(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 531 414**

(51) Int. CI.:

B60L 11/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.05.2010 E 10726019 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.12.2014 EP 2445746**

(54) Título: **Aseguramiento de la facturación de energía recibida a través de una estación de carga**

(30) Prioridad:

22.06.2009 DE 102009030091
03.05.2010 DE 102010019244

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.03.2015

(73) Titular/es:

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

(72) Inventor/es:

GAUL, ARMIN;
VOIT, STEPHAN y
WISY, MARTIN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Aseguramiento de la facturación de energía recibida a través de una estación de carga

El objeto se refiere a un procedimiento para la comunicación entre una estación de carga y un vehículo así como a un dispositivo y a un sistema para la comunicación entre una estación de carga y un vehículo. El objeto se refiere también a un procedimiento y a un dispositivo para asegurar la facturación de una cantidad de energía recibida de una estación de carga.

Probablemente, la distribución de vehículos operados eléctricamente aumentará rápidamente en el futuro cercano. Sin embargo, con la distribución de vehículos eléctricos que se operan con un motor eléctrico se debería asegurar que éstos se puedan alimentar de la manera más sencilla con energía. Para ello se debería proporcionar una infraestructura que funcione.

En particular se debería ofrecer la posibilidad de recibir energía para vehículos eléctricos en áreas públicas. En el caso de los alcances disponibles hasta el momento de vehículos eléctricos 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 en áreas públicas estaciones de carga 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 decisivo para la aceptación de vehículos eléctricos.

Sin embargo, en estaciones de carga instaladas en áreas públicas se debe asegurar que el cliente pague la energía recibida. También se debería asegurar que el cliente conozca los costes a esperar antes de recibir energía eléctrica. De manera correspondiente al proceso de repostado convencional, el cliente debería saber directamente antes de la carga de la batería qué costes le esperan. Así, por ejemplo, el cliente debería conocer el precio por kilovatio-hora. Además, debería estar asegurado que al cliente se le factura realmente sólo la cantidad de energía que también ha recibido.

A este respecto se deben tener en cuenta especialmente la integridad, la autenticidad y la posibilidad de verificación de los datos de facturación transmitidos tanto entre el vehículo y la estación de carga como entre la estación de carga y la central de facturación. Por un lado, es necesario que los datos acerca de la cantidad de carga y/o del usuario permanezcan sin falsificar. Por otro lado, una transmisión de datos de medición (datos de facturación) de la estación de carga a un sistema de facturación se debe proteger frente a manipulaciones para fines de facturación. El usuario debe poder asegurar y verificar que se le factura sólo la energía que ha recibido.

El documento US 2002 132 144 A1 describe un procedimiento para traficar corriente generada mediante pilas de combustible en vehículos. A este respecto se detecta la cantidad de corriente generada mediante contadores en el vehículo, en una estación de acoplamiento así como en una central. Para comprobar las cantidades de corriente medidas se realiza una comparación de los valores de medición de los tres contadores.

El documento EP 1 995 109 A1 muestra un sistema para leer transpondedores.

El documento WO 2010 009502 A1 muestra un procedimiento para identificar vehículos eléctricos con respecto a una estación de carga.

El documento WO 2009 039406 A1 muestra un procedimiento para recargar una batería de un vehículo eléctrico.

Sin embargo, en dicho estado de la técnica no se ha detectado el problema de que debe ser técnicamente posible para un usuario poder comprobar los datos de medición indicados en sus datos de facturación. Esta comprobación debe ser posible con medios técnicamente sencillos y, al mismo tiempo, debe ser impecable con respecto a la técnica de calibrado.

Por este motivo, el objeto se basó en el objetivo de proporcionar un procedimiento así como un dispositivo que garanticen una facturación asegurada, técnicamente comprobable de energía recibida de una estación de carga.

Este objetivo se consigue según el objeto mediante un procedimiento según la reivindicación 1 así como mediante un dispositivo según la reivindicación 12.

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 detecte para fines de facturación y que el usuario del vehículo obtenga conocimientos acerca de la cantidad de energía recibida.

Para posibilitar al vehículo o al usuario del vehículo al menos confirmar y comprobar los datos de facturación y/o la cantidad de energía recibida se propone la firma electrónica y la transmisión del paquete de datos desde la estación de carga al vehículo y/o a la central de facturación.

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

La estación de carga detecta además de la cantidad de energía al menos también una identificación del aparato de medición. Esto 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 al menos de estos valores se crea un paquete de datos. El paquete de datos puede tener además del nivel de contador (nivel de contador de aparato de medición) también un estado de contador (estado de aparato de medición), una identificación de contador (identificación de aparato de medición), una identificación de estación de carga, una información de hora, una información de fecha y/o una clave de aparato de medición pública así como, dado el caso, informaciones adicionales.

Un paquete de datos se firma electrónicamente en la estación de carga. Esto posibilita comprobar la autenticidad y la integridad del paquete de datos. El paquete de datos electrónicamente firmado se transmite según el objeto al vehículo eléctrico y/o la central de facturación.

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 a partir 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, adicionalmente, apunte 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 verificar una firma de este paquete de datos por parte del usuario cuando el usuario conoce adicionalmente 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, por ejemplo, contiene 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. Además, por ejemplo, puede estar contenida una identificación de contrato o de cliente en el paquete de datos.

El estado de aparato de medición puede contener una información acerca de 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 desde la estación de carga a la estación de facturación.

Mediante la firma del paquete de datos se asegura que el valor de medición contenido en el paquete de datos y la información de tiempo están relacionados de manera inseparable entre sí. Si se modifica uno de los dos valores, entonces resultaría una firma diferente. Dado que el propio usuario puede detectar la información de tiempo, también puede detectar una manipulación del valor de medición.

Al final de un periodo de facturación, el usuario recibe del operador de red de corriente/proveedor de energía una factura con respecto a la cantidad de energía que ha recibido. En esta factura puede estar alistado, por ejemplo, cada proceso de carga de forma desglosada según el inicio y el final del proceso de carga.

Adicionalmente, a cada partida de factura puede estar asignada la identificación de aparato de medición, por ejemplo, un ID de punto de carga, y también un número de contador. Adicionalmente, los niveles de contador iniciales y finales así como los tiempos iniciales y finales (hora, fecha) pueden estar asignados a cada partida de factura. Con estas informaciones se puede comunicar al cliente en la factura la cantidad de energía recibida por cada proceso de carga.

