(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 733 132**

(51) Int. CI.:

B60L 11/18 (2006.01)
H04L 9/32 (2006.01)
G08C 25/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.02.2011 PCT/EP2011/052904**

(87) Fecha y número de publicación internacional: **10.11.2011 WO11138059**

(96) Fecha de presentación y número de la solicitud europea: **28.02.2011 E 11705582 (2)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2019 EP 2531368**

(54) Título: **Procedimiento y dispositivo para asociar a un usuario un valor medido detectado por una estación de carga**

(30) Prioridad:

28.07.2010 DE 102010032580
03.05.2010 DE 102010019244

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2019

(73) Titular/es:

INNOGY SE (100.0%)
Opernplatz 1
45128 Essen, DE

(72) Inventor/es:

GAUL, ARMIN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y dispositivo para asociar a un usuario un valor medido detectado por una estación de carga

El objeto de la invención se refiere a un procedimiento como también a un dispositivo para asociar a un usuario con un valor medido detectado por una estación de carga.

La difusión de vehículos operados eléctricamente aumentará presumiblemente en forma rápida en el futuro próximo. Sin embargo, junto con la difusión de los vehículos eléctricos que son operados mediante un motor eléctrico, debería asegurarse que éstos sean reabastecidos de la manera más sencilla posible con energía. A tal efecto debería ponerse a disposición una infraestructura funcional.

En especial debería darse la posibilidad de adquirir energía para vehículos eléctricos en espacios públicos. Con las autonomías actualmente disponibles de los vehículos eléctricos de entre 50 km y unos pocos centenares de kilómetros, se da por sentado que también es posible una recarga de los vehículos fuera del entorno doméstico. A tal efecto, es necesario poner a disposición estaciones de carga en espacios públicos, a efectos de poner a disposición un suministro continuo de energía para vehículos eléctricos por medio de una red de suministro. Esta disponibilidad de energía eléctrica o bien de estaciones de carga es un criterio decisivo para la aceptación de los vehículos eléctricos.

Sin embargo, en cuanto a las estaciones de carga instaladas en espacios públicos, hay que asegurarse de que el cliente pague la energía adquirida. También debe asegurarse que el cliente tenga conocimiento acerca de los costos previsibles antes de la adquisición de la energía eléctrica. De manera similar al procedimiento convencional para la recarga del tanque de combustible líquido, el cliente ha de saber directamente antes de recargar su batería cuáles son los costos que deberá afrontar. Así, el cliente ha de conocer, por ejemplo, el precio de 1 kW hora. También hay que asegurarse de que al cliente se le debite realmente sólo aquella cantidad de energía que también haya adquirido. Finalmente, hay que asegurarse que el cliente también pague solamente aquellos procesos de reabastecimiento eléctrico que también hayan sido originados por él. Debe impedirse de manera segura que los datos medidos de procesos de reabastecimiento eléctrico individuales de varios clientes sean debitados en paralelo a un cliente en particular.

En especial en el caso de la movilidad eléctrica, se llevan a cabo procesos de carga de clientes sumamente diversos en una y la misma estación de carga. Los procesos de carga no están bajo el control permanente del operador del lugar de medición ni del cliente, por lo que es necesario asegurar que los valores medidos detectados por la estación de carga o bien por el aparato de medición en la estación de carga sean comunicados a una central de facturación sin alterar y de manera inequívoca asociables a un cliente en particular.

Por lo tanto, debe prestarse especial atención a la integridad, autenticidad, verificabilidad y asociabilidad de los datos de facturación transmitidos entre el vehículo y la estación de carga como también entre la estación de carga y la central de facturación. Por una parte es necesario que los datos relacionados con la cantidad de carga y/o con el usuario permanezcan sin adulterar. Por otra parte debe asegurarse contra manipulaciones una transmisión de los datos de medición (datos de facturación) desde la estación de carga a un sistema de facturación. El usuario ha de poder asegurar y verificar que se le factura solamente la energía adquirida por él. También debe asegurarse que un proceso de carga sea puesto a disposición del usuario correcto una sola vez.

El documento DE 20 2008 014 766 U1 describe un contador móvil de corriente eléctrica para la adquisición de energía eléctrica, independiente del lugar, de una unidad de almacenamiento y consumo móvil con un acumulador, en un puesto de suministro de energía eléctrica localmente fijo.

El documento DE 102 04 065 A1 se refiere a un procedimiento y a una disposición para el tratamiento de datos detectados por instrumentos individualmente identificados para la captación de datos como también a un producto programa de ordenador correspondiente y a un medio de almacenamiento correspondiente, que pueden utilizarse en especial en una “Facility and Energie Management”.

El documento DE 20 2008 014 768 U1 describe un dispositivo de control para una estación de suministro de energía eléctrica, que es adecuado para adquirir energía eléctrica y/o para almacenar energía eléctrica en una unidad móvil de almacenamiento y consumo.

En base a estas consideraciones el objeto de la presente es el de poner a disposición un procedimiento como también un dispositivo que garanticen una detección, comunicación y facturación, a pruebas de falsificaciones, de datos de medición, para la energía eléctrica adquirida en una estación de carga.

Este objetivo se logra específicamente mediante un procedimiento según la reivindicación 1 o 10, como también mediante un dispositivo según la reivindicación 11 o 12.

Durante el proceso de carga, el vehículo eléctrico se abastece de energía eléctrica desde la estación de carga. En la estación de carga se mide esta energía eléctrica con ayuda de un aparato de medición (un contador). Durante el proceso de carga como también al terminar el proceso de carga es necesario que la cantidad de energía adquirida

sea detectada para fines de facturación y que el usuario del vehículo obtenga un conocimiento acerca de la cantidad energética adquirida. Por lo general, la medición de por sí no será objeto de reparos por cuanto dicha medición se lleva a cabo mediante un contador calibrado. Al respecto cabe solamente asegurarse que el valor de la medición sea comunicado de manera segura a la central de facturación, para lo cual es necesario asegurar una asociación inequívoca, no falsificable, referida a un cliente/contrato.

A tal efecto se propone que en la estación de carga se capte una identificación del usuario (ID del usuario/ID del contrato o similar). La identificación del usuario puede ser un número y/o una secuencia de números. La identificación del usuario puede estar asociada a una contraseña.

El usuario puede comunicar su identificación de usuario antes de un proceso de carga en la estación de carga. Con ayuda de la identificación de usuario así detectada es posible asociar el valor de medición estáticamente a un usuario determinado. A tal efecto se propone que al paquete de datos formado por al menos el valor medido y la identificación del usuario se halla asociada una descripción inequívoca.

La descripción inequívoca puede estar configurada de manera que describa inequívocamente el paquete de datos. Una modificación en el paquete de datos conduciría a una descripción modificada. De esta manera, partiendo de un paquete de datos recibido y conociendo las especificaciones de elaboración para la descripción inequívoca, es posible establecer una descripción comparativa y compararla con la descripción inequívoca también recibida. Si ambas descripciones son diferentes entre sí, en tal caso debe partirse de una modificación del paquete de datos, es decir, de por lo menos una modificación de la identificación de usuario o del valor medido.

Se ha comprobado que, por lo general, la medición de la cantidad de energía adquirida es correcta y también que ha sido medida por un contador calibrado inspeccionado. Por lo tanto, solamente cabe la pregunta de cómo debe asegurarse que la cantidad de energía medida sea facturada exclusivamente al usuario correcto. Esto se logra mediante la vinculación del paquete de datos con la designación inequívoca. En especial, se emprende la designación inequívoca mediante el aparato de medición, que está calibrado y, por lo tanto, especialmente es digno de confianza.

El paquete de datos y las descripciones unívocas asociadas entre sí se ponen preferiblemente a disposición de un vehículo y/o de una central de facturación. A continuación, la central de facturación puede calcular a partir del paquete de datos recibido y mediante la especificación de cálculo por ella conocida, una descripción comparativa y comparar ésta con la descripción ligada al paquete de datos. Si existen diferencias puede llegarse a la conclusión de que hubo una manipulación de los datos. En este caso, es posible desechar el valor de medición y recurrir a otras medidas. Si la comparación es positiva, en tal caso, del paquete de datos puede extraerse la identificación del usuario y facturar al usuario asociado (el cliente) la cantidad de energía adquirida.

El paquete de datos, junto con la descripción, puede ser almacenado en memoria. De esta manera, es posible una verificación posterior de que un cliente determinado también ha iniciado un proceso de carga asociado, en el que ha puesto a disposición su identificación de usuario.

También es posible comunicar el paquete de datos junto con la designación al vehículo. En el vehículo el usuario puede entonces verificar eventualmente de manera inmediata, después del proceso de carga, si el paquete de datos es correcto y eventualmente signarlo. De esta manera, el vehículo, utilizando la especificación de cálculo conocida, también puede calcular una descripción comparativa y compararla con la descripción recibida.

De acuerdo con un ejemplo de realización, se propone que la descripción unívoca sea una primera firma o expresión protocolar para la protocolización unívoca permanente de una lectura del aparato de medición vinculada a la identificación del usuario.

