identificador de transacción está asignado a un saldo cuantificado. Un usuario puede comprar una tarjeta de saldo. En ésta está indicado de forma cubierta un identificador de transacción. Por ejemplo, es posible que el campo con el identificador de transacción esté laminado con plástico opaco y se rasque por parte del usuario.

También es posible que un usuario reciba un identificador de transacción mediante un cajero automático, un sistema de pago de Internet o similares en el que cambia un importe de dinero por el identificador de transacción. El identificador de transacción junto con el importe de dinero asignado a éste se almacena en la centralita.

Junto con un identificador de transacción se puede proporcionar una contraseña al usuario. Esta contraseña se puede usar para proteger adicionalmente el acceso a un comprobante de factura al tener que introducirse, además del identificador de transacción, una contraseña hasta que se conceda el acceso al comprobante de factura.

El usuario puede introducir el identificador de transacción previamente comprado y recibido en la estación de carga y, con ello, revelar su información de pago, o también transmitirlo por teléfono o SMS a la centralita. Una vez comprobado el identificador de transacción introducido con respecto a su validez y, dado el caso, una vez consultado el saldo asignado a este identificador, se puede liberar un proceso de carga.

La siguiente comprobación de la carga se puede realizar mediante el comprobante de factura al que se puede acceder mediante el identificador de transacción y, dado el caso, una contraseña.

Asimismo, es posible que sólo a continuación de la señalización de la disposición de pago se cree un identificador de transacción.

El identificador de transacción se puede indicar al usuario, por ejemplo, en la estación de carga o también se puede entregar por SMS, correo electrónico, dado el caso, incluso por correo o similares. El grado de anonimato se puede determinar en gran parte por el propio cliente mediante una elección adecuada de la recepción del identificador de transacción (por ejemplo, un teléfono móvil de prepago o una dirección de correo electrónico).

Una vez que el usuario haya señalado su disposición de pago y, dado el caso, haya revelado informaciones de pago o una solicitud de carga que incluye informaciones de pago, se puede crear el identificador de transacción. Éste se

le comunica al usuario. Si el identificador de transacción se crea en la centralita, éste se le comunica a la estación de carga. Si el identificador de transacción se crea en la estación de carga, éste se le comunica a la centralita.

En la estación de carga se asigna un identificador de transacción a un proceso de carga actual. De este modo se asegura que el proceso de carga se vuelve comprensible y se puede seguir. Por otro lado, el identificador de transacción garantiza una medida máxima de anonimato, ya que, dado el caso, el identificador de transacción es libre de características que identifican al usuario.

Preferiblemente, el identificador de transacción es una secuencia de cifras que está formada a partir de números y caracteres. En el caso de una secuencia de cifras lo suficientemente larga, ésta sólo se puede reproducir con dificultad. Por ejemplo, cuando la secuencia de cifras tiene una longitud de 30 caracteres y está formada a partir de cifras, caracteres especiales y números, ésta apenas se podrá reproducir. Asimismo, junto con el identificador de transacción se puede crear una contraseña que se le comunica al usuario junto con el identificador de transacción.

Una vez recibido el identificador de transacción se libera una corriente de carga en la estación de carga.

Durante el proceso de carga en marcha se registra en la estación de carga al menos un nivel de contador de aparato de medición que representa la cantidad de energía recibida por un vehículo de la estación de carga. Por ejemplo, a este respecto, también se puede indicar una tarifa variable en el tiempo siempre que en el registro del nivel de contador de aparato de medición se registre la hora local o un cambio de tarifa y se registre por cada intervalo de tarifa un nivel de contador inicial y un nivel de contador final. Para ahora establecer la factura también como comprobante admisible con respecto al derecho de calibración se propone también que el contador de energía utilizado o un aparato adicional correspondiente una todas las informaciones relevantes tales como el valor de medición, la hora, la fecha, el lugar y el identificador de transacción mediante procedimientos de firma de modo que se produce un conjunto de datos que ya no se puede modificar y que está asignado fijamente al número de transacción y éste también se tiene que indicar o transmitir de este modo en la factura.

Para ello se propone que al paquete de datos, que está formado a partir de al menos el valor de medición y el identificador de transacción, se le asigne una descripción unívoca.

La descripción unívoca puede ser tal que ésta defina de forma unívoca el paquete de datos. Un cambio en el paquete de datos conduciría a una descripción cambiada. Por tanto, es posible, partiendo de un paquete de datos recibido, conociendo la norma de creación para la descripción unívoca, crear una descripción de comparación y compararla con la descripción unívoca también recibida. Si las dos descripciones se diferencian entre sí, entonces se debe partir de un cambio del paquete de datos, esto es, al menos de un cambio del identificador de transacción o del valor de medición.

Se ha mostrado que, por regla general, la medición de la cantidad de energía recibida es correcta y también se mide mediante un contador aprobado con respecto al derecho de calibración. Por tanto, sólo queda la cuestión de cómo se puede asegurar que la cantidad de energía medida se asigna exclusivamente a la transacción correcta. Esto se consigue mediante la asociación del paquete de datos con la denominación unívoca. En particular se realiza la denominación unívoca mediante el aparato de medición que está calibrado y, por tanto, es especialmente fiable.

Los paquetes de datos asignados unos a otros y las descripciones unívocas se proporcionan preferiblemente a una centralita de contabilización. La centralita de contabilización puede calcular en primer lugar con la norma de cálculo que conoce a partir del paquete de datos recibido una descripción de comparación y comparar ésta con la descripción asociada con el paquete de datos. Si existen diferencias, entonces se puede concluir una manipulación de datos. En este caso, el valor de medición se puede descartar o se pueden tomar otras medidas. Si la comparación es positiva, entonces se puede deducir del paquete de datos el identificador de transacción y se puede contabilizar la cantidad de energía mediante las informaciones de pago recibidas, por ejemplo, al cargarse una factura de teléfono móvil, al enviarse un SMS de pago al usuario, al cargarse una tarjeta de crédito y similares. Al mismo tiempo se puede crear un comprobante de factura para la transacción.

Se puede almacenar el paquete de datos junto con la descripción. De este modo es posible una prueba posterior de que a una determinada transacción está asignado un proceso de carga. El usuario puede solicitar el comprobante de factura al usar el identificador de transacción que sólo él conoce y, dado el caso, la contraseña. A este respecto, el usuario puede permanecer anónimo. En particular es ventajoso un acceso basado en Internet a un comprobante de factura utilizando al menos el identificador de transacción.

Durante o, como muy tarde, a continuación de la carga, el proveedor de energía proporciona al usuario el comprobante de factura con respecto al proceso de carga bajo el identificador de transacción para un período de tiempo adecuado, por ejemplo, de 30 o 90 días. Por ejemplo, en un portal de Internet, éste está disponible para el usuario para su descarga. También es posible una consulta por fax u otra consulta del comprobante de factura utilizando el identificador de transacción.

Ahora es responsabilidad del usuario comprobar la factura y, dado el caso, reclamar la factura. A este respecto, el

usuario puede dejar su anonimato y demostrar que es él la persona a la que se le ha comunicado el identificador de transacción.

Para garantizar una asignación unívoca entre un proceso de carga y un identificador de transacción, el identificador de transacción debe ser unívoco y único. Además, para evitar accesos por terceros a los comprobantes de factura, el identificador de transacción debería tener una longitud suficiente.

Además, se propone proporcionar al cliente un software de verificación con cuya ayuda puede comprobar la exactitud del conjunto de datos recibido. A este respecto, el software debería verificar no sólo las firmas sino también la ausencia de errores en el contenido del conjunto de datos.

De acuerdo con un ejemplo de realización ventajoso, el identificador de transacción incluye características adecuadas mediante las que el proveedor de energía y el usuario pueden detectar de manera segura debido a qué solicitud de carga se creó. En el caso de prepago, se podría elegir a este respecto también el número de tarjeta/cliente al menos en parte como identificador de transacción por motivos de simplificación. Esto es válido en particular cuando ya está garantizado un anonimato suficiente mediante la tarjeta de prepago.

También se propone que en la estación de carga se cree una información de pago. La información de pago puede ser la información acerca de una disposición de pago o ya puede incluir un identificador de transacción comprado previamente por el usuario. La información de pago creada se puede transmitir a la centralita de contabilización. A continuación de la transmisión de la información de pago, el identificador de transacción se puede crear por la centralita de contabilización y se puede recibir en la estación de carga, siempre que aún no exista.