Además, con respecto a cada partida de factura el cliente puede recibir junto con la factura una información acerca del estado de aparato de medición y la firma que se ha creado para el paquete de datos correspondiente. Para cada partida de factura, por ejemplo, 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.

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

Dado que el cliente ha apuntado de forma autónoma tanto la identificación de aparato de medición como la hora del respectivo proceso de carga puede comprobar individualmente, junto con las informaciones adicionales de la 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 la clave pública comunicada mediante la misma. Por ejemplo, el cliente puede calcular un valor de referencia de comparación mediante la información que ha apuntado y la información adicional a partir de la factura y comprobar si los datos son idénticos. Por tanto, el cliente tiene la posibilidad de comprobar si las partidas de factura son correctas.

Por ejemplo, con una clave conocida en el lado del receptor, adecuada para la clave de firma se puede calcular de manera inversa 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 se puede partir de una integridad de datos.

Por ejemplo, se puede calcular a partir de datos útiles (paquete de datos) 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 junto con los datos útiles en un contenedor de datos como dos archivos separados o de forma empotrada en los datos útiles a un receptor. El receptor puede calcular con una clave pública adecuada para la clave privada el valor de referencia a partir de la firma. 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 se puede asegurar la integridad, la autenticación y la autenticidad de los datos útiles.

De manera ventajosa, al cliente se le comunica junto con la factura para cada paquete de datos una firma separada. Para cada partida 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 en un cambio de tarifa (con tres o cuatro mediciones) tres o cuatro conjuntos de datos, 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 respectivamente una firma. El primer conjunto de datos determina el inicio del proceso de carga y contiene adicionalmente, por ejemplo, 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 contiene 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 también están asignados 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 proporciona al usuario en texto plano. El usuario puede verificar la exactitud de la firma por que con ayuda de la identificación de contador y la información de tiempo que ha apuntado junto con las informaciones que se le han comunicado acerca del nivel de contador y de la palabra de estado y de la clave pública puede calcular una firma de comparación 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 del hecho de que compara el número de identificación del punto de carga (contador) así como informaciones de tiempo (fecha y/u hora) con sus registros.

Debido al hecho de que la firma comunicada se puede asignar de manera unívoca al paquete de datos, el usuario podría detectar una manipulación del valor del nivel de contador de aparato de medición. Entonces, por tanto, la firma que se le ha comunicado ya no sería idéntica a la firma calculada por él. Un nivel de contador cambiado con informaciones idénticas acerca del momento de la carga y/o la identificación de aparato de medición conduciría a una firma diferente. Sin embargo, el cliente apunta preferiblemente el momento del proceso de carga y la propia 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 relacionados con informaciones electrónicas con los que se puede identificar el firmante o titular de la firma y verificar la integridad de las informaciones electrónicas firmadas. Por regla general, en el caso de las informaciones electrónicas se trata de documentos electrónicos. La firma electrónica cumple por tanto, desde el punto de vista técnico, la misma finalidad que una firma manuscrita en documentos de papel. Una firma electrónica puede comprender, entre otras cosas, también una firma digital. La firma digital puede designar la firma criptográfica relacionada meramente con datos en la que se aplican métodos

matemáticos criptográficos. "Firmas electrónicas" pueden ser datos en forma electrónica que se añaden a otros datos electrónicos o están relacionados lógicamente 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 el vehículo o en la central de facturación, que la firma transmitida con el paquete de datos no es adecuada para el paquete de datos recibido y tiene que haber tenido lugar una modificación 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 da como resultado una diferencia entre estos dos valores con datos cambiados.

Según un ejemplo de realización ventajoso se propone que el paquete de datos y la respectiva firma se creen al menos al inicio y al final de un proceso de carga y se transmitan a la estación de facturación. En la estación de facturación se puede crear por tanto a partir de los dos paquetes de datos una partida de factura en la que se evalúa el cambio del nivel de contador de aparato de medición y en la que se calcula una cantidad de energía mediante este cambio. Junto con informaciones de tarifa se puede determinar con la cantidad de energía calculada un importe de factura. Debido al hecho de que para cada paquete de datos se haya creado una firma y el usuario haya apuntado de forma autónoma 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 la factura son correctas o no.

También se propone que el paquete de datos y la respectiva firma 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 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 cantidad de energía recibida respectivamente con una determinada tarifa. Si cambia una tarifa durante un proceso de carga, entonces se detecta el nivel de contador del aparato de medición 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 se crea un segundo paquete de datos directamente tras un cambio de tarifa. Cada uno de los paquetes de datos se firma y se transmite a la estación de facturación de modo que es posible una comprobación. De manera alternativa se puede crear también un paquete de datos para el momento de cambio.

Según un ejemplo de realización ventajoso se propone que la estación de carga y/o la estación de facturación 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 una partida de factura.

Tal como ya se explicó anteriormente se pueden proporcionar por la estación de facturación datos de facturación con respecto a la cantidad de energía recibida. Estos datos de facturación se pueden comunicar en el marco de una factura al usuario. La factura puede estar formada por varios elementos. Así, por ejemplo, una primera página de una factura puede alistar el total de las partidas de factura individuales por cada tarifa. Una segunda página de una factura puede proporcionar para cada partida de factura un momento de inicio y un momento de final. Adicionalmente a ello se pueden proporcionar informaciones con respecto a identificaciones de aparato de medición, por ejemplo, un ID de punto de carga y un número de contador. También se puede proporcionar la dirección de la respectiva estación de carga. Adicionalmente se puede proporcionar para cada momento un nivel de contador y éste se puede indicar junto con una tarifa en la factura. Finalmente se puede proporcionar para cada proceso de carga la cantidad de energía recibida.

En una página adicional, una factura puede proporcionar para cada partida de factura informaciones de tiempo. Además se pueden proporcionar el número de contador u otra identificación de aparato de medición 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 proporcionar entonces una firma que ha resultado de los datos indicados y de la clave de aparato de medición.

Finalmente se puede indicar en una página adicional de la factura para cada aparato de medición una clave pública.

La clave pública puede verificar junto con las informaciones que se han comunicado para cada paquete de datos al usuario si la firma es correcta. Dado que el usuario ha apuntado tanto el momento como el número de contador, puede verificar la firma para determinar la autenticidad y la integridad de esta última con las informaciones que él mismo ha apuntado.