Para permitir que el vehículo o bien el usuario del vehículo confirme y verifique por lo menos los datos de facturación y/o la cantidad de energía adquirida, se propone la firma electrónica del paquete de datos juntamente con la descripción y la subsiguiente comunicación desde la estación de carga al vehículo (y/o inversamente) y/o a la central de facturación.

En lo que sigue, los términos “firma”, “firmar”, etc. se utilizan en el sentido de una firma electrónica de técnica de datos. Mediante la firma electrónica del paquete de datos, puede asegurarse que el mismo ya no es objeto de una manipulación ulterior.

La expresión protocolar puede establecerse en la estación de carga y ser recuperada regularmente por la estación de carga. A partir de dicha expresión protocolar, puede reconocerse de manera unívoca cuál proceso de carga está vinculado con qué datos de usuario. En el caso de una verificación, es posible comparar las expresiones protocolares con la facturación del cliente y puede establecerse si se han utilizado datos de medición para más de una facturación. Los controles pueden ser de tipo aleatorio.

Como ya se describió con anterioridad, se propone que la descripción unívoca esté vinculada con el contenido del paquete de datos de modo que una modificación del contenido del paquete de datos tenga como efecto una descripción modificada. De esta manera, puede establecerse una relación de uno a uno entre el paquete de datos y

la descripción. Si se modifica tan sólo un bit en el paquete de datos, esto conduciría a una modificación de la descripción. En la estación de carga, preferiblemente en el aparato de medición de la estación de carga, se halla registrada una especificación de cálculo que permite elaborar una descripción unívoca a partir del paquete de datos. Esto puede tener lugar mediante la utilización de claves como se describe también a continuación. Si la especificación de cálculo y eventualmente la clave es conocida en el receptor, puede calcular una descripción comparativa a partir del paquete de datos recibido y compararla con la descripción asociada al paquete de datos y con ello descubrir manipulaciones. También es posible una verificación unívoca de una utilización de una estación de carga por el cliente, gracias al procedimiento descrito.

Para establecer la descripción unívoca, se propone también que por lo menos una parte de la clave del aparato de medición sea detectada. Puede tratarse de una clave privada que permita establecer la designación unívoca de que la misma es a prueba de manipulaciones.

También se propone que la primera firma del paquete de datos sea elaborada con ayuda de la clave del aparato de medición. La firma puede calcularse por sobre la totalidad del paquete de datos o de un resumen criptográfico del paquete de datos. También es posible firmar en primera instancia el paquete de datos a partir del estado del aparato de medición y de la identificación del usuario, resumir el paquete de datos y la firma en un nuevo paquete de datos y a continuación añadir otros datos, enumerados en lo que sigue, al nuevo paquete de datos. Este nuevo paquete de datos con los datos adicionales puede firmarse de nuevo.

De acuerdo con un ejemplo de realización se propone que el paquete de datos, además de la identificación del usuario y del estado de lectura del aparato de medición contenga por lo menos otros datos de entre una identificación del aparato de medición, un status del aparato de medición, informaciones temporales, informaciones de fechas, una identificación del contrato, una clave pública del aparato de medición o un índice de tiempo. Esta enumeración no es limitativa y puede completarse con otros datos relevantes.

Una introducción especialmente sencilla de la identificación del usuario es posible cuando la identificación del usuario es una secuencia ASCII.

Para la asociación unívoca de los datos de medición a un cliente, dicha asociación debe tener lugar lo más directamente posible en el lugar de la medición, a efectos de excluir ampliamente eventuales manipulaciones. Por ello se propone que las etapas de acuerdo con la reivindicación 1 sean efectuadas en el lado de la estación de carga.

También se propone que la identificación del usuario sea detectada mediante medios de detección dispuestos en la estación de carga. Los medios de identificación pueden estar dispuestos en, sobre o fuera de la estación de carga.

Se propone que la identificación del usuario sea detectada por la estación de carga mediante la introducción alámbrica mediante RFID, introducción manual por el usuario, datos biométricos del usuario, desde el vehículo y/o en forma inalámbrica. De esta manera, se posibilita detectar la identificación del usuario mediante procedimientos biométricos (escaneo de huellas digitales, escaneo del rostro, escaneo de iris o similares) por la estación de carga.

La identificación del usuario también puede ser leída desde por un transpondedor en una clave del vehículo o por otro transpondedor, por ejemplo, en el cable de carga o en la ficha de enchufe del cable de carga.

Además de ello, es posible detectar la identificación del usuario en una memoria en el cable de carga o en la ficha de enchufe del cable de carga y que sea leída allí por la estación de carga.

Además de la cantidad de energía y de la identificación de usuario, la estación de carga detecta por lo menos también una identificación del aparato de medición. Puede tratarse de un número del aparato. La identificación del aparato de medición puede ser también la identificación adicional de la estación de carga. Con ayuda de por lo menos estos valores, es posible ampliar el paquete de datos.

Con ayuda de un valor univoco, preferiblemente binario, elaborado a partir del paquete de datos y de una clave asociada al aparato de medición (contador) o a la estación de carga, es posible calcular una firma. A partir del paquete de datos, es posible calcular un valor de referencia, por ejemplo, un código de resumen criptográfico. Este valor de referencia también puede utilizarse para calcular la firma. Esta firma puede calcularse, por ejemplo, con ayuda del código de resumen criptográfico y de una clave asociada al aparato de medición (contador) o asociada a la estación de carga. También es posible calcular una firma directamente a partir del paquete de datos y a partir de la clave asociada al aparato de medición (contador) o asociada a la estación de carga.

La realización de una firma puede ser la elaboración de un criptograma como firma con ayuda de una clave preferiblemente binaria, en donde con ayuda de la clave y del paquete de datos por firmar o bien del valor de referencia elaborado a partir del mismo se establece un criptograma preferiblemente binario. Mediante un criptograma de este tipo es posible verificar si el paquete de datos ha sido realmente elaborado por la estación de carga.

Por ejemplo, en ocasión de un proceso de carga es posible que el usuario, al inicio de un proceso de carga, anote la

identificación del aparato de medición, que por ejemplo se halla dispuesto exteriormente en la carcasa de la estación de carga, y adicionalmente anote la hora del día del inicio del proceso de carga. Al final del proceso de carga, el usuario puede anotar nuevamente la hora del día.

Cuando estas informaciones temporales, junto con el estado de la lectura del aparato de medición, lleguen a ser parte del correspondiente paquete de datos, el usuario puede verificar la firma de este paquete de datos si el usuario conoce adicionalmente la clave pública del aparato de medición.

Por ejemplo, es posible que al inicio y al final de cada proceso de carga el usuario tome nota de la identificación del aparato de medición y de la hora correspondiente del día.

La estación de carga elabora un paquete de datos, que contiene una identificación del contrato o del usuario en un paquete en el paquete de datos y adicionalmente, por ejemplo, la hora del día como también la identificación del aparato de medición. Adicionalmente el paquete de datos puede contener el estado de la lectura del aparato de medición o el status del aparato de medición.

El status del aparato de medición puede contener una información acerca de la funcionalidad técnica de la estación de carga, por ejemplo, un valor binario que indique si la estación de carga opera libre de errores.

Con ayuda de la clave privada del aparato de medición, es posible elaborar una firma a partir de este paquete de datos. La firma junto con el paquete de datos puede ser comunicada desde la estación de carga a la estación de facturación.

Por medio de la firma del paquete de datos, se asegura que los valores de medición contenidos en el paquete de datos y la identificación del usuario están asociados entre sí de manera inseparable. Si se modifica uno de ambos valores, resultaría otra firma. Si el usuario también puede detectar por sí mismo la información temporal, puede comprobar si hubo una manipulación del valor de medición, si éste contiene la información temporal.

Al final de un intervalo de facturación, el operador de la red de corriente eléctrica/proveedor de la energía eléctrica proporciona al usuario una facturación por la cantidad de energía adquirida por éste. En este cálculo puede estar enumerado, por ejemplo, cada proceso de carga codificado en función de inicio y final del proceso de carga.

Adicionalmente, a cada posición de facturación puede estar asociada la identificación del aparato de medición, por ejemplo, una ID del punto de carga, como también un número de contador. Adicionalmente, a cada posición de facturación pueden estar asociados el estado de la lectura, inicial y final, del medidor como también los momentos de inicio y final (hora del día, fecha) de cada posición de facturación. Con esta información es posible comunicar al cliente en la facturación la cantidad de energía adquirida en cada proceso de carga.

Además de ello, el cliente puede obtener junto con la factura correspondiente a cada posición de facturación una información acerca del status del aparato de medición como también la firma de que ha sido elaborada por el correspondiente paquete de datos. Para cada posición de la facturación, es posible elaborar, por ejemplo, dos firmas. Una primera firma para el paquete de datos que ha sido elaborada al inicio del proceso de carga, y una segunda firma para el paquete de datos que ha sido elaborada al final del proceso de carga.