A este respecto, por ejemplo, cabe señalar el pago en un cajero automático o un distribuidor automático o en un terminal de pago con tarjeta en la estación de carga. Una vez que un usuario haya pagado un determinado importe en efectivo o mediante cobro en su cuenta de tarjeta, la información de pago se puede transmitir junto con un ID de la estación de carga, aunque preferiblemente de forma anónima, a la centralita de contabilización. Allí se crea el identificador de transacción. Asimismo, el identificador de transacción se puede crear en primer lugar en la estación de carga y se puede transmitir con la información de pago a la centralita. Con el identificador de transacción se asocian en la estación de carga los valores de medición y el cliente puede consultar y comprobar éstos mediante un comprobante de factura que se asocia con el identificador de transacción.

También se propone que el identificador de transacción esté formado al menos en parte a partir de informaciones de usuario. Éstas pueden ser, por ejemplo, también datos anónimos para el proveedor de energía tal como, por ejemplo, un número de tarjeta de una tarjeta de prepago. Por ejemplo, en el identificador de transacción pueden estar contenidas también al menos en parte informaciones de usuario determinadas a partir de un teléfono móvil o una tarjeta de telefonía móvil del usuario.

De acuerdo con un ejemplo de realización se propone que la descripción unívoca sea una firma para la protocolización unívoca permanente de un nivel de contador de aparato de medición asociado con un identificador de transacción.

Para permitir al usuario comprobar al menos los datos de contabilización y/o la cantidad de energía recibida, se propone la firma electrónica del paquete de datos junto con la descripción y la siguiente transmisión de la estación de carga a la centralita de contabilización.

A continuación, los términos "firma", "firmar", etc. se utilizan en el sentido de una firma electrónica de datos. También se puede asegurar mediante la firma electrónica del paquete de datos que éste ya no se manipula posteriormente.

Tal como ya se describió, también se propone que la descripción unívoca esté asociada con el contenido del paquete de datos de modo que un cambio del contenido del paquete de datos provoca una descripción cambiada. Por tanto, se puede crear una relación de uno a uno entre el paquete de datos y la descripción. Asimismo, si sólo cambia un bit en el paquete de datos, esto conduciría a un cambio de la descripción. En la estación de carga, preferiblemente en el aparato de medición de la estación de carga, está almacenada una norma de contabilización que permite crear a partir del paquete de datos una descripción unívoca. Esto se puede realizar utilizando claves, tal como también se describe a continuación. Si se conoce la norma de descripción y, dado el caso, la clave en el receptor, entonces ésta puede calcular una descripción de comparación a partir del paquete de datos recibido y comparar ésta con la descripción asignada al paquete de datos y, por tanto, descubrir manipulaciones. También es posible con el procedimiento descrito una prueba unívoca de un uso de una estación de carga por parte de un cliente.

Para crear la descripción unívoca se propone también que al menos se registre una parte de una clave de aparato de medición. Ésta puede ser una clave privada que permite crear la denominación unívoca de modo que ésta es segura frente a manipulaciones.

También se propone que se cree la firma del paquete de datos con ayuda de la clave de aparato de medición. La

firma se puede calcular mediante todo el paquete de datos o un valor hash del paquete de datos. También es posible firmar en primer lugar el paquete de datos compuesto por el nivel de contador de aparato de medición y el identificador de transacción, resumir el paquete de datos y la firma en un paquete de datos nuevo y, a continuación, añadir datos adicionales, tal como se enumeran a continuación, al paquete de datos nuevo. Este paquete de datos nuevo con los datos adicionales se puede firmar entonces de nuevo.

De acuerdo con un ejemplo de realización se propone que el paquete de datos incluya, además del identificador de transacción y del nivel de contador de aparato de medición, al menos datos adicionales a partir de una identificación de aparato de medición, un estado de aparato de medición, informaciones de tiempo, informaciones de fecha, una clave de aparato de medición pública, un índice de tiempo, una información de usuario y/o una información de pago. Esta enumeración no es limitativa y se puede complementar por datos relevantes adicionales.

Una introducción especialmente sencilla del identificador de transacción es posible cuando el identificador de transacción sea una secuencia de caracteres ASCII.

Para la asignación unívoca de los datos de medición a un usuario, ésta se debería realizar, en la medida de lo posible, directamente en el punto de medición para excluir en gran parte una manipulación. Por tanto, se propone que las etapas de acuerdo con la reivindicación 1 se realicen en el lado de la estación de carga.

También se propone que las informaciones de pago y/o la solicitud de carga se registren mediante medios de registro dispuestos en la estación de carga. Los medios de registro pueden estar dispuestos dentro de, en o fuera de la estación de carga.

La estación de carga registra, además de la cantidad de energía y del identificador de transacción, al menos también una identificación del aparato de medición. Ésta puede ser un número de aparato. La identificación del aparato de medición puede ser también la identificación adicional de la estación de carga. Con ayuda de al menos estos valores se puede ampliar el paquete de datos.

Con ayuda de un valor unívoco, preferiblemente binario, creado a partir del paquete de datos y una clave asignada al aparato de medición (contador) o a la estación de carga se puede calcular una firma. A partir del paquete de datos se puede calcular un valor de referencia, por ejemplo, un código hash. Este valor de referencia se puede utilizar también para calcular la firma. Esta firma se puede calcular, por ejemplo, con ayuda del código hash y una clave asignada al aparato de medición (contador) o a la estación de carga. También se puede calcular una firma directamente a partir del paquete de datos y de la clave asignada al aparato de medición (contador) o a la estación de carga.

La firma puede ser una creación de un criptograma como firma con ayuda de una clave preferiblemente binaria, creándose con ayuda de la clave y del paquete de datos a firmar o del valor de referencia creado a partir de ello un criptograma preferiblemente binario. Mediante un criptograma de este tipo es posible una comprobación para determinar si el paquete de datos se ha creado realmente por la estación de carga.

Por ejemplo, en un proceso de carga es posible que el usuario apunte al inicio de un proceso de carga la identificación de aparato de medición que, por ejemplo, está dispuesta por fuera en la carcasa de la estación de carga, y que apunte adicionalmente la hora del inicio del proceso de carga. Al final del proceso de carga, el usuario puede apuntar de nuevo la hora.

Cuando estas informaciones de tiempo junto con el nivel de contador de aparato de medición se convierten en parte del respectivo paquete de datos, entonces se puede comprobar una firma de este paquete de datos por parte del usuario cuando el usuario conoce adicionalmente el identificador de transacción y la clave de aparato de medición pública.

Por ejemplo, es posible que el usuario apunte al inicio y al final de cada proceso de carga la identificación de aparato de medición y la respectiva hora.

La estación de carga crea un paquete de datos que incluye un identificador de transacción en el paquete de datos y adicionalmente, por ejemplo, la hora y la identificación de aparato de medición. Adicionalmente, el paquete de datos puede contener el nivel de contador de aparato de medición y el estado de aparato de medición.

El estado de aparato de medición puede incluir una información con respecto a la funcionalidad técnica de la estación de carga, por ejemplo, un valor binario que indica si la estación de carga funciona sin errores.

Con ayuda de la clave de aparato de medición privada se puede crear una firma a partir de este paquete de datos. La firma junto con el paquete de datos se puede transmitir por la estación de carga a la estación de contabilización.

Mediante la firma del paquete de datos se asegura que los valores de medición incluidos en el paquete de datos y el identificador de transacción están conectados de forma inseparable entre sí. Si se modifica uno de los dos valores,

entonces resultaría otra firma. Por ejemplo, cuando el propio usuario puede registrar además la información de tiempo, también puede determinar una manipulación del valor de medición cuanto éste incluye la información de tiempo.

Una vez finalizado un proceso de carga, el operador de la red eléctrica/proveedor de energía crea un comprobante de factura con respecto a la cantidad de energía recibida. Por ejemplo, en este comprobante de factura puede estar enumerado el proceso de carga desglosado según el inicio y el final del proceso de carga.

Adicionalmente, a cada comprobante de factura puede estar asignada la identificación de aparato de medición, por ejemplo, un ID de punto de carga, y un número de contador. Adicionalmente, los niveles de contador de inicio y de final así como los tiempos de inicio y de final (hora, fecha) pueden estar asignados a un comprobante de factura. Con estas informaciones, el cliente puede leer en el comprobante de factura la cantidad de energía recibida para un proceso de carga asignado a un identificador de transacción.

Además, el usuario puede recibir junto con cada comprobante de factura una información con respecto al estado de aparato de medición y la firma que se ha creado para el paquete de datos correspondiente. Por ejemplo, para cada comprobante de factura se pueden crear dos firmas. Una primera firma para el paquete de datos que se ha creado al inicio del proceso de carga y una segunda firma para el paquete de datos que se ha creado al final del proceso de carga.

Mediante el uso del identificador de transacción en el paquete de datos, el usuario también puede comprobar si la cantidad de energía facturada está asignada realmente a la transacción o al proceso de carga que ha desencadenado.