También es posible que las informaciones anteriormente mencionadas se puedan consultar, en particular se puedan facilitar a través de una red de área amplia, en particular a través de Internet.

Según un ejemplo de realización ventajoso se propone que los datos de facturación se faciliten protegidos frente a un acceso. En particular los datos relacionados con facturas y relacionados con clientes se pueden facilitar protegidos frente a un acceso, por ejemplo, protegidos con una contraseña junto con una identificación de cliente o de contrato. Por tanto se asegura que sólo personas autorizadas tienen acceso a informaciones 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 manera alternativa se puede prescindir en este caso incluso totalmente de una protección frente a un acceso.

Para asegurar que por parte del proveedor de energía no se puede realizar una manipulación de los datos de factura lo que, por ejemplo, sería posible si se manipula la clave pública, se propone que las claves de aparato de medición públicas de aparatos de medición de las estaciones de carga estén disponibles en un ordenador separado de manera lógica y/o espacial de la estación de facturación. En particular se pueden tener preparadas las claves públicas en un organismo de calibrado u organismo de control de modo que una manipulación por parte del proveedor de energía se vuelve imposible.

Para facilitarle al cliente la verificación de los datos de factura se propone que se proporcione un programa informático para calcular y/o verificar la firma para el nivel de contador de aparato de medición respectivamente asignado. Este programa puede calcular la firma, por ejemplo, a partir de los datos de factura disponibles en línea o también a partir de los datos de factura introducidos por parte de clientes. Por ejemplo, el cliente puede introducir manualmente 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. Esta firma se puede comparar entonces automáticamente mediante el programa con la firma que estaba contenida en los datos de factura. Sin embargo, también el propio cliente puede realizar esta verificación, ya que la firma de comparación calculada por el programa se proporciona en texto plano y la firma en la que se basan los datos de factura también se ha proporcionado en texto plano. Este programa se puede proporcionar por un ordenador que está separado de manera lógica y/o espacial de la estación de facturación. En particular, un organismo de calibrado puede proporcionar este programa además de las claves públicas.

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

En el lado del receptor, por ejemplo, en una central de facturación o por parte del usuario se puede verificar 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 en el lado del receptor a partir del paquete de datos posibilita la verificación de la integridad de datos.

Debido al hecho de que con una clave pública asignada de manera unívoca a un usuario, a un vehículo o a un contrato se puede descifrar el criptograma, también se puede verificar la autenticidad de la firma en caso de una certificación correspondiente de la pareja de claves pertenecientes una a la otra. La firma se puede calcular a partir de un valor de referencia o directamente a partir del paquete de datos.

El paquete de datos junto con la primera firma (SD) se puede transmitir al vehículo.

Por ejemplo, es posible que se conozca la clave de aparato de medición pública (PuM) en una central de facturación. Asimismo, la clave de aparato de medición pública (PuM) puede estar contenida en el paquete de datos.

Asimismo, la clave de aparato de medición pública se puede transmitir junto con la primera firma (SD) al vehículo. Asimismo, la clave pública (PuM) se puede transmitir a una central de facturación junto con un paquete de datos cualificados explicado en más detalle a continuación.

También se propone que el paquete de datos y la primera firma (SD) se reciban en el vehículo.

Según un ejemplo de realización ventajoso se propone que en el vehículo se cree un código Hash (H) del conjunto de datos a partir del paquete de datos y la primera firma (SD).

Un código Hash se puede calcular mediante un procedimiento de cálculo unívoco como un valor de referencia estadísticamente unívoco. 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 modificado en caso de un cambio del conjunto de datos. El hecho de que dos conjuntos de datos diferentes generen un código Hash idéntico es extremadamente poco probable dependiendo 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. Otros procedimientos, en particular procedimientos criptográficos, son igualmente adecuados. Una función Hash criptológica debería ser al menos una función unidireccional. Las denominadas funciones Hash unidireccionales (*One-Way-Hash Functions*, OWHF) cumplen con la condición de ser una función unidireccional, es decir, con respecto a un valor de salida dado h(x) = y es prácticamente imposible encontrar un valor de entrada x (en inglés *preimage resistance*). Además, una función Hash es más adecuada para la criptografía cuando no se produzcan colisiones en la medida de lo posible. Es decir, para dos valores diferentes x y x' también debería ser diferente en la medida de lo posible el valor Hash (código Hash): h(x) desigual a h(x'). Si este es siempre el caso, entonces se puede hablar de una función Hash resistente a colisiones (*Collision Resistant Hash Function*, CRHF).

Según un ejemplo de realización se propone también que el código Hash (H) se firme mediante una clave de vehículo privada (Pi2) en el lado del vehículo, con lo que se produce un código Hash criptográfico (H'). La segunda firma (SF1) así formada, que corresponde al código Hash criptográfico (H'), posibilita verificar la integridad del conjunto de datos a partir del paquete de datos y la primera firma (SD). También se puede verificar con esta segunda firma (SF1) la autenticidad de la firma cuando la pareja de claves correspondiente, que en este caso está formada a partir de la clave de vehículo privada y la clave de vehículo pública, se haya certificado y sea conocida la clave pública en el lado del receptor.

Se propone que en el lado del vehículo estén almacenadas una clave de vehículo privada (Pi2) y una clave de vehículo pública (Pu2). Junto con el conjunto de datos compuesto por el paquete de datos, la primera firma (SD) y la segunda firma (SF1), la clave de vehículo pública (Pu2) en el lado del vehículo se puede transmitir a la estación de carga y se puede recibir allí. La estación de carga puede transmitir a una central de facturación este conjunto de datos recibido, que también se denomina paquete de datos cualificados. De manera paralela a ello, la estación de carga puede transmitir un conjunto de datos formado a partir del paquete de datos y la primera firma (SD) a la central de facturación.

En la central de facturación se puede calcular con ayuda del paquete de datos recibido el código Hash (H). Con ayuda de la clave de vehículo pública (Pu2) que, dado el caso, se ha recibido por la estación de carga o por el vehículo o que ya se conoce en la central de facturación, también se puede calcular un código Hash (H) a partir de la segunda firma (SF1) o a partir del código Hash criptográfico (H'). Los dos códigos Hash calculados se pueden comparar entre sí en la central de facturación. En caso de un resultado de comparación positivo se puede concluir una transmisión de datos íntegra desde el vehículo a través de la estación de carga a la central de facturación.