Mediante la utilización de la identificación del usuario en el paquete de datos, el usuario puede también verificar si la cantidad de energía indicada en la facturación está realmente asociada a su identificación de usuario.

A continuación, al usuario puede comunicársele la clave pública del aparato de medición.

Dado que el cliente ha anotado de manera autónoma tanto la identificación del usuario, la identificación del aparato de medición como también la hora del día del correspondiente proceso de carga, juntamente con las informaciones adicionales contenidas en la facturación, por ejemplo la identificación del punto de carga, número del contador, lectura del medidor y la clave pública, puede verificar individualmente la firma, comunicada a él, para cada paquete de datos. Con ello puede calcular, por ejemplo, el valor de referencia mediante la firma comunicada a él y mediante la clave comunicada a él. El cliente puede calcular un valor de referencia comparativo, por ejemplo, mediante la información anotada por él y las informaciones adicionales contenidas en la facturación y verificar si los datos son idénticos. Con ello, el cliente tiene la posibilidad de verificar si las posiciones de la facturación son correctas.

Por ejemplo, puede recalcular mediante una clave conocida en el lado del receptor, adecuada correspondiente a la clave de firma, el valor de referencia o el paquete de datos por firmar a partir de la firma. A tal efecto, es posible calcular, por ejemplo, en el lado del receptor un valor de referencia comparativo partiendo del paquete de datos. Si el valor de referencia calculado y el valor de referencia comparativo coinciden, puede suponerse que los datos son íntegros.

Por ejemplo, a partir de los datos útiles (paquete de datos) es posible calcular un valor de referencia. A partir de este valor de referencia es posible calcular una firma mediante una clave privada. La firma, junto con los datos útiles, puede ser enviada a un contenedor de datos, en forma de dos conjuntos de datos separados o integrados en un receptor. A partir de la firma, el receptor puede calcular la clave pública correspondiente a la clave privada. A partir

de los datos útiles también recibidos es también posible calcular en el lado del receptor un valor de referencia comparativo. Si el valor de referencia y el valor de referencia comparativo concuerdan, puede asegurarse la integridad, autentificación, autenticidad de los datos útiles.

De manera ventajosa, al cliente se le comunica junto con la facturación para cada paquete de datos una firma por separado. Para cada posición de la facturación, compuesta de dos mediciones, a saber, el inicio y el final de un proceso de carga, se dispone de dos conjuntos de datos, o bien en el caso de un cambio de tarifa (con tres o cuatro mediciones) se encuentran a disposición tres o cuatro conjuntos de datos, a saber, el inicio y el final del proceso de carga como también un conjunto de datos adicional para el cambio de tarifa o dos conjuntos de datos, uno para el final de la primera tarifa y una para el final de la segunda tarifa, o bien los correspondientes instantes de tiempo dentro de una tarifa, a cada uno de los cuales está asociada una firma. El primer conjunto de datos determina el inicio del proceso de carga y contiene adicionalmente, por ejemplo, identificaciones del aparato de medición (ID del punto de carga, número de contador), el estado de lectura del medidor y la palabra de status. Para el final del proceso de carga existe un segundo conjunto de datos, que contiene el instante de tiempo del final del proceso de carga. Rige análogamente para el conjunto de datos en caso de un cambio de tarifas, a los que también están asociados una información de tiempo, una identificación del aparato de medición y un estado de lectura del medidor.

Para cada conjunto de datos, se calcula en la estación de carga una firma que se pone a disposición al usuario en lenguaje claro. El usuario puede verificar si la firma es correcta mediante la ayuda de la identificación, anotada por él, del contador y de la información temporal juntamente con las informaciones comunicadas a él, acerca de la lectura del medidor y de la palabra de status como también de la clave pública, lo cual le permite calcular una firma de comparación y verificar si la firma comunicada es idéntica a la firma de comparación calculada. La utilidad fundamental de un conjunto de datos para el usuario resulta del hecho que compara el número de identificación del punto de carga (el contador) como también las informaciones temporales (fecha y/o hora del día) con sus anotaciones.

Por el hecho de que la firma comunicada puede asociarse de manera unívoca al paquete de datos, el usuario puede comprobar una eventual manipulación del valor de la lectura del aparato de medición, por cuanto en este caso la firma comunicada a él ya no coincide con la firma calculada por él. Una lectura modificada del medidor con idénticas informaciones acerca de la hora del día de la carga y/o de la identificación del aparato de medición conduciría a otra firma. Sin embargo, es preferible que el cliente anote por sí mismo la hora del día del proceso de carga como también la identificación del aparato de medición, de modo que pueda reconocer una eventual manipulación en cuanto a la lectura del aparato de medición.

La expresión “firma electrónica” comprende también datos vinculados con informaciones electrónicas, mediante los que es posible identificar el firmante o bien la persona que efectuó la firma y puede verificarse la integridad de las informaciones electrónicas firmadas. En cuanto a las informaciones electrónicas, por lo general, se trata de documentos electrónicos. Con ello, desde el punto de vista técnico, la firma electrónica satisface la misma función que una firma de puño y letra sobre documentos de papel. La expresión “firma electrónica” puede comprender también una firma digital. La expresión “firma digital” puede referirse a una firma criptográfica, basada exclusivamente en tecnología de datos, en la que se utilizan métodos matemáticos criptográficos. Las “firmas electrónicas” pueden ser datos en forma electrónica, añadidos a otros datos electrónicos o vinculados lógicamente con ellos, y que sirven para la autenticación.

Si durante la comunicación se modifican valores dentro del paquete de datos, podrá establecerse en el lado de recepción o bien en el vehículo o bien en la central de facturación que la firma transmitida junto con el paquete de datos no pasa al paquete de datos recibido y que debe haber tenido lugar una modificación del paquete de datos. En el caso de datos modificados, 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 comparativo tiene como un resultado una diferencia entre ambos valores.

Según un ejemplo de realización ventajoso, se propone que se elabore el paquete de datos y la descripción unívoca, por lo menos al inicio y al final de un proceso de carga y/o cíclicamente durante un proceso de carga y sea comunicado al vehículo y/o a la estación de facturación. Por lo tanto, en la estación de facturación puede elaborarse a partir de ambos paquetes de datos una posición de facturación, en la que se evalúa la modificación del estado de lectura del aparato de medición y en base a esta modificación se calcula una cantidad de energía. Junto con informaciones sobre las tarifas, es posible determinar un importe de facturación gracias a la cantidad de energía calculada. Por el hecho de que para cada paquete de datos se elabora una firma y que el usuario al inicio y al final de cada proceso de carga anote por su cuenta información temporal, las parte del paquete de datos y con ello relevantes para la firma, el usuario puede verificar con ayuda de la firma si las informaciones base de la facturación son correctas o no.

También se propone que el paquete de datos y la descripción unívoca sean elaborados en el instante de tiempo de un cambio de tarifa, en donde en el instante de tiempo de un cambio de tarifa se elabora un primer paquete de datos y la correspondiente firma para un final de una primera tarifa y un segundo paquete de datos y la correspondiente firma para un inicio de una segunda tarifa, o solamente un paquete de datos que represente el cambio de tarifa. De esta manera, se asegura que, en caso de un cambio de tarifa, sea posible comprobar la cantidad de energía

adquirida bajo una tarifa determinada. Si cambia la tarifa durante un proceso de carga, en tal caso se detecta el estado del contador del aparato de medición en el momento del cambio de tarifa. Con ayuda de esta lectura del medidor y de la información temporal inmediatamente antes del cambio de tarifa, se elabora un primer paquete de datos y juntamente con la información temporal, inmediatamente después de un cambio de tarifa, se elabora un segundo paquete de datos. Cada uno de los paquetes de datos recibe una firma y es comunicado a la estación de facturación, de manera tal que sea posible una verificación. Como alternativa, es también posible elaborar un paquete de datos para el instante de tiempo del cambio de tarifa.

De acuerdo con un ejemplo de realización ventajoso, se propone que la estación de carga y/o la estación de facturación, calcule una cantidad de energía a partir del estado de lectura del aparato de medición, al inicio de un proceso de carga, y a partir del estado de lectura del aparato de medición al final de un proceso de carga, o en caso de un cambio de tarifa. Con ayuda de la diferencia entre las lecturas correspondientes del aparato de medición es posible calcular una cantidad de energía que puede utilizarse para elaborar una posición de facturación.

Como ya se explicó en lo que precede, la estación de facturación puede poner a disposición datos de facturación relacionados con la cantidad de energía adquirido. Estos datos de facturación pueden comunicarse al usuario en el alcance de una facturación. La facturación puede estar compuesta de varios elementos. Así por ejemplo, una primera página de una facturación puede enumerar la suma de las posiciones de facturación individuales por tarifa. Una segunda página de una facturación puede emitir para cada posición de la facturación un instante de tiempo de inicio y de terminación. Además pueden emitirse informaciones relacionadas con la identificación de los aparatos de medición, por ejemplo, la ID de un punto de carga, como también un número de contador. También es posible emitir la dirección de la correspondiente estación de carga. Adicionalmente, para cada instante de tiempo puede emitirse una lectura del medidor e indicarla juntamente con una tarifa en la facturación. Adicionalmente, para cada proceso de carga puede emitirse la cantidad de energía adquirida.