Finalmente, se le puede comunicar al usuario la clave de aparato de medición pública.

Dado que el cliente ha apuntado de forma autónoma tanto el identificador de transacción, la identificación de aparato de medición y la hora del respectivo proceso de carga, puede comprobar individualmente junto con las informaciones adicionales a partir del comprobante de factura, por ejemplo, la identificación de punto de carga, el número de contador, el nivel de contador y la clave pública, la firma que se le ha comunicado para cada paquete de datos. Para ello, por ejemplo, puede calcular el valor de referencia mediante la firma que se le ha comunicado y mediante la clave pública que se le ha comunicado. Por ejemplo, el cliente puede calcular un valor de referencia de comparación mediante la información que ha apuntado y la información adicional a partir del comprobante de factura y puede comprobar si los datos son idénticos. Por tanto, el cliente tiene la posibilidad de comprobar la exactitud del comprobante de factura.

Por ejemplo, se puede calcular de forma retroactiva con una clave conocida por el receptor, que es adecuada para la clave de firma, el valor de referencia o el paquete de datos a firmar a partir de la firma. Para ello, por ejemplo, se puede calcular en el lado del receptor un valor de referencia de comparación partiendo del paquete de datos. Si el valor de referencia calculado y el valor de referencia de comparación coinciden, entonces se puede partir de una integridad de datos.

Por ejemplo, a partir de datos útiles (paquete de datos) se puede calcular un valor de referencia. A partir de este valor de referencia se puede calcular con una clave privada una firma. La firma se puede enviar a un receptor junto con los datos útiles en un contenedor de datos como dos ficheros separados o de forma incrustada en los datos útiles. El receptor puede calcular el valor de referencia a partir de la firma con una clave pública que es adecuada para la clave privada. A partir de los datos útiles también recibidos se puede calcular en el lado del receptor también un valor de referencia de comparación. Si el valor de referencia y el valor de referencia de comparación coinciden, entonces se puede asegurar la integridad, la autentificación y la autenticidad de los datos útiles.

De manera ventajosa se le comunica al cliente junto con el comprobante de factura para cada paquete de datos una firma separada. Para cada comprobante de factura que se componga por dos mediciones, concretamente el inicio y el final de un proceso de carga, están disponibles dos conjuntos de datos o están disponibles tres o cuatro conjuntos de datos en caso de un cambio de tarifa (con tres o cuatro mediciones), concretamente el inicio y el final del proceso de carga así como un conjunto de datos adicional para el cambio de tarifa o dos conjuntos de datos, uno para el final de la primera tarifa y uno para el final de la segunda tarifa o los respectivos momentos dentro de una tarifa, a los que está asignada en cada caso una firma. El primer conjunto de datos determina el inicio del proceso de carga y, por ejemplo, incluye adicionalmente identificaciones de aparato de medición (ID de punto de carga, número de contador), el nivel de contador y la palabra de estado. Para el final del proceso de carga existe un segundo conjunto de datos que incluye el momento del final del proceso de carga. Lo mismo es válido para los conjuntos de datos en un cambio de tarifa a los que están asignados también una información de tiempo, una identificación de aparato de medición y un nivel de contador.

Para cada conjunto de datos se calcula en la estación de carga una firma que se le proporciona al usuario en el comprobante de factura en texto sin codificar. El usuario puede comprobar la exactitud de la firma por que puede calcular una firma de comparación con ayuda del identificador de transacción que ha comunicado y, dado el caso, la

identificación de contador y la información de tiempo apuntadas junto con las informaciones que se le han comunicado con respecto al nivel de contador y la palabra de estado y la clave pública y puede comprobar si la firma comunicada y la firma de comparación calculada son idénticas. La utilidad básica de un conjunto de datos resulta para el cliente por que compara el identificador de transacción, el número de identificación del punto de carga (contador) así como informaciones de tiempo (fecha y/u hora) con sus registros.

Debido a que la firma comunicada se puede asignar de forma unívoca al paquete de datos, el usuario podría determinar una manipulación del valor del nivel de contador de aparato de medición. El caso es que entonces la firma que se le ha comunicado ya no sería idéntica a la firma que ha calculado. Un nivel de contador cambiado con informaciones idénticas con respecto al identificador de transacción, al momento de la carga y/o a la identificación de aparato de medición conduciría a otra firma. Sin embargo, preferiblemente, el propio cliente apunta el identificador de transacción, el momento del proceso de carga y la identificación de aparato de medición de modo que puede detectar una manipulación en la región del nivel de contador de aparato de medición.

Por una firma electrónica se pueden entender también datos asociados con informaciones electrónicas con los que se puede identificar al firmante o creador de la firma y se puede comprobar la integridad de las informaciones electrónicas firmadas. Por regla general, en el caso de las informaciones electrónicas se trata de documentos electrónicos. Por tanto, desde el punto de vista técnico, la firma electrónica cumple la misma finalidad que una firma manuscrita sobre documentos de papel. Una firma electrónica puede comprender, entre otras cosas, también una firma digital. La firma digital puede designar la firma criptográfica meramente de datos en la que se aplican métodos matemáticos criptográficos. "Firmas electrónicas" pueden ser datos en forma electrónica que están adjuntados a otros datos electrónicos o están asociados de forma lógica con los mismos y que sirven para la autenticación.

Si en la transmisión cambian valores dentro del paquete de datos, entonces se puede determinar en el lado del receptor, por ejemplo, en la centralita de contabilización, que la firma transmitida con el paquete de datos no es adecuada para el paquete de datos recibido y que tiene que haber tenido lugar un cambio del paquete de datos. La comparación de la firma recibida con una firma de comparación calculada o la comparación de un valor de referencia con un valor de referencia de comparación proporciona una diferencia entre estos dos valores en caso de datos cambiados.

De acuerdo con un ejemplo de realización ventajoso se propone que el paquete de datos y la descripción unívoca se creen al menos al inicio y al final de un proceso de carga y/o de forma cíclica durante un proceso de carga y se transmitan a la centralita de contabilización. Por tanto, en la centralita de contabilización se puede crear a partir de los dos paquetes de datos un comprobante de factura en el que se evalúa el cambio del nivel de contador de aparato de medición y se calcula una cantidad de energía mediante este cambio. Junto con informaciones de tarifa se puede determinar un importe de factura con la cantidad de energía calculada. Debido a que se ha creado para cada paquete de datos una firma y el propio usuario ha apuntado al inicio y al final de cada proceso de carga informaciones de tiempo que son partes del paquete de datos y, por tanto, son relevantes para la firma, el cliente puede comprobar mediante la firma si las informaciones en las que se basa el comprobante de factura son correctas o no.

También se propone que el paquete de datos y la descripción unívoca se creen en un momento de un cambio de tarifa, creándose en un momento de un cambio de tarifa un primer paquete de datos y la respectiva firma para un final de una primera tarifa y creándose un segundo paquete de datos y la respectiva firma para un inicio de una segunda tarifa, o sólo un paquete de datos que representa el cambio de tarifa. Por tanto, se asegura que en caso de un cambio de tarifa se puede determinar la respectiva cantidad de energía recibida con respecto a una determinada tarifa. Si cambia una tarifa durante un proceso de carga, entonces el nivel de contador del aparato de medición se registra en el momento del cambio de tarifa. Con ayuda de este nivel de contador y la información de tiempo directamente antes del cambio de tarifa se crea un primer paquete de datos y junto con la información de tiempo directamente tras un cambio de tarifa se crea un segundo paquete de datos. Cada uno de los paquetes de datos se firma y se transmite a la estación de contabilización de modo que es posible una comprobación. De forma alternativa, también se puede crear un paquete de datos para el momento de cambio.

De acuerdo con un ejemplo de realización ventajoso se propone que la estación de carga y/o la estación de contabilización calculen una cantidad de energía recibida a partir del nivel de contador de aparato de medición al inicio de un proceso de carga y a partir del nivel de contador de aparato de medición al final de un proceso de carga o en caso de un cambio de tarifa. Con ayuda de la diferencia entre los respectivos niveles de contador de aparato de medición se puede calcular una cantidad de energía que se puede utilizar para la creación de un comprobante de factura.

Tal como ya se explicó anteriormente, se pueden proporcionar por la estación de contabilización datos de contabilización con respecto a la cantidad de energía recibida. Estos datos de contabilización se pueden comunicar al usuario en el marco de un comprobante de factura. Para cada proceso de carga se puede emitir un momento de inicio y un momento de final. Adicionalmente a este respecto se pueden emitir informaciones con respecto a identificaciones de aparato de medición, por ejemplo, un ID de punto de carga, y un número de identificador. También se puede emitir la dirección de la respectiva estación de carga. Adicionalmente, un nivel de contador se

puede emitir para cada momento y se puede indicar junto con una tarifa en el comprobante de factura. Finalmente, para cada proceso de carga se puede emitir la cantidad de energía recibida.