Con ayuda de una segunda firma de este tipo es posible que la exactitud de los valores de medición se confirme mediante el vehículo. Esto es ventajoso para fines de facturación, ya que, de este modo, es posible una asignación del valor de medición, por un lado, a una determinada estación de carga y, por otro lado, a un vehículo o a un contrato, tal como aún se describe a continuación. Asimismo, un usuario puede estar seguro de que los datos de medición que ha confirmado también se han recibido sin errores en la central de facturación.

Con ayuda de la primera firma (SD) y el paquete de datos recibido en la central de facturación se pueden verificar también la autenticidad y la integridad del paquete de datos creado por la estación de carga. En la central de facturación o para el usuario es conocida o se ha recibido por la estación de carga la clave de aparato de medición pública (PuM). Además se ha recibido en la estación de carga la primera firma.

A partir de la primera 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 verificar si se han manipulado los datos de medición contenidos en el paquete de datos en el trayecto de comunicación desde la estación de carga hasta el vehículo y de vuelta y, a continuación, hacia la central de facturación.

En un momento antes de un proceso de carga, por ejemplo, en caso de concluir un contrato con un proveedor de energía, se pueden almacenar en el vehículo una clave de vehículo pública (Pu2) y una clave de vehículo privada (Pi2). Con ayuda de esta primera tupla se puede garantizar una asignación de valores asignados por el vehículo al vehículo así como la integridad y la autenticidad de los datos recibidos por el vehículo en la central de facturación.

Sin embargo, puede ser deseable que precisamente una asignación entre un conjunto de datos y un determinado vehículo no sea posible. Sin embargo, esta asignación se puede dar precisamente cuando el conjunto de datos recibido por la estación de carga se firme en el vehículo con ayuda de la pareja de claves de vehículo (Pi2, Pu2) en el lado del vehículo, tal como se describió anteriormente. Para evitar esta asignación es posible que en el momento de una conclusión de contrato se creen una clave de contrato pública (Pu3) y una clave de contrato privada (Pi3). Al menos la clave de contrato pública (Pu3) se puede almacenar en una central de facturación.

Además se puede formar por un vehículo para un proceso de carga una tupla a partir de una clave temporal privada (Pi4) y una clave temporal pública (Pu4). Esta tupla se puede crear por cada proceso de carga o en intervalos regulares o en intervalos irregulares.

Ante una firma de un paquete de datos en el vehículo se puede consultar la clave de contrato privada (Pi3) por el vehículo. Esto se puede realizar, por ejemplo, mediante una entrada por parte del usuario. Asimismo, la clave de contrato privada (Pi3) se puede leer eléctricamente por una clave de vehículo. Esto se puede realizar, por ejemplo, mediante un transpondedor.

Con ayuda de la clave de contrato privada se puede firmar una clave temporal pública. Con ayuda de una clave temporal privada se pueden firmar el conjunto de datos y la primera firma. En la central de facturación se puede descifrar con una clave de contrato pública conocida la clave temporal pública. Con esta clave temporal pública se puede descifrar la firma del conjunto de datos con la primera firma. Según 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 curvas elípticas. A este respecto, por ejemplo, es posible que se utilice un procedimiento ECC con 192 bits.

Según 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 posibilitar una asignación de un valor de medición a un momento 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 por toda la vida útil del aparato cargador tenga un crecimiento muy monótono en el sentido matemático y represente 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 operativos que puede ser un número natural de crecimiento monótono cuyo objetivo es la asignación unívoca del momento de un acontecimiento al tiempo legal supuesto como sistema de referencia.

Para informar al vehículo permanentemente acerca de valores de medición momentáneos de modo que, por ejemplo, un usuario esté informado acerca del estado de carga y la energía recibida, se propone que se determine cíclicamente al menos un valor de medición mediante la estación de carga y que se intercambie un paquete de datos que contiene al menos el valor de medición entre la estación de carga y el vehículo eléctrico.

Asimismo, la estación de carga puede transmitir a la central de facturación el paquete de datos creado y firmado al inicio de una medición y el paquete de datos creado al final de una medición para calcular allí la cantidad de energía extraída del delta de los valores de medición.

También se puede calcular en la estación de carga un delta a partir de los valores de medición al final de un proceso de carga, pudiendo este delta al menos dar información acerca de la cantidad de energía recibida. Un paquete de datos con este delta se puede transmitir de forma firmada al vehículo y también se puede firmar allí, tal como se describió anteriormente. El paquete de datos así firmado se puede transmitir a la central de facturación.

Un objeto adicional es un procedimiento según la reivindicación 19 así como un procedimiento según la reivindicación 41.

En el vehículo es posible verificar si el paquete de datos recibido está sin falsificar. Para ello se utiliza la firma recibida. La firma se puede verificar con ayuda de la clave pública recibida por la estación de carga. La clave pública se puede utilizar para calcular una firma de comparación en el vehículo. En el vehículo se calcula por tanto con ayuda del paquete de datos y de la clave pública una segunda firma (firma de comparación) que se compara con la firma recibida del paquete de datos. Si las firmas coinciden, el paquete de datos se ha recibido de manera inalterada. En caso contrario se debe partir de una modificación del paquete de datos. Por ejemplo, el vehículo puede transmitir entonces un mensaje de error a la estación de carga. En este caso, el paquete de datos se puede transmitir de nuevo junto con la firma. También se puede cancelar el proceso de carga tras un determinado número de transmisiones erróneas. Entonces puede ser relevante para la facturación el último paquete de datos recibido de manera no falsificada por el vehículo.

Según un objeto adicional se reivindica un dispositivo según la reivindicación 20 así como un dispositivo según la reivindicación 42.

Un objeto adicional es un dispositivo según la reivindicación 21 así como un dispositivo según la reivindicación 43.

Un objeto adicional es un sistema según la reivindicación 22 así como un sistema según la reivindicación 44.

Las características de los procedimientos y los dispositivos se pueden combinar libremente entre sí. En particular, características de las reivindicaciones dependientes pueden ser inventivas por sí solas o de manera libremente combinada entre sí evitando las características de las reivindicaciones independientes.