En otra página, una facturación puede emitir informaciones temporales para cada posición de la facturación. Además, puede informarse el número de contador o una identificación cualquiera de un aparato de medición juntamente con la lectura del medidor y/o un status del aparato de medición. Estos datos pueden haber sido, por ejemplo, componentes del paquete de datos. En la misma línea puede indicarse una firma resultante de los datos indicados y de la clave del aparato de medición.

A continuación, en otra página de la facturación, puede indicarse una clave pública para cada aparato de medición.

La clave pública puede ser verificada juntamente con las informaciones que son comunicadas al usuario para cada paquete de datos para determinar si la firma es correcta. Dado que el usuario ha anotado tanto el instante de tiempo como también el número del contador, puede verificar mediante las informaciones anotadas por el mismo la firma para establecer su autenticidad e integridad.

También es posible mantener a disposición las informaciones arriba mencionadas de manera descargable, en especial mediante una red de área amplia, por ejemplo, por intermedio de Internet.

De acuerdo con un ejemplo de realización ventajoso, se propone que los datos de facturación se mantengan disponibles protegidos contra acceso. En especial, los datos relacionados con la facturación y con los clientes pueden mantenerse disponibles protegidos contra acceso, por ejemplo, protegidos mediante contraseña junto con una identificación de usuario o de contrato. De esta manera, se asegura que solamente las partes autorizadas tengan acceso a información de facturación. Sin embargo, el acceso a la clave pública de los correspondientes aparatos de medición puede estar protegido de manera tal que todos los clientes de un proveedor de energía tengan un acceso en común. Como alternativa puede aún renunciarse por completo a una protección contra acceso.

Para asegurar que del lado del proveedor de energía eléctrica no pueda tener lugar ninguna manipulación de los datos de facturación, lo que, por ejemplo, sería posible manipulando la clave pública, se propone que la clave pública de aparatos de medición de los aparatos de medición de la estaciones de carga sea puesta a disposición por una ordenador lógica y/o especialmente separada de la estación de facturación. En especial, las claves públicas pueden quedar reservadas en un lugar de calibración o de verificación, de manera de hacer que una manipulación por el proveedor de energía eléctrica sea imposible.

Para facilitarle al cliente la verificación de los datos de la facturación, se propone poner a disposición un programa de ordenador para el cálculo y/o verificación de la firma para la lectura correspondientemente asociada del aparato de medición. Este programa puede calcular la firma, por ejemplo, a partir de los datos de facturación disponible en línea o también a partir de los datos de facturación ingresados por el cliente. Por ejemplo, el cliente puede ingresar manualmente el instante de tiempo anotado por él como también el número de contador anotado por él. Junto con estas informaciones, el programa puede calcular la firma a partir de las informaciones de facturación, por ejemplo, la lectura del medidor y la palabra de status, utilizando la clave pública. Esta firma a continuación puede ser comparada automáticamente por el programa con la firma que estaba contenida en los datos de facturación. Sin embargo, el cliente puede llevar a cabo esta verificación por sí mismo, ya que la firma de comparación calculada por el programa se emite en texto claro y la firma base de los datos de facturación también se emite en texto claro. Este programa puede ser puesto a disposición por un ordenador lógico y/o espacialmente separado de la estación de

facturación. En especial, un lugar de calibración puede poner a disposición este programa junto con la clave pública.

De acuerdo con un ejemplo de realización, en el aparato de medición o en la estación de carga puede haberse almacenado una clave pública de aparato de medición (PuM) y una clave privada del aparato de medición (PiM). Con ayuda de la clave privada de aparato de medición (PiM) es posible elaborar una primera firma (SD) del paquete de datos. Con ello puede calcularse un criptograma, por ejemplo, a partir de un valor de referencia asociado al paquete de datos, con ayuda de la clave privada del aparato de medición (PiM). Este valor de referencia puede ser un código de resumen criptográfico.

En el lado de recepción, por ejemplo, en una central de facturación o por medio del usuario, es posible verificar la autenticidad y la integridad de los datos del paquete de datos recibido decodificando el criptograma recibido con ayuda de la clave pública del aparato de medición, conocido en el lado del receptor, y con ello se calcula el valor de referencia. Una comparación con un valor de referencia calculado en el lado del receptor a partir del paquete de datos permite verificar la integridad de los datos.

Por el hecho de que con una clave pública asociada unívocamente con un usuario, un vehículo o un contrato sea posible decodificar el criptograma y en caso de una correspondiente certificación del par de claves asociados entre sí, es también posible verificar la autenticidad de la firma. La firma puede calcularse a partir de un valor de referencia o directamente a partir del paquete de datos.

Por ejemplo, es posible que la clave pública del aparato de medición (PuM) sea conocida en una central de facturación. La clave pública del aparato de medición (PuM) también puede estar contenida en el paquete de datos.

Un código de resumen criptográfico puede calcularse mediante un procedimiento de cálculo unívoco como un valor de referencia estadísticamente unívoco. Un código de resumen criptográfico puede ser un valor determinado a partir de una pluralidad finita de valores. Debido a la pluralidad del código de resumen criptográfico posible, tiene lugar una modificación del conjunto de datos, obteniéndose un código de resumen criptográfico modificado. El hecho de que dos conjuntos de datos diferentes generen un mismo código de resumen criptográfico, en función del número y tipo de coeficientes para el cálculo del resumen criptográfico, es sumamente improbable. Para esta probabilidad es esencial el procedimiento para el cálculo del valor del resumen criptográfico. Los ejemplos de métodos para el cálculo del código de resumen criptográfico pueden comprender MD2, MD4, MD5, SHA, RIPEMD-160, Tiger, HAVAL, Whirlpool, LM-Hash o NTLM. También son adecuados otros procedimientos, en especial procedimientos criptográficos.

Una función de resumen criptológico debería ser por lo menos una función de una vía. Las denominadas funciones de resumen criptográfico de una sola vía (One-Way-Hash Functions, OWHFs) satisfacen la condición de ser una función de una sola vía, es decir, con respecto a un valor de salida dado h(x) = y es prácticamente imposible hallar un valor de entrada x (en inglés: preimage resistance). Además, una función de resumen criptográfico es más adecuada para la criptografía cuando en lo posible no se presente ninguna colisión. Es decir, que para dos valores x y x' distintos, el valor de resumen criptográfico (código de resumen criptográfico) también ha de ser lo más distinto posible: h(x) no es igual a h(x'). Si este es siempre el caso, puede hablarse de una función de resumen criptográfico resistente a las colisiones (Collision Resistant Hash Function, CRHF).

Con ayuda de la primera firma (SD) y del paquete de datos recibido en la central de facturación, es posible verificar la autenticidad e integridad del paquete de datos elaborado por la estación de carga. En la central de facturación o para el usuario, la clave pública del aparato de medición (PuM) es conocida o fue recibida por la estación de carga. Además, en la estación de carga se recibió la primera firma. A partir de la primera firma, es posible calcular un valor de referencia con ayuda de la clave pública del aparato de medición (PuM), que puede ser comparado con un valor de referencia comparativo calculado a partir del paquete de datos. De esta manera, puede verificarse si los datos de medición contenidos en el paquete de datos han sido manipulados en el tramo de comunicación que abarca desde la estación de carga hasta el vehículo y de regreso y, finalmente, hacia la central de facturación.

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

En especial, se propone la determinación de una firma con ayuda de un procedimiento de criptografía de curva elíptica. De esta manera, es posible utilizar, por ejemplo, un procedimiento ECC de 192 bits.

De acuerdo con un ejemplo de realización ventajoso se propone también que el paquete de datos sea firmado mediante un procedimiento asimétrico. En este procedimiento, para la decodificación de la firma se utiliza, como se explicó lo que precede, una clave privada para una firma y una clave pública conocida en el lado del receptor.

Para posibilitar una asociación de un valor de medición a un instante de tiempo de medición, se propone que el paquete de datos contenga un índice de tiempo. Un índice de tiempo puede ser por ejemplo un índice de segundos, que en el sentido matemático y a lo largo de la vida útil total del aparato de carga crece de una manera estrictamente monótona y representa un número natural. Con ayuda del índice de segundos es posible llevar a cabo una asociación unívoca del instante de medición a un valor de medición. También es posible utilizar un contador de segundos operativos que puede ser un número natural que crece de manera monótona, cuya finalidad es la

asociación unívoca del instante de tiempo de un acontecimiento con respecto al tiempo legal adoptado como sistema de referencia.

Para informar al vehículo de manera continua acerca del valor de medición instantáneo, de modo que, por ejemplo, un usuario sea informado por medio del panel de carga acerca de la energía adquirida, se propone que se determine cíclicamente por lo menos un valor medido por la estación de carga y que se intercambie un paquete de datos que contenga por lo menos el valor de medición entre la estación de carga y el vehículo eléctrico.