En un comprobante de factura también se pueden emitir informaciones de tiempo para cada proceso de carga. Además, el número de contador u otra identificación de aparato de medición se puede emitir junto con el nivel de contador y/o un estado de aparato de medición. Por ejemplo, estos datos pueden haber formado parte del paquete de datos. En la misma línea se puede emitir entonces una firma que ha resultado de los datos indicados y de la clave de aparato de medición.

Con la clave pública se puede comprobar junto con las informaciones que se han comunicado al usuario para cada paquete de datos si la firma es correcta. Dado que el usuario ha apuntado tanto el momento como el número de contador y conoce el identificador de transacción, puede comprobar con las informaciones que él mismo ha apuntado la autenticidad y la integridad de la firma.

También es posible que las informaciones anteriormente mencionadas se tengan a disposición de modo que se pueden consultar, en particular mediante una red de área amplia, en particular mediante Internet.

De acuerdo con un ejemplo de realización ventajoso se propone que los datos de contabilización se tengan a disposición de forma protegida frente a accesos. En particular, los datos se pueden tener a disposición de forma protegida frente a accesos mediante el identificador de transacción. Por tanto, se asegura que sólo personas autorizadas tienen acceso al comprobante de factura. Sin embargo, el acceso a las claves públicas de los respectivos aparatos de medición puede estar protegido de modo que todos los clientes de un proveedor de energía tienen un acceso común a ello. De forma alternativa, en este caso incluso se puede renunciar totalmente a una protección frente a accesos.

Para asegurar que no se puede realizar una manipulación de los datos de factura por parte del proveedor de energía lo que, por ejemplo, sería posible por que se manipula la clave pública, se propone que las claves de aparato de medición públicas se tengan a disposición por aparatos de medición de las estaciones de carga mediante un ordenador separado de forma lógica y/o espacial de la estación de contabilización. En particular, las claves públicas se pueden tener a disposición en un órgano de calibración u órgano de verificación de modo que una manipulación por parte del proveedor de energía se vuelve imposible.

Para facilitar a los usuarios la comprobación de los datos de factura se propone que se proporcione un programa informático para calcular y/o comprobar la firma para el nivel de contador de aparato de medición asignado en cada caso. Por ejemplo, este programa puede calcular la firma a partir de los datos de factura disponibles en línea o también a partir de los datos de factura introducidos por usuarios. Por ejemplo, el usuario puede introducir manualmente el identificador de transacción, el momento que ha apuntado así como el número de contador que ha apuntado. Junto con estas informaciones, el programa puede calcular la firma a partir de las informaciones de factura, por ejemplo, el nivel de contador y la palabra de estado utilizando la clave pública. Mediante el programa, esta firma se puede comparar entonces automáticamente con la firma que estaba incluida en los datos de factura. Sin embargo, también el propio usuario puede realizar esta comprobación, ya que la firma de comparación calculada por el programa se emite en texto sin codificar y también se ha emitido en texto sin codificar la firma en la que se basan los datos de factura. Este programa se puede proporcionar por un ordenador que está separado de forma lógica y/o espacial de la estación de contabilización. En particular, un organismo de calibración puede proporcionar este programa además de las claves públicas.

De acuerdo con un ejemplo de realización puede estar almacenada en el aparato de medición o en la estación de carga una pareja formada por la clave de aparato de medición pública (PuM) y la clave de aparato de medición privada (PiM). Con ayuda de la clave de aparato de medición privada (PiM) se puede crear una firma (SD) del paquete de datos. Por ejemplo, para ello se puede calcular un criptograma a partir de un valor de referencia asignado al paquete de datos con ayuda de la clave de aparato de medición privada (PiM). Este valor de referencia puede ser un código hash.

En el lado del receptor, por ejemplo, en una centralita de contabilización o por parte del usuario se puede comprobar la autenticidad y la integridad de datos del paquete de datos recibido por que el criptograma recibido se descifra con ayuda de la clave de aparato de medición pública conocida en el lado del receptor y, por tanto, se calcula el valor de referencia. Una comparación con un valor de referencia calculado a partir del paquete de datos en el lado del receptor permite la comprobación de la integridad de datos. Por ejemplo, es posible que sea conocida la clave de aparato de medición pública (PuM) en una centralita de contabilización. Asimismo, la clave de aparato de medición pública (PuM) puede estar incluida en el paquete de datos.

Un código hash se puede calcular mediante un procedimiento de cálculo unívoco como un valor de referencia unívoco estadísticamente. Un código hash puede ser un valor determinado a partir de una pluralidad finita de valores. Debido a la pluralidad de los posibles códigos hash se produce un código hash cambiado en caso de un cambio del conjunto de datos. El hecho de que dos conjuntos de datos diferentes generen un código hash idéntico es muy poco probable en función del número y del tipo de los coeficientes para calcular el código hash. Para esta

probabilidad es fundamental el procedimiento para calcular el valor hash. Ejemplos de métodos de cálculo de código hash pueden ser MD2, MD4, MD5, SHA, RIPEMD-160, Tiger, HAVAL, Whirlpool, LM-Hash o NTLM. Igualmente son adecuados otros procedimientos, en particular procedimientos criptográficos.

Una función hash criptológica debería ser al menos una función unidireccional. Las denominadas funciones hash unidireccionales (*One-Way-Hash Functions*, OWHF) cumplen con el requisito de ser una función unidireccional, es decir, es prácticamente imposible encontrar un valor de introducción x con respecto a un valor de emisión dado h(x) = y (en inglés *preimage resistance*). Además, una función hash es más adecuada para la criptografía cuando no se producen colisiones en la medida de lo posible. Es decir, a ser posible, el valor hash (código hash) también debería ser diferente para dos valores diferentes x y x': h(x) distinto a h(x'). Si éste es siempre el caso, entonces se puede hablar de una función hash resistente frente a colisiones (*Collision Resistant Hash Function*, CRHF).

A partir de la firma se puede calcular con ayuda de la clave de aparato de medición pública (PuM) un valor de referencia que se puede comparar con un valor de referencia de comparación calculado a partir del paquete de datos. De este modo se puede comprobar si los datos incluidos en el paquete de datos se han manipulado en el trayecto de comunicación de la estación de carga a la centralita de contabilización.

De acuerdo con un ejemplo de realización ventajoso se propone también que se determine una firma mediante un procedimiento SHA-256. A este respecto, por ejemplo, se puede utilizar una variante FIPS 180-2.

En particular se propone que se determine una firma con ayuda de un procedimiento de criptografía de curva elíptica. A este respecto, por ejemplo, es posible que se utilice un procedimiento ECC con 192 bits.

De acuerdo con un ejemplo de realización ventajoso se propone también que el paquete de datos se firme mediante un procedimiento asimétrico. Tal como ya se explicó anteriormente, en este procedimiento se utilizan una clave privada para una firma y una clave pública, que es conocida en el lado del receptor, para el descifrado de la firma.

Para permitir una asignación de un valor de medición a un momento de medición se propone que el paquete de datos incluya un índice de tiempo. Por ejemplo, un índice de tiempo puede ser un índice de segundos que tiene un crecimiento muy monótono en el sentido matemático por toda la vida útil del aparato de carga y que representa un número natural. Con ayuda de este índice de segundos es posible realizar una asignación unívoca del momento de medición a un valor de medición. También se puede utilizar un contador de segundos de operación que puede ser un número natural que crece de forma monótona cuyo objetivo es la asignación univoca del momento de un acontecimiento al tiempo legal supuesto como sistema de referencia.

Por ejemplo, cuando un usuario desea realizar una carga, puede enviar un SMS a una centralita de contabilización con el número de la estación de carga, en la que desea realizar la carga, o, por ejemplo, indicar el número de la estación de carga en una aplicación móvil. De este modo se crea una solicitud de carga en la centralita de contabilización. Cuando existen informaciones de pago suficientes que también pueden estar incluidas en la solicitud de carga, a continuación de la solicitud de carga recibida se puede crear y transmitir a la estación de carga el identificador de transacción.

También se propone que en primer lugar se reciba una solicitud de carga en una centralita de contabilización. En la solicitud de carga puede estar incluida la fuente de las informaciones de fuente que definen la solicitud de carga. Por ejemplo, éstas pueden ser un número de teléfono móvil, un número de teléfono, una dirección de correo electrónico, un número de tarjeta de crédito o similares. Asimismo, una información de fuente puede ser el identificador de transacción ya comprado por el usuario. El identificador de transacción se crea de modo que éste incluye al menos en parte las informaciones de fuente.