Los procedimientos anteriormente mencionados también se pueden realizar como programa informático o como programa informático almacenado en un medio de almacenamiento. A este respecto, en el lado del vehículo, en el lado de la estación de carga y/o en el lado de la central de facturación puede estar programado de manera adecuada un microprocesador para realizar las respectivas etapas de procedimiento mediante un programa informático.

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

La figura1 una estructura esquemática de un sistema para cargar un vehículo eléctrico;

Las figuras 2a-d 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 a través de un cable de conexión 4 con un vehículo 6. En la estación de carga 2 está prevista una caja de conexión 8 para la conexión del cable de conexión 4. A través del 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 a través de la caja de conexión 8 al vehículo 6 a través del cable de conexión 4. La potencia eléctrica se recibe a través de una conexión eléctrica 12 desde 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 detectar una identificación unívoca asignada al aparato cargador 2 o al aparato de medición 10, por ejemplo, una clave de aparato de medición privada (PiM) 18a. También se puede detectar una clave de aparato de medición pública (PuM) 18b.

La unidad de cálculo 16 está conectada a través de una red de datos 20 con una central de facturación 22.

Además está previsto un ordenador adicional 23 que está separado de manera lógica y espacial de la central de facturación 22. En particular, el ordenador 23 puede estar conectado con la red de datos 20, por ejemplo, una red de área amplia, por ejemplo, Internet. El ordenador 23 se puede operar, por ejemplo, en las localidades y/o bajo vigilancia de un organismo de calibrado.

A través de la red de datos 20, usuarios pueden acceder tanto a la central de facturación 22 como al ordenador 23. En la central de facturación 22, los usuarios pueden consultar datos de factura. En el ordenador 23, usuarios, por ejemplo, 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 posibilita el envío y la recepción de datos en el cable de conexión 4. A la unidad de comunicación 28 está conectada una unidad de firma 30. La unidad de firma 30 puede detectar una identificación 32 unívoca del vehículo 6.

Durante el proceso de carga del vehículo 6 en la estación de carga 2 se alimenta energía desde la red de alimentación de energía 14 en la batería 26 del vehículo 6. La cantidad de la energía alimentada se detecta 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 estado de contador inicial, un estado de contador final y/o similares se puede transmitir a través del cable de conexión 4 al vehículo 6 y/o a la central de facturación 22.

Para ello, la unidad de comunicación 16 transmite un paquete de datos tal como está explicado en la figura 2. En el paquete de datos se pueden almacenar dichas magnitudes de medición. En el paquete de datos también se puede almacenar una clave de aparato de medición pública (PuM) 34e. También se pueden intercambiar, además del paquete de datos, la clave de aparato de medición pública (PuM) 34e y/o 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 se pueden intercambiar a través del cable de conexión 4 entre la estación de carga 2 y el vehículo 6 y/o la central de facturación 22.

La figura 2a muestra un primer paquete de datos 34 ejemplar en el que están almacenados 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) 34e y/o posiblemente datos adicionales 34f en un orden de números binario. La identificación de aparatos 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 primera firma (SD) 36. Así, por ejemplo, se puede determinar en la etapa de cálculo 38 un valor Hash a partir del primer paquete de datos y este valor Hash se puede convertir con la clave de aparato de medición privada (PiM) en la firma (SD) 36.

Para la transmisión del primer paquete de datos 34 al vehículo 6 y/o la central de facturación 22 se embala el primer paquete de datos 34 con la firma 36 en un conjunto de datos 40. El conjunto de datos 40 se transmite por la estación de carga 2 a través del cable de conexión 4 al vehículo 6 o a través de la red de alimentación 14 o a través de la red de datos 20 o de otra manera a la central de facturación 22. 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 central de facturación 22. Los datos obtenidos de ello se pueden utilizar para una facturación, tal como aún se describirá a continuación. El usuario puede verificar los datos de factura utilizando la firma 36 y las notas que ha hecho para determinar la autenticidad y la integridad de los mismos.

Para asegurar adicionalmente la transmisión es posible de manera alternativa y/o adicional transmitir el conjunto de datos en primer lugar al vehículo 6.

En el vehículo 6 se puede recibir mediante la unidad de comunicación 28 el conjunto de datos 40. En la unidad de firma 30 se puede evaluar el conjunto de datos 40. A este respecto es posible que con ayuda de la primera firma (SD) 36 se pueda verificar la autenticidad del primer paquete de datos 34.

Para ello, por ejemplo, es posible que se conozca la clave de aparato de medición pública (PuM) 34e en el vehículo 6. Con ayuda de esta información se puede realizar una inversión desde la primera firma (SD) 36 en el vehículo 6 de la etapa de cálculo 38 y se puede calcular el paquete de datos 34. Con ayuda del paquete de datos 34 recibido y el paquete de datos calculado se puede realizar una comparación que asegure la integridad de datos.

Una vez que se haya verificado en el vehículo 6 el primer paquete de datos 34 y posiblemente se haya detectado su integridad, tal como se representa en la figura 2c, se puede calcular en el vehículo 6 mediante la unidad de firma 30 en una segunda etapa de cálculo 42 en primer lugar un código Hash 44 a partir del conjunto de datos 40.

Con ayuda del código Hash 44 y una clave de vehículo privada 46 (Pi1) se puede calcular en una etapa de cálculo 48 una segunda firma (SF1) 50. Para ello se puede utilizar en la etapa de cálculo 48, por ejemplo, un procedimiento de cifrado ECC. Por ejemplo, se puede utilizar un algoritmo SHA-256.

Por ejemplo, la segunda firma (SF1) 50 puede firmar de nuevo el primer paquete de datos 34 junto con la primera firma 36.

Tal 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, de manera opcional se puede adjuntar la clave de vehículo pública (Pu1). El paquete de datos cualificados 52 así creado se puede transmitir por el vehículo 6 a través del cable de conexión 4 a la estación de carga 2. A continuación, el paquete de datos cualificados 52 se puede transmitir por la estación de carga 2 mediante la unidad de comunicación 16a a través de la red de datos 20 a la central de facturación 22. De manera paralela a ello, por ejemplo, la estación de carga puede transmitir el paquete de datos 34 adicionalmente a la central de facturación 22.