La estación de carga puede también comunicar a la central de facturación un paquete de datos elaborado y firmado al inicio de una medición y un paquete de datos elaborado al final de la medición, a efectos de poder calcular en dicha central la cantidad de energía adquirida a partir del valor delta de los valores de medición.

Al final de un proceso de carga, también es posible calcular un valor delta a partir de los valores de medición, con lo cual este valor delta puede por lo menos entregar información acerca de la cantidad de energía adquirida. Un paquete de datos con este valor delta puede comunicarse a la central de facturación.

Las características del procedimiento y de los dispositivos pueden combinarse arbitrariamente entre sí. En especial es posible combinar las características de las reivindicaciones independientes prescindiendo de las características de las reivindicaciones independientes en forma individual o libremente combinadas entre sí de modo autónomo.

Los procedimientos mencionados en lo que precede también pueden implementarse como programa de ordenador o como programa de ordenador almacenado en un medio de memoria. De esta manera, es posible programar de modo adecuada mediante un programa de ordenador en el lado del vehículo, en el lado de la estación de carga y/o en el lado de la estación de facturación, un microprocesador para implementar las correspondientes etapas del procedimiento.

A continuación, se explica el objeto de la invención con mayor detenimiento mediante dibujos representativos de un ejemplo de realización. En los dibujos:

la Figura 1a es la representación esquemática de la estructura de un sistema para cargar un vehículo eléctrico;

la Figura 1b es una representación esquemática de un aparato de medición con medios de detección para detectar una identificación del usuario;

las Figuras 2a-d representan ejemplos de paquetes de datos y de firmas; y

la Figura 3 es un diagrama de flujo de un ejemplo de procedimiento.

La Figura 1 muestra una estación de carga 2 que por medio de un cable de conexión 4 está conectada eléctricamente a un vehículo 6. En la estación de carga 2 se ha previsto una caja de conexiones 8 para la conexión del cable de conexión 4. Por intermedio del cable de conexión 4 se transmite, por una parte, energía y, por otra parte, se intercambian datos entre el vehículo 6 y la estación de carga 2.

La caja de conexiones 8 está conectada eléctricamente a un aparato de medición 10. El apoyo de medición 10 mide la potencia eléctrica que, por intermedio de la caja de conexiones 8, es entregada al vehículo 6 por intermedio del cable de conexión 4. La potencia eléctrica es tomada por intermedio de una conexión eléctrica 12 desde una red de suministro de energía eléctrica 14.

Acoplado al aparato de medición 10 hay una unidad de ordenador 16 con una unidad de comunicaciones 16a y una unidad de firma 16b. La unidad de firma 16b puede detectar una identificación unívoca asociada al aparato de carga 2 o bien al aparato de medición 10, por ejemplo, una clave privada del aparato de medición (PiM) 18a. También puede detectarse una clave pública del aparato de medición (PuM) 18b.

La unidad de ordenador 16 está conectada a una central de facturación 22 por intermedio de una red de datos 20.

Además, se ha previsto otro ordenador 23 separado lógica y espacialmente con respecto a la central de facturación 22. En especial, el ordenador 23 puede estar conectado a la red de datos 20, por ejemplo, una red de área amplia, por ejemplo, Internet. El ordenador 23 puede ser operado, por ejemplo, en los espacios y/o bajo la supervisión de un organismo de calibración oficial.

Por intermedio de la red de datos 20, los usuarios pueden acceder tanto a la central de facturación 22 como también al ordenador 23. En la central de facturación 22, los usuarios pueden descargar datos de facturación. En el ordenador 23, los usuarios pueden obtener, por ejemplo, claves públicas de aparatos de medición y/o programas para calcular una firma comparativa.

En el vehículo 6, además de una batería 26 conectada a una unidad 24, se ha previsto una unidad de comunicaciones 28. La unidad de comunicaciones 28 permite el envío y la recepción de datos en el cable de conexión 4. Hay una unidad de firma 30 acoplada a la unidad de comunicaciones 28. La unidad de firma 30 puede detectar una identificación unívoca 32 desde el vehículo 6.

Durante el proceso de carga del vehículo 6 en la estación de carga 2 se introduce energía eléctrica procedente de la red de suministro de energía eléctrica 14 en la batería 26 del vehículo 6. La cantidad de energía introducida es detectada por el aparato de medición 10. La cantidad de energía eléctrica, por ejemplo una lectura de contador del aparato de medición 10, como también otros datos, tales como, por ejemplo, la identificación de la estación de carga 2 y/o la identificación del aparato de medición 10, un sello de hora, un índice de tiempo, un status de la estación de carga 2 y/o un status del aparato de medición 10, una lectura inicial del contador, una lectura final del contador y/o similares, pueden ser complicados por intermedio del cable de conexión 4 al vehículo 6 y/o a la central de facturación 22.

Para una asociación unívoca del valor numérico del aparato de medición con respecto a un cliente debe formarse un paquete de datos configurado como lectura del contador e identificación del usuario junto con una descripción unívoca, por ejemplo, una firma. A tal efecto se lee una identificación de usuario 19 por intermedio de la estación de carga.

Esto se muestra por ejemplo en la Figura 1b. En la Figura 1b, se muestra un aparato de medición 10 con un medidor de corriente eléctrica 10a. La lectura del contador del aparato de medición del medidor de corriente eléctrica 10a puede ser emitida por el aparato de medición 10. Esto puede dar lugar de manera codificada y firmada, como se describe en lo que sigue. A tal efecto, en el aparato de medición 10 puede estar dispuesto el equipamiento de firma 12. En el aparato de medición 10 puede haberse dispuesto una CPU 10b, y la clave del aparato de medición 18 consistente en la clave privada del aparato de medición 18a y clave pública del aparato de medición 18b puede estar almacenada en memoria.

La CPU 10b está conectada a un aparato de lectura de transpondedor 3. Este aparato de lectura de transpondedor 3 puede estar dispuesto en el aparato de medición 10 o fuera del mismo. Por intermedio del aparato de lectura de transpondedor, es posible leer una identificación de usuario 19 desde un transpondedor dispuesto en una ficha de cable de carga 4a.

También el aparato de lectura 3 del transpondedor puede ser reemplazado por otro aparato de lectura. Por ejemplo, puede establecerse una comunicación con el vehículo 2 y por intermedio de un conductor piloto del cable de carga 4 podría detectarse la identificación del usuario.

El aparato de lectura también podría ser un teclado a través del cual el usuario ingresa su identificación de usuario. También la identificación de usuario podría ser leída de una tarjeta de chip o tarjeta de banda magnética del usuario, por intermedio del aparato de lectura.

También podría ponerse a disposición la identificación de usuario 19 al aparato de lectura 3 desde una central de facturación 22. En tal caso un usuario podría liberar, por ejemplo, un proceso de carga telefónicamente en la central de facturación 22, mediante la mención de la ID de la estación de carga. A tal efecto debería dar a conocer por ejemplo su identificación del usuario 19 y una contraseña a la central de facturación 22. Si una verificación de la contraseña es positiva, en tal caso la central de facturación 22 puede comunicar, por ejemplo, de manera codificada, la identificación de usuario por intermedio de la red de datos 20 a la estación de carga 2 y al aparato de lectura 3.

Para ahora vincular los datos de facturación firmemente con la identificación del usuario, se propone que un paquete de datos comunique a la central de facturación 22 el estado de la lectura del aparato de medición y la identificación de usuario.

A tal efecto, la unidad de comunicaciones 16 transmite un paquete de datos, como se muestra en la Figura 2. En el paquete de datos pueden estar almacenadas las mencionadas magnitudes de medición. En el paquete de datos puede almacenarse en especial una clave pública del aparato de medición (PuM) 18b. Además del paquete de datos pueden intercambiarse la clave pública del aparato de medición (PuM) 18b y/o las firmas entre la estación de carga 2 y el vehículo 6 y/o la central de facturación 22.

Las Figuras 2 muestran el cálculo de un paquete de datos y de una firma, que por intermedio del cable de conexión 4 entre la estación de carga 2 y el vehículo 6 y/o por intermedio de la red de datos 20 pueden ser intercambiados entre la estación de carga 2 y la central de facturación 22.

La Figura 2a muestra un ejemplo de primer paquete de datos 34, en el que se han almacenado una identificación de usuario 19, una lectura de contador 34a, opcionalmente un status del aparato de medición 34b, opcionalmente una identificación del aparato de medición 34c, opcionalmente una información del tiempo 34d, opcionalmente una clave pública del aparato de medición (PuM) 18b y/o eventualmente otros datos 34f en una secuencia numérica binaria. La identificación del aparato de medición 34c puede ser una designación unívoca del aparato de medición 10 y/o de la estación de carga 2.