También se propone que el identificador de transacción se comunique al usuario mediante un centro de llamadas, un mensaje corto, un correo electrónico, una página de Internet o un dispositivo de emisión dispuesto en la estación de carga. Con el identificador de transacción comunicado de este modo, un usuario puede solicitar un comprobante de factura y comprobar la exactitud de los datos incluidos en el mismo.

También se propone que el identificador de transacción esté formado al menos en parte a partir de un identificador de cliente temporal. Un identificador de cliente temporal puede ser tal que éste está construido como un número de cliente aunque sólo existe temporalmente y no está asignado a un cliente real. Más bien, esto permite que tanto clientes utilizando su número de cliente como usuarios anónimos utilizando el identificador de transacción tengan acceso a comprobantes de factura mediante el mismo modo de acceso, por ejemplo, un portal de Internet. Los procedimientos anteriormente mencionados también se pueden realizar como programa informático o como programa informático almacenado en un medio de almacenamiento. A este respecto, un microprocesador puede estar programado de manera adecuada mediante un programa informático en el lado de la estación de carga y/o en el lado de la centralita de contabilización para realizar las respectivas etapas de procedimiento.

Las características de los procedimientos y dispositivos se pueden combinar libremente entre sí. En particular, características de la descripción y/o de las reivindicaciones dependientes pueden ser inventivas independientemente

por sí solas o combinadas libremente entre sí también omitiendo de forma completa o parcial características de las reivindicaciones independientes.

A continuación se explica en más detalle el objeto mediante un dibujo que muestra ejemplos de realización. En el dibujo muestran:

La figura 1a	una estructura esquemática de un sistema para cargar un vehículo eléctrico;
La figura 1b	una estructura esquemática de un aparato de medición con medios de registro para registrar una información de pago;
Las figuras 2a a b,	paquetes de datos y firmas ejemplares;
La figura 3	un diagrama de desarrollo de un procedimiento ejemplar.

La figura 1 muestra una estación de carga 2 que está conectada eléctricamente con un vehículo 6 mediante un cable de conexión 4. En la estación de carga 2 está prevista una caja de conexión 8 para la conexión del cable de conexión 4. Mediante el cable de conexión 4, por un lado, se transmite energía y, por otro lado, se intercambian datos entre el vehículo 6 y la estación de carga 2.

La caja de conexión 8 está conectada eléctricamente con un aparato de medición 10. El aparato de medición 10 mide la potencia eléctrica que se emite mediante la caja de conexión 8 al vehículo 6 mediante el cable de conexión 4. La potencia eléctrica se recibe mediante una conexión eléctrica 12 por una red de alimentación de energía eléctrica 14.

Al aparato de medición 10 está acoplada una unidad de cálculo 16 con una unidad de comunicación 16a y una unidad de firma 16b. La unidad de firma 16b puede registrar una identificación unívoca asignada al aparato de carga 2 o al aparato de medición 10, por ejemplo, una clave de aparato de medición privada (PiM) 18a. También se puede registrar una clave de aparato de medición pública (PuM) 18b.

La unidad de cálculo 16 está conectada mediante una red de datos 20 con una centralita de contabilización 22.

Además está previsto un ordenador adicional 23 que está separado de forma lógica y espacial de la centralita de contabilización 22. En particular, el ordenador 23 puede estar conectado con la red de datos 20, por ejemplo, con una red de área amplia, por ejemplo, Internet. Por ejemplo, el ordenador 23 se puede operar en las instalaciones y/o bajo la supervisión de un organismo de calibración.

Mediante la red de datos 20, usuarios pueden acceder tanto a la centralita de contabilización 22 como al ordenador 23. Los usuarios pueden consultar datos de factura en la centralita de contabilización 22. Por ejemplo, en el ordenador 23, usuarios pueden adquirir claves de aparato de medición públicas y/o programas para calcular una firma de comparación.

En el vehículo 6 está prevista, además de una batería 26 conectada con una conexión 24, una unidad de comunicación 28. La unidad de comunicación 28 permite el envío y la recepción de datos en el cable de conexión 4. Durante el proceso de carga del vehículo 6 en la estación de carga 2 se introduce energía por la red de alimentación de energía 14 en la batería 26 del vehículo 6. La cantidad de la energía introducida se registra mediante el aparato de medición 10. La cantidad de energía, por ejemplo, un nivel de contador del aparato de medición 10, igual que otros datos como, por ejemplo, la identificación de la estación de carga 2 y/o la identificación del aparato de medición 10, un sello de tiempo, un índice de tiempo, un estado de la estación de carga 2 y/o un estado del aparato de medición 10, un nivel de contador inicial, un nivel de contador final y/o similares se pueden transmitir a la centralita de contabilización 22.

Para una asignación unívoca del valor de recuento del aparato de medición a una transacción se debe asociar un paquete de datos, que está formado a partir del nivel de contador y del identificador de transacción, con una descripción unívoca, por ejemplo, una firma. Para ello se comunica un identificador de transacción 19 a la estación de carga 2.

Esto se muestra a modo de ejemplo en la figura 1b. La figura 1b muestra una estación de carga 2 con un aparato de medición 10 con un amperímetro 10a. El nivel de contador de aparato de medición del amperímetro 10a se puede emitir mediante el aparato de medición 10. Esto se puede realizar de forma cifrada y firmada, tal como aún se describirá a continuación. Para ello puede estar dispuesto en el aparato de medición 10 el dispositivo de firma 12. En el aparato de medición 10 puede existir una CPU 10b y puede estar almacenada la clave de aparato de medición 18 compuesta por la clave de aparato de medición privada 18a y la clave de aparato de medición pública 18b.

En la estación de carga 2 está dispuesto un distribuidor automático 3a. Cuando un usuario anónimo desea usar la estación de carga para cargar su vehículo, por ejemplo, puede pagar en el distribuidor automático 3a un importe de dinero de manera correspondiente a la energía a recibir. La estación de carga 2 registra el importe de dinero y envía una solicitud de carga junto con la información con respecto al importe de dinero pagado a la centralita de contabilización 22. En la centralita de contabilización 22 se recibe la solicitud de carga. A continuación se crea en la

centralita de contabilización 22 un identificador de transacción. Esto se transmite en primer lugar a la estación de carga 2 y, dado el caso, se emite mediante una pantalla en el distribuidor automático 3a.

En lugar de utilizar el distribuidor automático 3a, dado el caso, el usuario podría enviar mediante su teléfono móvil 4 un SMS a la centralita de contabilización. Por ejemplo, en este SMS podría estar indicado el ID de estación de carga. Además, con el SMS se podría transmitir una IMSI a la centralita de contabilización. En caso de que el teléfono móvil esté equipado con una tarjeta de prepago, la IMSI sería una secuencia anónima de cifras que no permite una conclusión de la identidad del usuario. La centralita de contabilización 22 podría crear un identificador de transacción 19 como respuesta a la recepción de un SMS de este tipo. Este identificador de transacción 19 se enviaría con un SMS de vuelta al usuario. Por ejemplo, la respuesta podría requerir un pago mediante SMS de modo que se podría contabilizar la energía con ello. Los costes del SMS se utilizarían como informaciones de pago en la estación de carga 2. Por tanto, el usuario recibe el identificador de transacción 19. De manera paralela a ello, la centralita de contabilización 22 enviaría el identificador de transacción 19 a la estación de carga 2 con el ID de estación de carga que se le ha comunicado en el SMS.

Después de que se haya recibido el identificador de transacción 19 en la estación de carga 2 se puede liberar un proceso de carga. La duración del proceso de carga puede resultar de las informaciones de pago. Durante la carga, el aparato de medición 10 registra los datos de medición y crea a partir de los mismos un conjunto de datos de contabilización relevantes para la contabilización.

Para ahora asociar los datos de contabilización fijamente con el identificador de transacción 19 se propone que un paquete de datos, que comprende al menos el nivel de contador de aparato de medición y el identificador de transacción 19, se transmita de forma firmada a la centralita de contabilización 22 una vez finalizado el proceso de carga.

Para ello, la unidad de comunicación 16 transmite un paquete de datos tal como se explica en la figura 2. En el paquete de datos se pueden almacenar dichas magnitudes de medición. En el paquete de datos se puede almacenar en particular una clave de aparato de medición pública (PuM) 18b. Asimismo, además del paquete de datos, se pueden intercambiar la clave de aparato de medición pública (PuM) 18b y/o firmas entre la estación de carga 2 y la centralita de contabilización 22.

Las figuras 2 muestran el cálculo de un paquete de datos y una firma que se pueden intercambiar mediante la red de datos 20 entre la estación de carga 2 y la centralita de contabilización 22.