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

En primer lugar se puede calcular en la central de facturación 22 a partir del paquete de datos 34 y de la primera firma (SD) 36 de manera correspondiente a la etapa de cálculo 42 una firma de comparación. A partir de la segunda firma 50 se puede calcular en la central de facturación 22 con ayuda de la clave de vehículo pública (Pu2) conocida allí o recibida en el paquete de datos cualificados 52 el código Hash 44 con el procedimiento de la etapa de cálculo 48. Una comparación del código Hash de comparación calculado en la central de facturación con el código Hash calculado en la central de facturación a partir de la segunda firma (SF1) posibilita la verificación de la integridad de datos. Además, mediante una certificación de la respectiva pareja de claves, en este caso de la clave de vehículo privada (Pi2) y de la clave de vehículo pública (Pu2), se puede verificar por quién se ha calculado la segunda firma (SF1).

Con ayuda del código Hash y del código Hash de comparación se puede verificar si el paquete de datos cualificados 52 se ha recibido sin errores en la central de facturación 22.

A continuación se puede realizar de manera inversa y/o de nuevo la etapa de cálculo 38 en la central de facturación 22 con ayuda de la primera firma (SD) y la clave de aparato de medición pública (PuM) conocida en la central de facturación 22. De este modo se puede verificar si el paquete de datos 34 se ha transmitido sin errores de la estación de carga 2 al vehículo 6 y, desde allí, de vuelta a la central de facturación 22.

Para un cliente es posible con ayuda de la primera firma (SD) o la clave de aparato de medición pública (PuM) una verificación para determinar si los paquetes de datos 34 utilizados en la central de facturación 22 para fines de facturación también proceden realmente de las estaciones de carga 2 en las que ha recibido energía.

Para ello, el usuario puede descargar, dado el caso, del ordenador 23 la clave de aparato de medición pública (PuM) de la estación de carga 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 factura. Los datos de factura relacionados con este ID de estación de carga (paquetes de datos) están provistos en cada caso de una firma en la factura. El usuario puede verificar esta firma junto con las informaciones de tiempo que ha apuntado y la clave de aparato de medición pública cargada (PuM) de la estación de carga. Para ello, el usuario puede usar un programa cargado a través del ordenador 23.

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

Esto garantiza una alta integridad de datos en la facturación. También es posible una verificación de plausibilidad. Finalmente se asegura que el paquete de datos 34 se ha recibido tanto sin falsificar en el vehículo 6 como sin falsificar en la central de facturación 22.

La figura 2c muestra la firma con una clave de vehículo privada (Pi2) que permite rastrear un proceso de carga con respecto a un determinado vehículo. Sin embargo, puede ser deseable que precisamente este rastreado no sea posible.

Para evitar esto es posible que en el momento de una conclusión de contrato se creen una clave de contrato pública (Pu3) y una clave de contrato privada (Pi3). Al menos la clave de contrato pública (Pu3) se puede almacenar en una central de facturación 22.

Además, se puede formar por un vehículo 6 para un proceso de carga una tupla compuesta por claves temporales privadas (Pi4) y claves temporales públicas (Pu4). Esta tupla se puede crear por cada proceso de carga o en intervalos regulares o en intervalos irregulares.

Ante una firma del conjunto de datos 40 en el vehículo 6 se puede consultar la clave de contrato privada (Pi3) por el vehículo 6. Esto se puede realizar, por ejemplo, mediante una entrada por parte del usuario. Asimismo, la clave de contrato privada (Pi3) se puede leer eléctricamente por una clave de vehículo (no mostrada). Esto se puede realizar, por ejemplo, mediante un transpondedor.

Con ayuda de la clave de contrato privada (Pi3) se puede firmar una clave temporal pública de vehículo (pu4) que se ha creado previamente en el vehículo 6. Se produce la tercera firma (SK). Con ayuda de la clave temporal privada de vehículo (Pi4) previamente creada en el vehículo 6 se puede generar una cuarta firma (SF2) del conjunto de datos 40 a partir del paquete de datos 34 y de la primera firma (SD) 36, tal como se describió anteriormente para la segunda firma (SF1) 50 en las etapas de cálculo 42 y/o 48.

El paquete de datos cualificados 50 que está formado a partir del paquete de datos 34, la primera firma (SD) 36, la cuarta firma (SF2) y la tercera firma (SK) se puede transmitir por el vehículo 6 a través de la estación de carga 2 a la central de facturación 22.

En la central de facturación 22 se puede calcular de manera inversa la clave temporal privada (Pi4) mediante la clave de contrato pública (Pu3) conocida allí a partir de la tercera firma (SK). Con la clave temporal privada (Pu4) así determinada se puede verificar la cuarta firma (SF2) de manera correspondiente a la descripción anterior de la verificación de la segunda firma (SF1).

A este respecto se puede calcular en la central de facturación una firma de comparación (SF2') con ayuda de los datos recibidos y de la clave temporal privada (Pi4). Esta firma de comparación (SF2') se puede comparar con la cuarta firma (SF2) recibida. Si ambas firmas coinciden, entonces se puede concluir que los datos se hayan recibido sin falsificar. Con ayuda de las claves temporales y las claves de contrato es posible una asignación entre el conjunto de datos y el contrato, aunque ya no es posible un rastreado para determinar un determinado vehículo, ya que se modifican las claves temporales en el vehículo y, por tanto, no se puede asignar una clave temporal unívoca a un vehículo.

La figura 3 muestra un diagrama de desarrollo de un procedimiento para verificar los datos de medición por parte del usuario.

En una primera etapa 60, un usuario se desplaza con su vehículo 6 hasta una estación de carga 2. En el momento en el que se ha enchufado el cable de carga 4 en el vehículo 6 y empieza el proceso de carga se detecta 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 hora así como la fecha. Además, la unidad de cálculo detecta el nivel de contador actual del aparato de medición 10. Además, la unidad de cálculo detecta 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 se detecten el valor de medición, la hora y la fecha así como el estado y la firma en el aparato de medición 10. También es posible que partes del mismo se detecten en la unidad de cálculo 16 y que el paquete de datos se firme en la unidad de cálculo 16.

De manera paralela a este respecto, el usuario también puede apuntar la hora y la fecha del inicio del proceso de carga. Para ello, por ejemplo, usa 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 segunda etapa 62, la unidad de firma 16b calcula la firma 36 a partir del paquete de datos 34 que contiene las informaciones anteriormente mencionadas y la clave de aparato de medición 18a.