Para una autenticación del primer paquete de datos 34, es posible elaborar una firma 36. A tal efecto, en una etapa de cálculo 38 se utilizan el primer paquete de 34 juntamente con una clave privada del aparato de medición (PiM) 18a, para calcular la primera firma (SD) 36. Así, por ejemplo, en la etapa de cálculo 38, puede determinarse un valor de resumen criptográfico a partir del primer paquete de datos, y este valor de resumen criptográfico puede ser convertido por cálculo con la clave privada de aparato de medición (PiM) de modo de obtener la firma (SD) 36.

Para la transmisión del primer paquete de datos 34 al vehículo 6 y/o a la central de facturación 22, se empaqueta el primer paquete de datos 34 con la firma 36 en un conjunto de datos 40. El conjunto de datos 40 es transmitido desde la estación de carga 2 por intermedio del cable de conexión 4 al vehículo 6 o por intermedio de la red de alimentación 14 o por intermedio de la red de datos 20 o de alguna otra manera a la central de facturación 22. En la Figura 2b, se muestra el conjunto de datos 40 formado a partir del primer paquete de datos 34 y la firma 36.

El conjunto de datos 40 puede ser enviado de manera directa a la central de facturación 22. Los datos así obtenidos pueden utilizarse para elaborar un cálculo como se describe en lo que sigue. El usuario puede verificar los datos de facturación utilizando la firma 36 y las anotaciones hechas por él mismo para verificar la autenticidad e integridad.

Alternativa o adicionalmente, para asegurar más aún la transmisión, es posible comunicar de inmediato el conjunto de datos al vehículo 6.

En el vehículo 6, por medio de la unidad de comunicación 28, es posible recibir el conjunto de datos 40. En la unidad de firma 30, es posible evaluar el conjunto de datos 40. De esta manera y mediante la ayuda de la primera firma (SD) 36, es posible verificar la autenticidad del primer paquete de datos 34.

A tal efecto es posible, por ejemplo, que la clave pública del aparato de medición (PuM) 18b sea conocida en el vehículo 6. Con ayuda de esta información, y a partir de la primera firma (SD) 36 en el vehículo 6 es posible invertir la etapa de cálculo 38 y calcular el paquete de datos 34. Con ayuda del paquete de datos 34 recibido y del paquete de datos calculado es posible llevar a cabo una comparación que asegure la integridad de los datos.

Después de haberse verificado en el vehículo 6 el primer paquete de datos 34, y que eventualmente se haya comprobado su integridad, como se presenta en la Figura 2c, en el vehículo 6 y mediante la unidad de firma 30, en una segunda etapa de cálculo 42 es posible calcular en primera instancia un código de resumen criptográfico 44 a partir del conjunto de datos 40.

Con ayuda del código de resumen criptográfico 44 y de una clave privada del vehículo 46 (Pi1), en una etapa de cálculo 48 puede calcularse una segunda firma (SF1) 50. A tal efecto, en la etapa de cálculo 48 puede utilizarse, por ejemplo, un procedimiento de codificación ECC. Por ejemplo, puede utilizarse un algoritmo SHA-256.

La segunda firma (SF1) 50 puede firmar nuevamente por ejemplo el primer paquete de datos 34 juntamente con la primera firma 36.

Como se representa en la Figura 2d, la unidad de firma 30 puede adjuntar la segunda firma (SF1) 50 al primer paquete de datos 34 y la primera firma (SD) 36. Adicionalmente puede adicionalmente adjuntarse opcionalmente la clave pública del vehículo (Pul). El paquete de datos así calificado 52 puede ser transmitido desde el vehículo 6 por intermedio del cable de conexión 4 a la estación de carga 2. A continuación es posible transmitir el paquete de datos calificados 52 desde la estación de carga 2 por intermedio de la unidad de comunicaciones 16a por intermedio de la red de datos 20 a la central de facturación 22. Paralelamente a ello es posible comunicar adicionalmente por ejemplo a la estación de carga el paquete de datos 34 a la central de facturación 22.

Con ayuda del paquete de datos calificados 52, es posible verificar la autenticidad e integridad del primer paquete de datos 34 y del conjunto de datos 40.

A continuación, en la central de facturación 22, es posible calcular a partir del paquete de datos 34 y de la primera firma (SD) 36 correspondiente a la etapa de cálculo 42 una firma de comparación. A partir de la segunda firma 50, en la central de facturación 22 y con ayuda de la clave pública del vehículo (Pu2) allí conocida o recibida en el paquete de datos calificados 52 es posible calcular el código de resumen criptográfico 44 mediante el procedimiento de la etapa de cálculo 48. Una comparación del código de resumen criptográfico comparativo calculado en la central de facturación mediante el código de resumen criptográfico calculado en la central de facturación a partir de la segunda firma (SF1), permite verificar la integridad de los datos. Además de ello, mediante una certificación del correspondiente par de claves, en este caso de la clave privada del vehículo (Pi2) y de la clave pública del vehículo (Pu2) puede verificarse a partir de donde se calculó la segunda firma (SF1).

Con ayuda del código de resumen criptográfico y del código de resumen criptográfico comparativo puede verificarse si el paquete de datos calificados 52 fue recibido libre de errores en la central de facturación 22.

A continuación, en la central de facturación 22 y con ayuda de la primera firma (SD) y de la clave pública del aparato de medición (PuM) 18b conocida en la central de facturación 22, puede repetirse la etapa de cálculo 38 de manera invertida y/o nuevamente. De esta manera puede verificarse si el paquete de datos 34 ha sido transmitido libre de errores desde la estación de carga 2 al vehículo 6 y desde allí de regreso a la central de facturación 22.

Si el paquete de datos 34 y la firma 36 concuerdan, puede considerarse esto como un fundamento de que el paquete de datos no ha sido falsificado. Dado que en el paquete de datos está contenida la identificación de usuario 19, puede establecerse con ello que la energía eléctrica adquirida ha sido facturada al cliente correcto.

Para un cliente, con ayuda de la primera asignatura (SD) o bien de la clave pública del aparato de medición (PuM)

18b es también posible verificar si el paquete de datos 34 utilizado en la central de facturación 22 para fines de facturación también procede efectivamente de las estaciones de carga 2 de las que ha extraído energía eléctrica.

A tal efecto el usuario puede descargar desde el ordenador 23 la clave pública del aparato de medición (PuM) 18b de la estación de carga 2, cuya ID anotó durante el proceso de carga. Puede comparar la ID de la estación de carga con una ID de estación de carga en su factura. Los datos de cálculo extraídos en esta ID de estación de carga (paquete de datos) deben proveerse en cada caso con una firma. Esta firma 36 puede ser verificada por el usuario junto con las informaciones de tiempo anotadas por él y la clave pública cargada del aparato de medición (PuM) 18b de la estación de carga 2. A tal efecto puede el usuario utilizar un programa cargado por intermedio del ordenador 23.

Las etapas de cálculo 38 y 48 pueden estar basadas en procedimientos de codificación asimétricos, los que por medio de claves públicas y privadas permiten la elaboración, la comparación y la validación de criptogramas.

Esto garantiza una elevada integridad de los datos durante la facturación. También es posible una verificación de la plausibilidad. Finalmente, se asegura que el paquete de datos 34 sea recibido no adulterado en el vehículo 6, como también no adulterado en la central de facturación 22.

La Figura 3 muestra un diagrama de flujo para que el usuario verifique los datos de medición.

En una primera etapa 60, el usuario se dirige con su vehículo 6 a una estación de carga 2. En el instante en que el cable de conexión 4 es insertado en el vehículo 6, y empieza el proceso de carga, en la estación de carga 2, preferiblemente en el aparato de medición 10 pero en lo posible también en la unidad de ordenador 16, se detecta la hora real del día o un índice de hora como también la fecha. Además, la unidad de ordenador del aparato de medición 10 detecta el estado actual del contador. Por otra parte, la unidad de ordenador detecta por lo menos también un status de la estación de carga (por ejemplo, en orden/fuera de servicio) y la identificación del aparato de medición. De esta manera es posible detectar el valor de medición, la hora del día y la fecha como también el status y firma en el aparato de medición 10.

Para dar inicio al proceso de carga, el aparato de lectura 3 también detecta la identificación de usuario 19. Esto puede leerse, por ejemplo, sin contacto mediante un transpondedor. El usuario también puede ingresar, por ejemplo, mediante un campo de teclado en el aparato de lectura 3, su identificación de usuario 19. Después del ingreso es posible verificar su validez mediante una consulta efectuada a la central de facturación 22.

También es posible que partes de los datos anteriormente mencionados sean detectadas en la unidad de ordenador 16 y que el paquete de datos sea firmado en la unidad de ordenador 16.

Paralelamente a ello, el usuario puede anotar, por ejemplo, también la hora del día y la fecha del inicio del proceso de carga. A tal efecto utiliza, por ejemplo, su propio reloj. También es posible que el usuario lea y anote la identificación del aparato de medición o las ID de los aparatos de medición preferentemente dispuestos exteriormente en la estación de carga 2.

En una segunda etapa 62, la unidad de firma 16b calcula a partir del paquete de datos 34, que contiene las informaciones arriba mencionadas, en especial la identificación del usuario, y la clave del aparato de medición 18a y la firma 36.