La figura 2a muestra un primer paquete de datos 34 ejemplar en el que están almacenados un identificador de transacción 19, un nivel de contador 34a, opcionalmente un estado de aparato de medición 34b, opcionalmente una identificación de aparato de medición 34c, opcionalmente una información de tiempo 34d, opcionalmente una clave de aparato de medición pública (PuM) 18b y/o posiblemente datos adicionales 34f en una secuencia binaria de números. La identificación de aparato de medición 34c puede ser un identificador unívoco del aparato de medición 10 y/o de la estación de carga 2.

Para una autenticación del primer paquete de datos 34 se puede crear una firma 36. Para ello se utiliza en una etapa de cálculo 38 el primer paquete de datos 34 junto con una clave de aparato de medición privada (PiM) 18a para calcular una firma (SD) 36. Así, por ejemplo, en la etapa de cálculo 38 se puede determinar un valor hash a partir del primer paquete de datos y este valor hash se puede convertir en la firma (SD) 36 con la clave de aparato de medición privada (PiM).

Para la transmisión del primer paquete de datos 34 a la centralita de contabilización 22 se empaqueta el primer paquete de datos 34 con la firma 36 en un conjunto de datos 40. El conjunto de datos 40 se transmite a la centralita de contabilización 22 mediante la red de alimentación 14 o la red de datos 20 o de otro modo.

La figura 2b muestra el conjunto de datos 40 que está formado a partir del primer paquete de datos 34 y la firma 36.

El conjunto de datos 40 se puede enviar directamente a la centralita de contabilización 22. Los datos obtenidos a partir de ello se pueden utilizar para crear un comprobante de factura, tal como aún se describirá a continuación. El usuario puede comprobar la autenticidad y la integridad del comprobante de factura utilizando la firma 36, el identificador de transacción 19 que se le ha comunicado así como sus apuntes que él mismo ha realizado.

En la centralita de contabilización 22 se puede realizar a la inversa y/o de nuevo la etapa de cálculo 38 con ayuda de la firma (SD) 36 y la clave de aparato de medición pública (PuM) conocida en la centralita de contabilización 22. De este modo se puede comprobar si el paquete de datos 34 se ha transmitido sin errores de la estación de carga 2 a la centralita de contabilización 22.

Cuando el paquete de datos 34 y la firma 36 son compatibles, esto se puede utilizar como prueba de que el paquete de datos está sin falsificar. Por tanto, dado que en el paquete de datos está incluido el identificador de transacción 19, se puede asegurar que la energía recibida está asociada con la transacción correcta y se puede consultar un

comprobante de factura mediante el identificador de transacción.

Para un usuario también es posible con ayuda de la primera firma (SD) o la clave de aparato de medición pública (PuM) 18b una comprobación para determinar si los paquetes de datos 34 utilizados en la centralita de contabilización 22 para fines de contabilización realmente están relacionados con la transacción que se ha desencadenado por él y proceden de la estación de carga 2 en la que ha recibido energía.

Para ello, el usuario puede descargar del ordenador 23 la clave de aparato de medición pública (PuM) 18b de la estación de carga 2 cuyo ID ha apuntado en el proceso de carga.

Puede comparar el ID de estación de carga con un ID de estación de carga en su comprobante de factura. Los datos de factura que se refieren a este ID de estación de carga (paquetes de datos) están provistos de una firma en el comprobante de factura. El usuario puede comprobar esta firma 36 junto con el identificador de transacción 19, las informaciones de tiempo que ha apuntado y la clave de aparato de medición pública (PuM) 18b cargada de la estación de carga 2. Para ello, el usuario puede usar un programa cargado mediante el ordenador 23.

Las etapas de cálculo 38 y 48 se pueden basar en procedimientos asimétricos de descifrado que permiten la creación, la comparación y la validación de criptogramas mediante claves públicas y privadas.

Esto garantiza una alta integridad de datos en la contabilización. También es posible una comprobación de plausibilidad. Finalmente, se asegura que el paquete de datos 34 se ha recibido sin falsificar en la centralita de contabilización 22.

La figura 3 muestra un diagrama de desarrollo de un procedimiento para comprobar los datos de medición mediante el usuario.

En una primera etapa 60, un usuario se desplaza con su vehículo 6 hasta una estación de carga 2.

Para iniciar el proceso de carga se tiene que transmitir en primer lugar una solicitud de carga a la centralita de contabilización 22. Esto se puede realizar, por ejemplo, tal como se describe en la figura 1b. Por ejemplo, mediante un aparato lector de tarjetas en la estación de carga 2 se puede leer una tarjeta bancaria y se puede desencadenar un proceso de pago. Cuando el proceso de pago esté finalizado, esta información se puede transmitir como información de pago junto con una solicitud de carga de la estación de carga 2 a la centralita de contabilización 22.

A continuación, en la centralita de contabilización se crea un identificador de transacción 19 en la etapa 62. Este identificador de transacción 19 se envía de vuelta al usuario. Por ejemplo, esto se puede realizar mediante la emisión en una pantalla en la estación de carga 2. Por tanto, la estación de carga 2 también conoce el identificador de transacción 19.

Una vez que empiece el proceso de carga, se registra en la estación de carga 2, preferiblemente en el aparato de medición 10, aunque posiblemente también en la unidad de cálculo 16, la hora actual o un índice de tiempo así como la fecha. Además, la unidad de cálculo registra del aparato de medición 10 el nivel de contador actual. Además, la unidad de cálculo registra al menos un estado de la estación de carga (por ejemplo, en orden / error) y la identificación de aparato de medición. A este respecto es posible que el valor de medición, la hora y la fecha así como el estado y la firma se registren en el aparato de medición 10.

También es posible que partes de los datos anteriormente mencionados se registren en la unidad de cálculo 16 y que se firme el paquete de datos en la unidad de cálculo 16.

De manera paralela a ello, el usuario también puede apuntar el identificador de transacción 19 que se le ha comunicado, la hora y la fecha del inicio del proceso de carga. Para ello, por ejemplo, utiliza su propio reloj. Asimismo, el usuario puede leer y apuntar la identificación de aparato de medición o un ID de estación de carga que preferiblemente está colocado por fuera en la estación de carga 2.

En una siguiente etapa 64, la unidad de firma 16b calcula la firma 36 a partir del paquete de datos 34 que incluye las informaciones anteriormente mencionadas, en particular el identificador de transacción 19 y la clave de aparato de medición 18a.

El paquete de datos 34 y la firma 36 se transmiten a continuación a la centralita de contabilización 22.

En una siguiente etapa 66, el usuario finaliza el proceso de carga. En este momento, la unidad de cálculo 16 registra de nuevo la hora actual o un índice de tiempo así como la fecha. Además, la unidad de cálculo registra de nuevo del aparato de medición 10 el nivel de contador actual. Además, la unidad de cálculo registra de nuevo al menos un estado de la estación de carga (por ejemplo, en orden / error) y la identificación de aparato de medición.

De manera paralela a ello, el usuario también puede apuntar de nuevo la hora y la fecha del final del proceso de

carga. Para ello usa, por ejemplo, su propio reloj.

En una siguiente etapa 68, la unidad de firma 16b calcula la nueva firma 36 a partir del nuevo paquete de datos 34, que incluye el identificador de transacción 19 y las informaciones anteriormente mencionadas, y la clave de aparato de medición 18a.

El nuevo paquete de datos 34 y la nueva firma 36 se transmiten a la centralita de contabilización 22 en una siguiente etapa 70.

En la etapa 72 se determinan en la centralita de contabilización 22 las informaciones relevantes para la contabilización a partir de los dos paquetes de datos recibidos.

Para el usuario se crea y se almacena para cada proceso de carga en cada caso un comprobante de factura.

Utilizando el identificador de transacción 19 está disponible un comprobante de factura para cada proceso de carga. Este comprobante de factura indica toda la cantidad de energía recibida en un proceso de carga para una tarifa y el precio.

Además, el comprobante de factura indica para el proceso de carga el tiempo de inicio y el tiempo de final, la fecha, el ID de estación de carga, el número de contador, la dirección de la estación de carga 2, los niveles de contador al inicio y al final del proceso de carga y la cantidad de energía.

Además, el comprobante de factura indica para cada tiempo de inicio y cada tiempo de final el número de contador, el nivel de contador, el estado de aparato de medición y la firma 36. Esta firma 36 es la firma calculada en la estación de carga 2. Estos datos también están disponibles de modo que se pueden consultar en línea por los usuarios utilizando el identificador de transacción 19.

Asimismo, claves de aparato de medición públicas están disponibles para el usuario de modo que se pueden consultar.