El paquete de datos 34 y la firma 36 se transmiten en una siguiente etapa 64 a la central de facturación 22.

En una siguiente etapa 66, el usuario finaliza el proceso de carga. En este momento, la unidad de cálculo 16 detecta de nuevo la hora actual o un índice de hora así como la fecha. Además, la unidad de cálculo detecta de nuevo el nivel de contador actual del aparato de medición 10. Además, la unidad de cálculo detecta de nuevo además 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, por ejemplo, usa 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 contiene las informaciones anteriormente mencionadas, y a partir de la clave de aparato de medición 18a.

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

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

Para un cliente o un ID de contrato se recopilan todos los procesos de carga durante un periodo de facturación.

En el momento de la facturación 74, el usuario recibe una factura. Esta factura indica para cada tarifa la cantidad de energía total recibida y el precio.

Además, la factura indica para cada proceso de carga la hora de inicio y 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, la factura indica para cada hora de inicio y cada hora de final el número de contador, el nivel de contador y 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 están también disponibles para el cliente de modo que los puede consultar en línea.

También están disponibles para el cliente claves de aparato de medición públicas de modo que las puede consultar.

En una etapa 74, el cliente puede verificar con las informaciones de tiempo e identificaciones de aparato de medición que ha apuntado las firmas que se le han comunicado. Para ello puede utilizar las informaciones apuntadas junto con las informaciones comunicadas con respecto al nivel de contador y el estado para verificar la firma con la clave de aparato de medición pública. Para ello puede usar un programa que también se proporciona 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 un vehículo y/o una central de facturación. 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, posibilita verificar 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 decisivo para el tráfico de datos tanto entre la estación de carga 2 y el vehículo 6 como entre la estación de carga 2 y la central de facturación 22. La firma y un posible cifrado no deben provocar un aumento excesivo del tamaño de los paquetes de datos, ya que, en caso contrario, el volumen de datos sería demasiado grande. Para el uso masivo son especialmente adecuados por tanto procedimientos de clave pública.

REIVINDICACIONES

1. Procedimiento para asegurar una facturación de una cantidad de energía recibida de una estación de carga, con las etapas de:

al inicio de un proceso de carga:

- recibir en una estación de facturación central (22) un primer paquete de datos (34) que comprende al menos un primer nivel de contador de aparato de medición, una primera hora y una identificación 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 (3) y
- recibir en una estación de facturación central (22) una firma (36) creada con ayuda de una clave de aparato de medición privada asignada al aparato de medición (10) del primer paquete de datos (34),

al final de un proceso de carga:

- recibir en la estación de facturación central (22) un segundo paquete de datos (34) que comprende al menos un segundo nivel de contador de aparato de medición, una segunda hora y la identificación de aparato de medición del aparato de medición (10) que mide la cantidad de energía recibida por el vehículo (6) de la estación de carga (3) y
- recibir en la estación de facturación central (22) una firma (36) creada con ayuda de la clave de aparato de medición privada asignada al aparato de medición (10) del segundo paquete de datos (34) y
- proporcionar datos de facturación con respecto a la cantidad de energía recibida de la estación de facturación (22) que comprende al menos el primer y el segundo nivel de contador de aparato de medición, la respectiva hora, la identificación de aparato de medición y las respectivas firmas primera y segunda así como una clave de aparato de medición pública asignada al aparato de medición (10).

2. Procedimiento según la reivindicación 1, **caracterizado por que** el paquete de datos (34) contiene al menos una de las informaciones que consisten en

A) un estado de aparato de medición,
B) una identificación de cliente y/o de contrato,
C) informaciones acerca de una cantidad de energía recibida,
D) una clave de aparato de medición pública (34e);
E) un índice de tiempo.

3. Procedimiento según una de las reivindicaciones 1 a 2, **caracterizado por que** la firma se crea con ayuda de al menos un valor de referencia del conjunto de datos a firmar.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado por que** se cifra el paquete de datos (34).

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado por que** el paquete de datos (34) y la respectiva firma (36) se crean en un momento de un cambio de tarifa, creándose en un momento de un cambio de tarifa un tercer paquete de datos (34) y la respectiva firma (36) para un final de una primera tarifa y por que se crea un cuarto paquete de datos (34) y la respectiva firma (36) para un inicio de una segunda tarifa o sólo un paquete de datos (34) y una firma (36) para el momento del cambio de tarifa.

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado por que** la estación de carga (2) determina, 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, una cantidad de energía recibida y/o la estación de facturación (22) determina una cantidad de energía recibida a partir del nivel de contador de aparato de medición en caso de un cambio de tarifa.

7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado por que** en los datos de facturación se emite, además de la cantidad de energía recibida, al menos un valor que consiste en:

A) una identificación de cliente y/o de contrato,
B) informaciones de fecha,
C) un estado de aparato de medición y/o
D) una clave de aparato de medición pública (PuM) en texto plano.

8. Procedimiento según las reivindicaciones 1 a 7, **caracterizado por que** los datos de facturación están disponibles de modo que se pueden consultar en la estación de facturación central (22).

9. Procedimiento según la reivindicación 8, **caracterizado por que** los datos de facturación están disponibles protegidos frente a un acceso.

10. Procedimiento según una de las reivindicaciones 1 a 9, **caracterizado por que** las claves de aparato de medición públicas de aparatos de medición de las estaciones de carga están disponibles en un ordenador (23) separado de manera lógica y/o espacial de la estación de facturación (22).

11. Procedimiento según una de las reivindicaciones 1 a 10, **caracterizado por que** los datos de facturación y/o la clave de aparato de medición se pueden consultar a través de una red de área amplia (20), en particular Internet.

12. Procedimiento según una de las reivindicaciones 1 a 11, **caracterizado por que** se proporciona un programa que se puede consultar a través de una red de área amplia (20) para calcular la firma para el nivel de contador de aparato de medición respectivamente asignado, a partir de al menos uno de los valores:

A) identificación de cliente y/o de contrato,
B) informaciones de hora,
C) informaciones de fecha,
E) identificación de aparato de medición,
F) estado de aparato de medición y/o
G) clave de aparato de medición pública (PuM).