El paquete de datos 34 y la firma 36 son comunicados en la etapa 64 siguiente a la central de facturación 22.

En la siguiente etapa 66 el usuario concluye el proceso de carga. En este momento, la unidad de ordenador 16 detecta nuevamente la hora real del día o un índice de tiempo como también la fecha. Además, la unidad de ordenador detecta nuevamente a partir del aparato de medición 10 el estado real del medidor. Además de ello, la unidad de ordenador detecta nuevamente por lo menos también un status de la estación de carga (por ejemplo en orden / fuera de servicio y la identificación del aparato de medición.

Paralelamente a ello, el usuario puede también anotar nuevamente la hora del día y la fecha del fin del proceso de carga. Para ello utiliza, por ejemplo, su propio reloj.

En la siguiente etapa 68, la unidad de firma 16b calcula a partir del nuevo paquete de datos 34, que contiene las informaciones arriba mencionadas, y de la clave del aparato de medición 18a la nueva firma 36.

El nuevo paquete de datos 34 y la nueva firma 36 son comunicados en una etapa subsiguiente 70 a la central de facturación 22.

En la central de facturación 22, en la etapa 72 se determinan a partir de ambos paquetes de datos recibidos las informaciones relevantes para el cálculo.

Para un cliente o bien para la ID de un contrato se reúnen todos los procesos de carga a lo largo de un intervalo de tiempo de facturación.

En el momento de la facturación 74, el usuario recibe una factura. Esta factura presenta por una parte para cada tarifa la cantidad total de energía adquirida y el precio.

Además, la factura presenta para cada proceso de carga el momento de inicio y el momento de terminación, la fecha, la ID de la estación de carga, el número del contador, la dirección de la estación de carga 2, el estado de lectura del contador al inicio y al final del proceso de carga y la cantidad de energía.

Además de ello, la factura presenta para cada tiempo de inicio y para cada momento de terminación el número del contador, el estado o lectura del contador, el status del 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 al cliente para su descarga en línea.

También están disponibles al usuario para su descarga las claves públicas de los aparatos de medición

En una etapa 74 puede el cliente efectuar la verificación de las firmas comunicadas a él mediante las informaciones temporales anotadas por él y las identificaciones de los aparatos de medición. A tal efecto puede utilizar las informaciones anotadas juntamente con las informaciones comunicadas relacionadas con los status de medidor, para verificar la firma por medio de las claves públicas de los aparatos de medición. A tal efecto puede utilizar un programa puesto a disposición, también descargable.

Con ayuda del procedimiento mostrado, es posible asegurar la integridad de los datos y la autenticidad durante la transmisión de los datos de medición entre una estación de carga y un vehículo y/o una central de facturación. La utilización de una firma, que puede elaborarse mediante un procedimiento de codificación ECC, y que puede calcularse, por ejemplo, a partir de un código de resumen criptográfico, permite verificar la autenticidad y la integridad de los datos de medición en los equipamientos de recepción. El cálculo de las firmas puede efectuarse mediante procedimientos de Clave Pública. La ventaja de esto es que los paquetes de datos calculados no han de ser ampliados innecesariamente debido a la firma. La longitud de los paquetes de datos es un criterio decisivo para el tráfico de datos tanto entre la estación de carga 2 y el vehículo 6, como también entre la estación de carga 2 y la central de facturación 22. La firma como también una posible codificación no ha de permitir que los paquetes de datos se hagan demasiado grandes, ya que en caso contrario el volumen de los datos sería excesivo. Por lo tanto, para la utilización en gran escala son especialmente adecuados los procedimientos de Clave Pública.

REIVINDICACIONES

1. Procedimiento para asociar un valor de medición detectado por una estación de carga a un usuario, con:

- detección de por lo menos un estado de lectura del aparato de medición representativo de la cantidad de energía adquirida por un vehículo (6) de la estación de carga (2) en un aparato de medición (10) dentro de la estación de carga (2),

- detección de una identificación de usuario (19) por la estación de carga (2),

- elaboración de un paquete de datos (34) que comprende por lo menos el estado del medidor del aparato de medición, la identificación del usuario (19) y una designación unívoca de la estación de carga (34c);

- elaboración de una descripción unívoca del paquete de datos (34) en el aparato de medición (10);

- transmisión de por lo menos el paquete de datos (34) y de la descripción (36) desde la estación de carga (2) al vehículo eléctrico (6) y/o a una central de facturación (22).

2. Procedimiento según la reivindicación 1, caracterizado por que la descripción unívoca es una primera firma (36) o una expresión de protocolo para la protocolización unívoca duradera de un estado del contador del aparato de medición vinculado con una identificación de usuario.

3. Procedimiento según la reivindicación 1, caracterizado por que la descripción unívoca está vinculada con el contenido del paquete de datos de manera tal que tiene como efecto una descripción modificada.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado por que el paquete de datos (34) contiene, además de la identificación de usuario (19) y del estado de lectura del contador del aparato de medición, por lo menos una información de entre los siguientes:

A) una identificación del aparato de medición,

B) un status del aparato de medición,

C) informaciones temporales,

D) informaciones de fecha,

E) la identificación de un contrato,

F) una clave pública del aparato de medición (34e);

G) un índice de tiempo.

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado por que la identificación del usuario (19) se detecta en el medio de detección (3) asociado a la estación de carga (2).

6. Procedimiento según la reivindicación 5, caracterizado por que la identificación de usuario (19) es detectada por la estación de carga (2) alámbricamente, mediante RFID, ingreso manual del usuario, datos biométricos del usuario, por el vehículo y/o de manera inalámbrica.

7. Procedimiento según una de las reivindicaciones 2 a 6, caracterizado por que la clave del aparato de medición (18) contiene por lo menos una clave pública del aparato de medición (18a) y una clave privada del aparato de medición (18b) y por que la primera firma (36) se elabora con la ayuda del aparato de medición (18b).

8. Procedimiento según una de las reivindicaciones 1 a 7, caracterizado por que en la estación de carga (2) se recibe un paquete de datos calificados desde el vehículo eléctrico (6), en donde el paquete de datos calificados contiene por lo menos el paquete de datos transmitido desde la estación de carga al vehículo eléctrico, la descripción unívoca y una segunda firma (50), una tercera firma y/o una cuarta firma.

9. Estación de carga para asociar un valor de medición detectado por la estación de carga a un usuario, con:

- un equipamiento de medición (10) instalado en la estación de carga (2) para detectar por lo menos un estado del contador del aparato de medición representativo de la cantidad de energía eléctrica extraída por un vehículo (6) desde la estación de carga (2),

- medios de detección (3) para detectar una identificación de usuario (19),

- un equipamiento de firma (12) dentro del equipamiento de medición (10) instalado para detectar un paquete de datos (34) que comprende por lo menos el estado de lectura del aparato de medición y la identificación del usuario (19) y una designación unívoca de la estación de carga (34c), y para elaborar una descripción unívoca del paquete

de datos,

- y un equipamiento de comunicaciones (16a) instalado para transmitir por lo menos el paquete de datos (34) y la descripción unívoca desde la estación de carga (2) al vehículo eléctrico y/o a una central de facturación (22).