En una etapa 74, el usuario puede comprobar las firmas que se le han comunicado con el identificador de transacción 19 que ha apuntado e informaciones de tiempo e identificaciones de aparato de medición. Para ello puede utilizar las informaciones apuntadas junto con las informaciones comunicadas con respecto al identificador de transacción 19, al nivel de contador y al estado para comprobar la firma con la clave de aparato de medición pública. Para ello puede usar un programa también proporcionado de modo que se puede consultar.

Con ayuda del procedimiento mostrado es posible asegurar la integridad de datos y la autenticidad en la transmisión de datos de medición entre una estación de carga y una centralita de contabilización. El uso de una firma que se puede crear mediante un procedimiento de cifrado ECC y que, por ejemplo, se puede calcular a partir de un código hash, permite comprobar la autenticidad y la integridad de los valores de medición en los dispositivos de recepción. El cálculo de las firmas se puede realizar mediante procedimientos de clave pública. La ventaja de ello es que los paquetes de datos que se calculan no se amplían innecesariamente debido a la firma. La longitud de los paquetes de datos es un criterio significativo del tráfico de datos entre la estación de carga 2 y la centralita de contabilización 22. La firma y un posible cifrado no deben provocar un aumento excesivo de los paquetes de datos, ya que, en caso contrario, el volumen de datos sería demasiado grande. Por tanto, para el uso masivo son especialmente adecuados procedimientos de clave pública.

REIVINDICACIONES

1. Procedimiento para asignar un valor de medición registrado por una estación de carga a un identificador de transacción que comprende

- asignar un identificador de transacción (19) a un proceso de carga actual,
- liberar una corriente de carga en una recepción del identificador de transacción (19) en la estación de carga (2),
- registrar en la estación de carga (2) al menos un nivel de contador de aparato de medición que representa la cantidad de energía recibida por un vehículo (6) de la estación de carga (2),
- crear un paquete de datos (34) que comprende al menos el nivel de contador de aparato de medición y el identificador de transacción (19)
- crear una descripción unívoca del paquete de datos (34),
- transmitir al menos el paquete de datos (34) y la descripción (36) a la centralita de contabilización (22).

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que** una centralita de contabilización (22) recibe un identificador de transacción (19) comunicado a un usuario o por que el identificador de transacción (19) se crea en la estación de carga o lo recibe un usuario y se transmite a la centralita de contabilización (22).

3. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que e**n la estación de carga (2) se crea una información de pago y por que la información de pago creada se transmite a la centralita de contabilización (22).

4. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado por que** a continuación de la transmisión de la información de pago se recibe el identificador de transacción (19) en la estación de carga (2).

5. Procedimiento de acuerdo con una de las reivindicaciones 1 a 2, **caracterizado por que** el identificador de transacción (19) está formado en parte a partir de informaciones de usuario y/o por que el identificador de transacción (19) está formado en parte a partir de una información de usuario determinada por un teléfono móvil o una tarjeta de telefonía móvil del usuario y/o por que el identificador de transacción está impreso sobre una tarjeta de saldo y/o por que el identificador de transacción se recibe de un cajero automático.

6. Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, **caracterizado por que** el paquete de datos (34) incluye, además del identificador de transacción (19) y del nivel de contador de aparato de medición, al menos una de las informaciones de entre

A) una identificación de aparato de medición,
B) un estado de aparato de medición,
C) informaciones de tiempo,
D) informaciones de fecha,
E) una clave de aparato de medición pública (34e);
F) un índice de tiempo;
G) una información de usuario;
H) una información de pago.

7. Procedimiento de acuerdo con una de las reivindicaciones 1 a 6, **caracterizado por que** la descripción unívoca se crea en el aparato de medición (10).

8. Procedimiento para asignar un valor de medición registrado por una estación de carga a un identificador de transacción, que comprende

- recibir en una centralita de contabilización (22) un paquete de datos (34) que comprende al menos un nivel de contador de aparato de medición y el identificador de transacción (19) de un aparato de medición (10) que mide la cantidad de energía recibida por un vehículo (6) de la estación de carga (2),
- recibir de la estación de carga (2)en la centralita de contabilización (22) una descripción unívoca del paquete de datos (34),
- comprobar la descripción unívoca con ayuda del paquete de datos (34) recibido,
- almacenar la cantidad de energía recibida determinada a partir del nivel de contador de aparato de medición junto con el identificador de transacción (19) contenido en el paquete de datos,
- proporcionar un acceso protegido por al menos el identificador de transacción (19) a al menos la cantidad de energía recibida determinada a partir del nivel de contador de aparato de medición.

9. Procedimiento de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado por que** un identificador de transacción (19) se crea en la centralita de contabilización (22) y por que el identificador de transacción (19) creado se transmite a un usuario y a una estación de carga (2).

10. Procedimiento de acuerdo con una de las reivindicaciones 1 a 9, **caracterizado por que** se recibe una solicitud de carga de un usuario y por que, a continuación de la solicitud de carga recibida, se crea el identificador de

transacción (19) y/o por que a partir de la solicitud de carga se determinan al menos informaciones de fuente que definen la fuente de la solicitud de carga y por que el identificador de transacción (19) incluye al menos en parte las informaciones de fuente.

11. Procedimiento de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado por que** el identificador de transacción (19) se crea al menos en parte a partir de un identificador de cliente temporal, creándose el identificador de cliente temporal preferiblemente en la centralita de contabilización (22).

12. Procedimiento de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado por que** se crea un comprobante de factura a partir de al menos el nivel de contador de aparato de medición recibido y por que se proporciona un acceso al comprobante de factura de forma asegurada mediante el identificador de transacción (19) mediante una red de área amplia.

13. Dispositivo para asignar un valor de medición registrado por una estación de carga a un identificador de transacción asignado a un proceso de carga actual que comprende

- un dispositivo de medición (10) que está configurado para registrar en la estación de carga (2) al menos un nivel de contador de aparato de medición que representa la cantidad de energía recibida por un vehículo (6) de la estación de carga (2),
- medios de recepción (3) que están configurados para recibir el identificador de transacción (19),
- medios de cálculo (16) que están configurados para crear un paquete de datos (34) que comprende al menos el nivel de contador de aparato de medición y el identificador de transacción (19), y para crear una descripción unívoca del paquete de datos,
- y un dispositivo de comunicación (16a) que está configurado para transmitir a la centralita de contabilización (22) al menos el paquete de datos (34) y la descripción unívoca.

14. Dispositivo para asignar un valor de medición registrado por una estación de carga a un identificador de transacción asignado a un proceso de carga actual que comprende

- medios de recepción que están configurados para recibir un paquete de datos (34) que comprende al menos un nivel de contador de aparato de medición de un aparato de medición (10) que mide la cantidad de energía recibida por un vehículo (6) de la estación de carga (2) y el identificador de transacción (19), y para recibir una descripción unívoca del paquete de datos (34) en una centralita de contabilización (22) central, y
- medios de evaluación que están configurados para evaluar la descripción unívoca y para determinar el identificador de transacción (19) a partir del paquete de datos (24),
- medios de almacenamiento que están configurados para almacenar la cantidad de energía recibida determinada a partir del nivel de contador de aparato de medición junto con el identificador de transacción (19) contenido en el paquete de datos y
- medios de provisión que están configurados para proporcionar un acceso protegido mediante al menos el identificador de transacción (19) a al menos la cantidad de energía recibida determinada a partir del nivel de contador de aparato de medición.

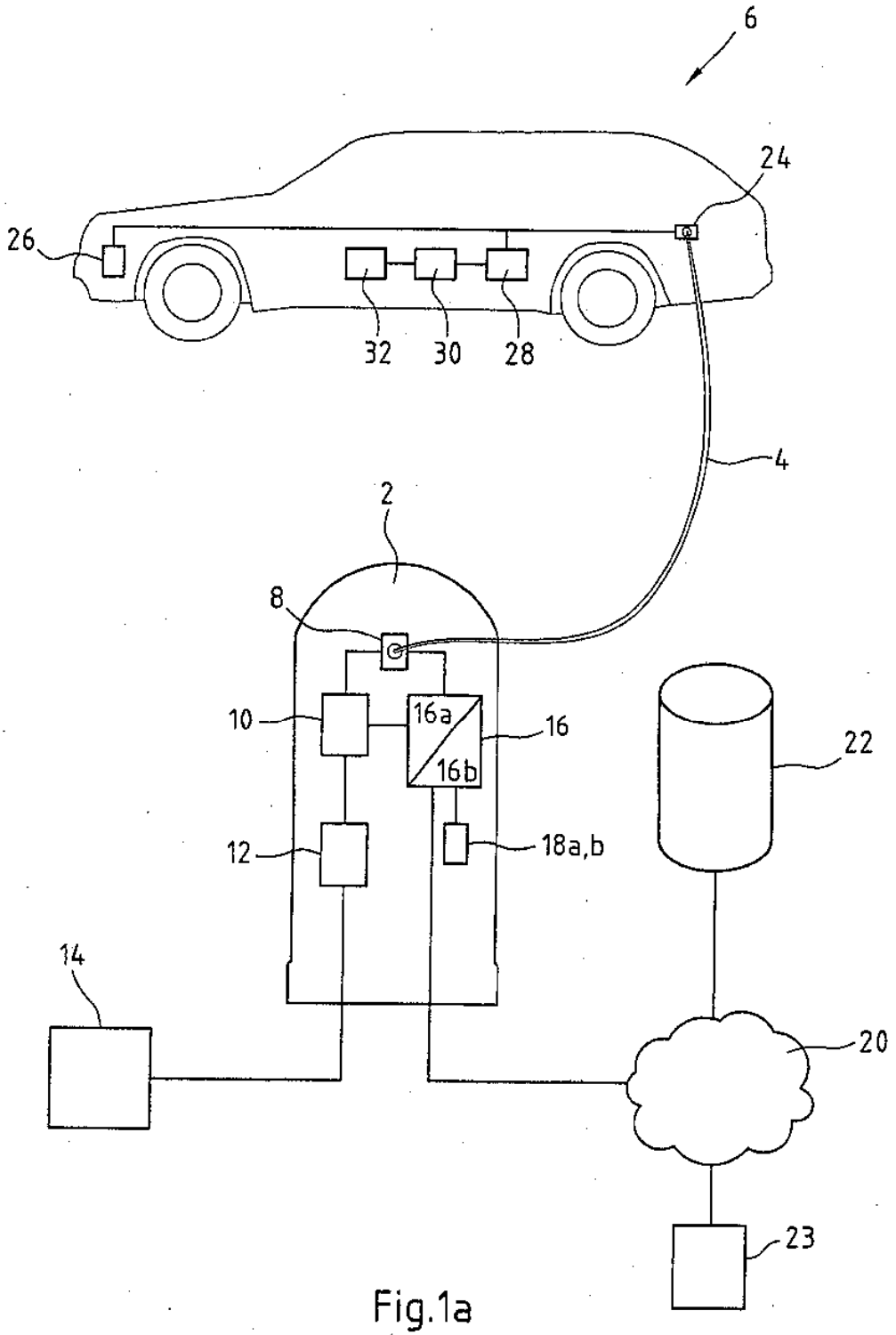

Fig.1a

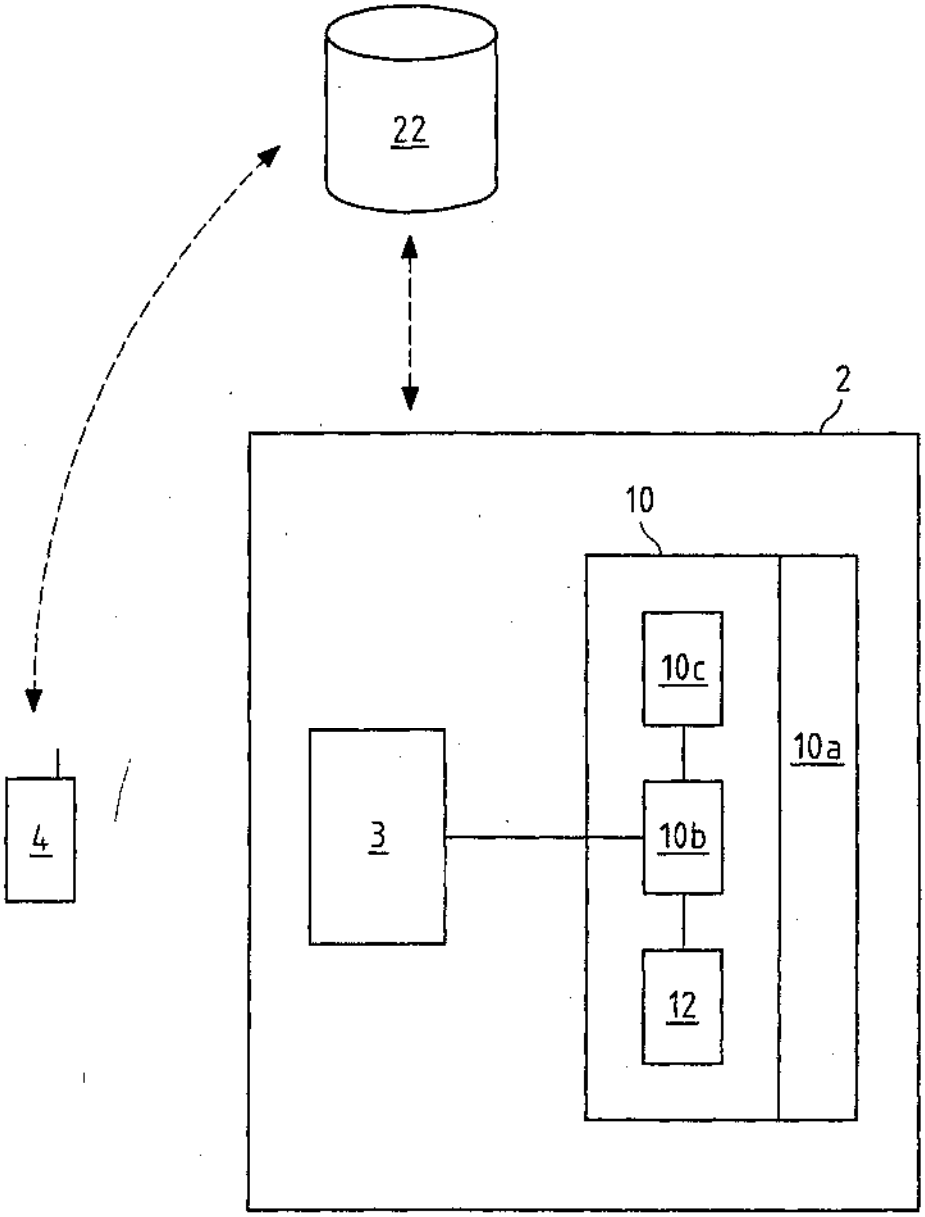

Fig.1b

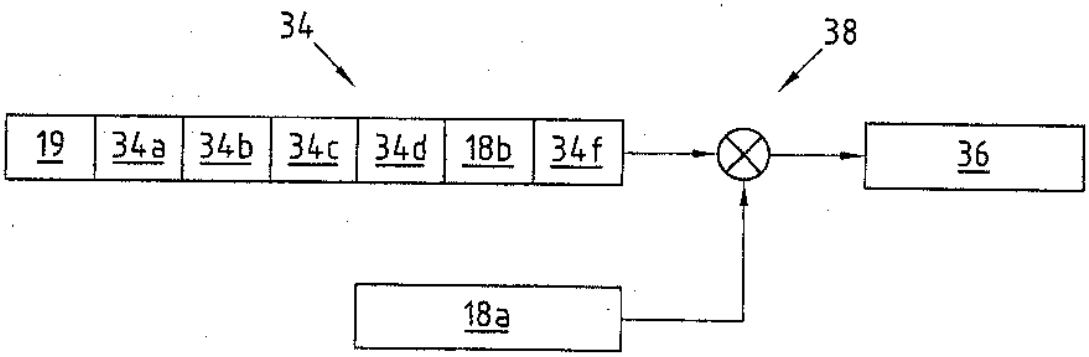

Fig.2a

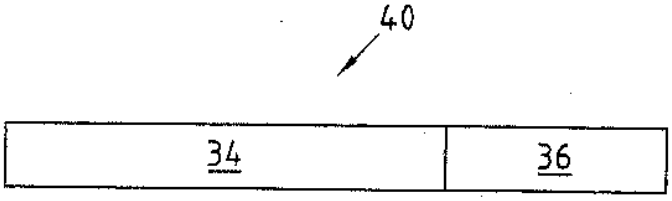

Fig.2b

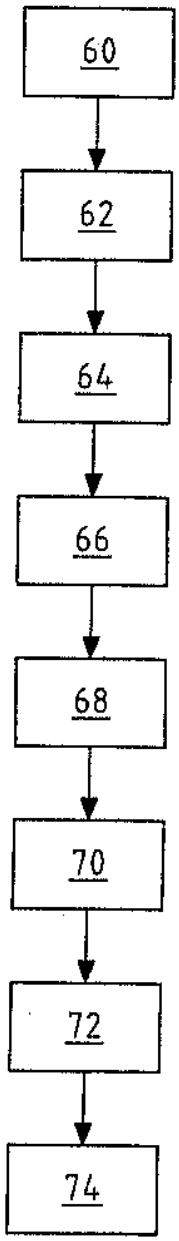

Fig.3