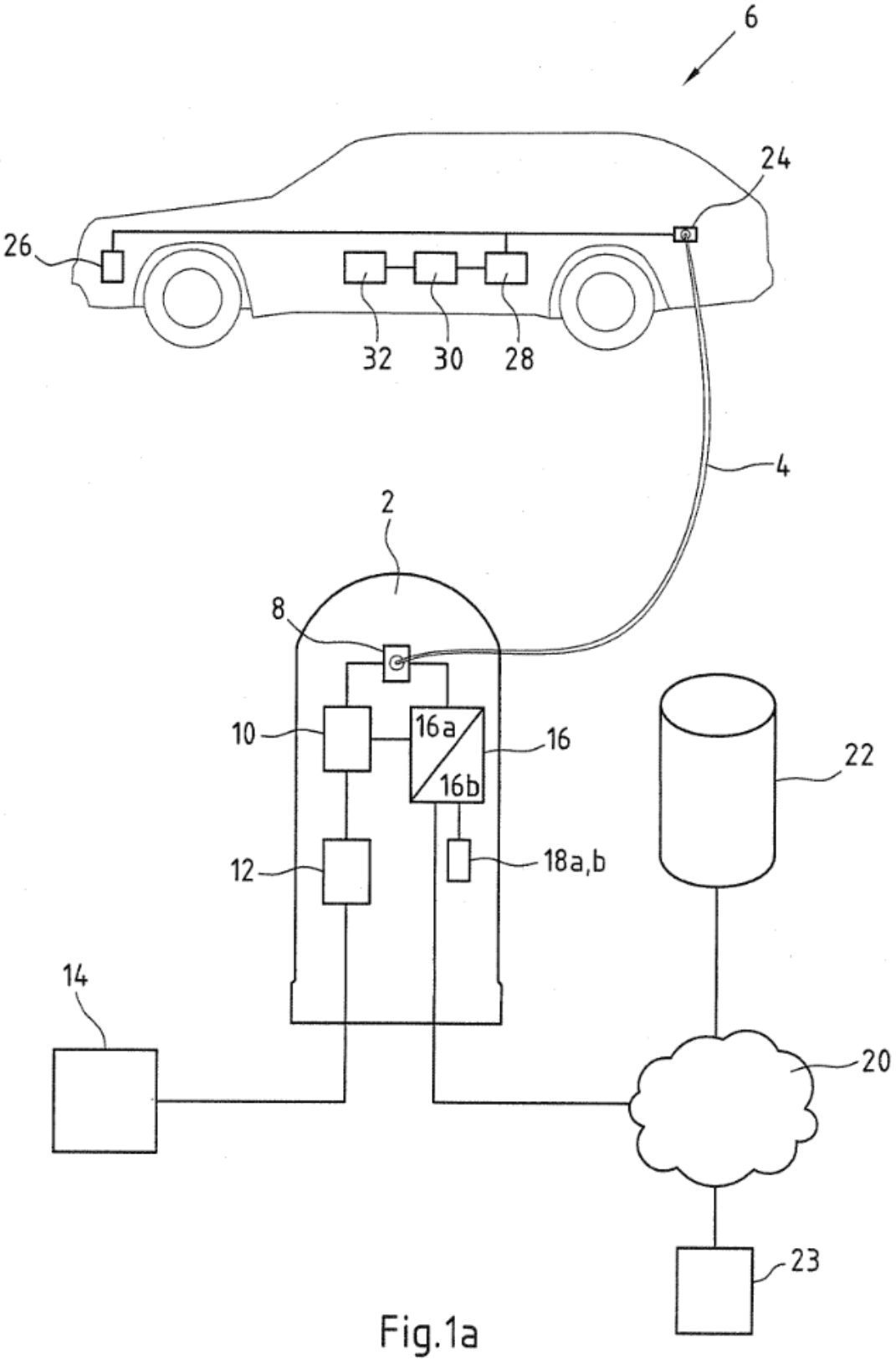

Fig.1a

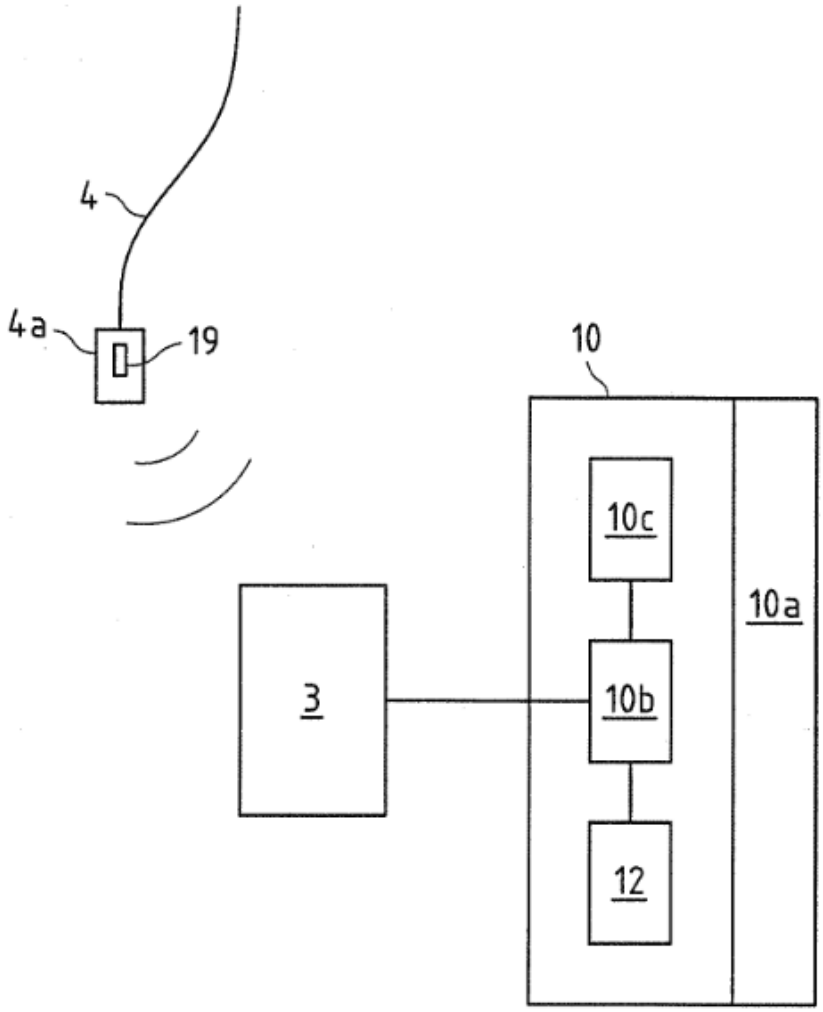

Fig.1b

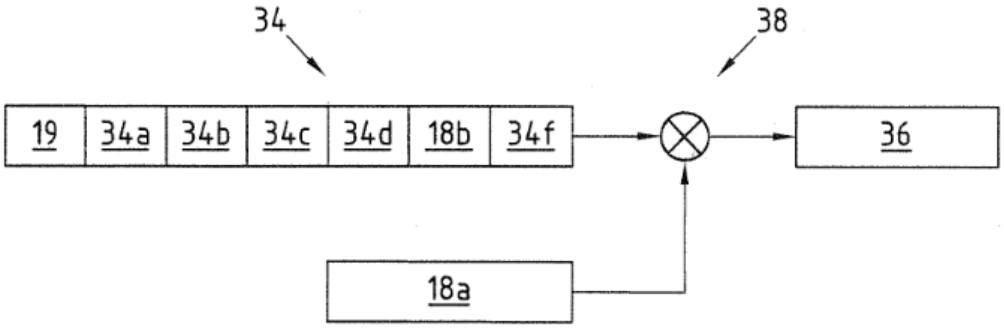

Fig.2a

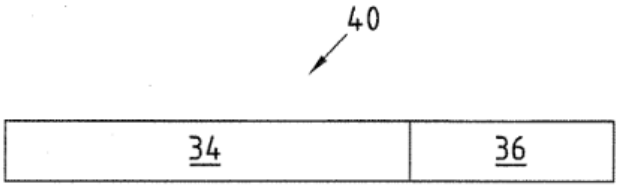

Fig.2b

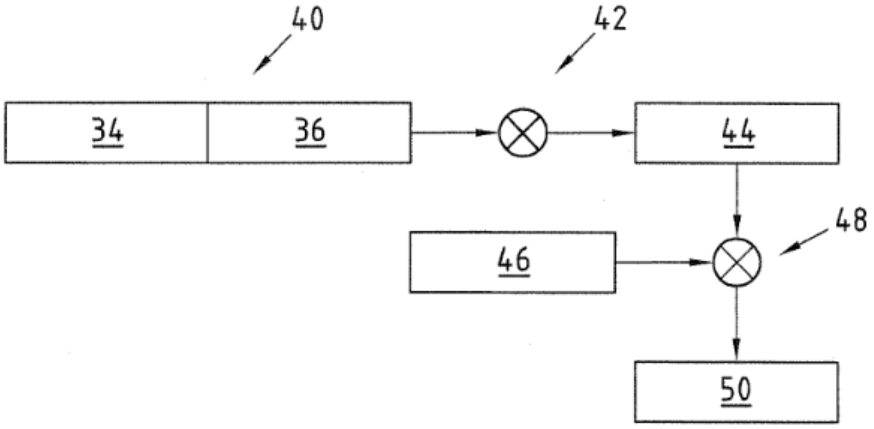

Fig.2c

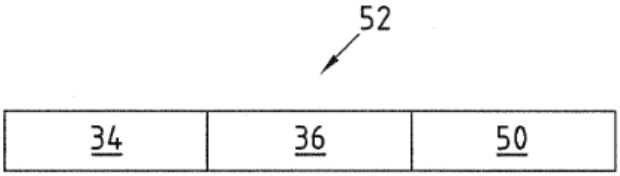

Fig.2d

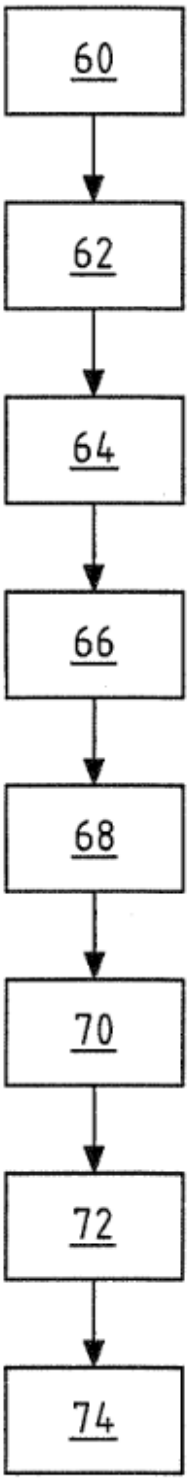

Fig.3