13. Dispositivo para asegurar una facturación de una cantidad de energía recibida de una estación de carga con

- un aparato de medición (10) que está configurado para detectar 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 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 para crear una firma (36) del paquete de datos con ayuda de una parte de una clave de aparato de medición asignada al aparato de medición (10),
- medios de envío que están configurados
- para transmitir un primer paquete de datos (34) que comprende al menos un primer nivel de contador de aparato de medición, una primera hora y una identificación 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 (3) y
- una firma (36) del primer paquete de datos (34) creada con ayuda de una clave de aparato de medición privada asignada al aparato de medición (10) al inicio de un proceso de carga y
- para transmitir un segundo paquete de datos (34) que comprende al menos un segundo nivel de contador de aparato de medición, una segunda hora y la identificación de aparato de medición del aparato de medición (10) que mide la cantidad de energía recibida por el vehículo (6) de la estación de carga (3) y
- una firma (36) del segundo paquete de datos (34) creada al final de un proceso de carga con ayuda de la clave de aparato de medición privada asignada al aparato de medición (10).

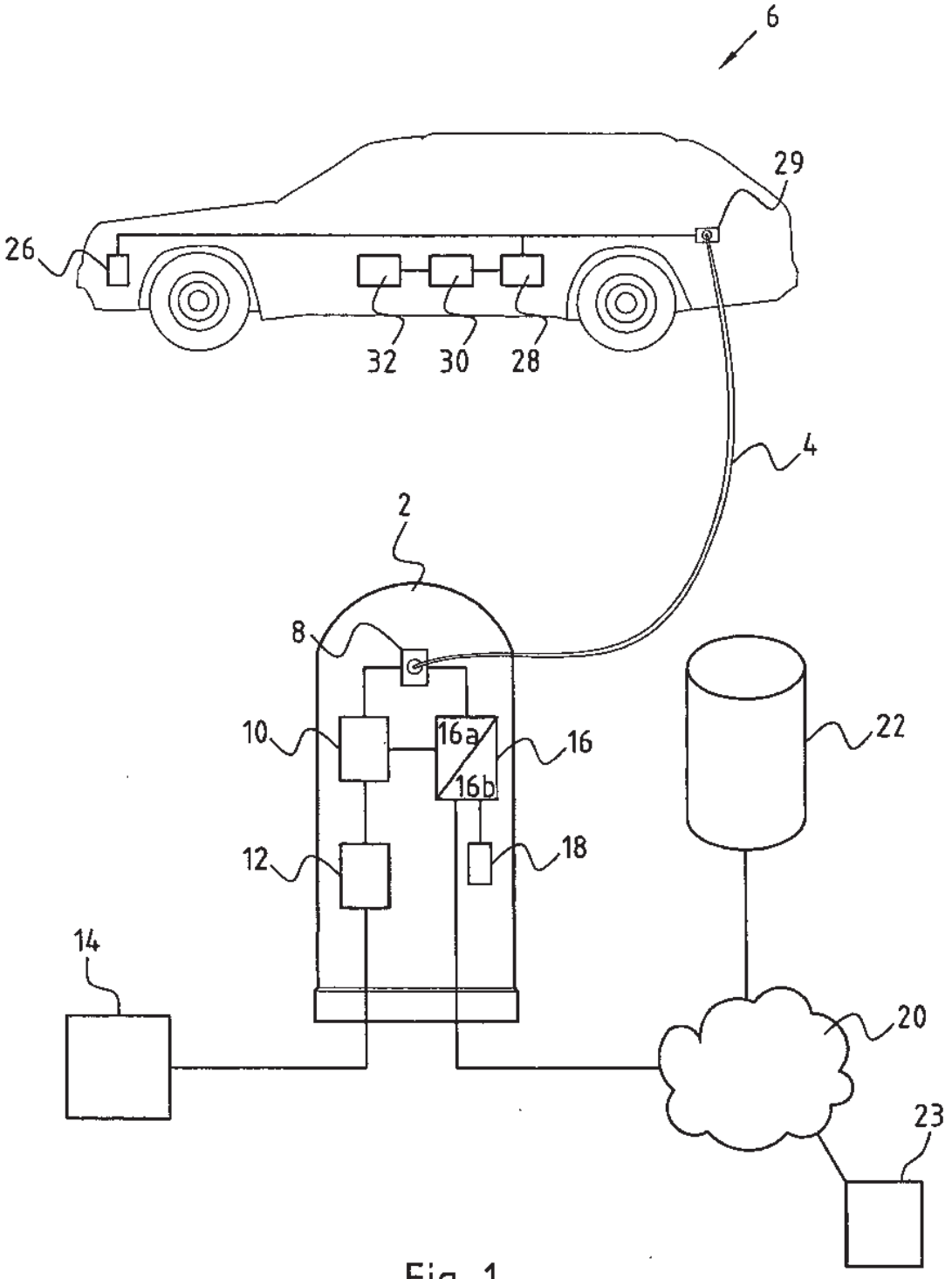

Fig. 1

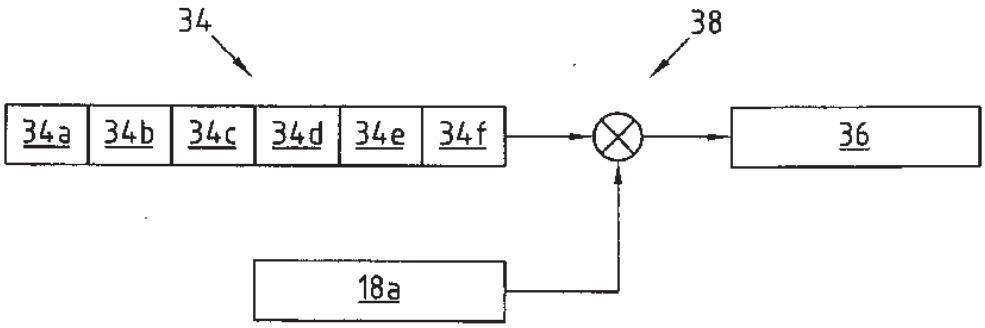

Fig. 2a

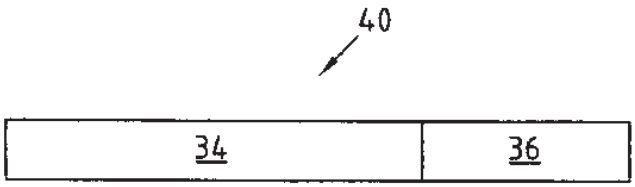

Fig. 2b

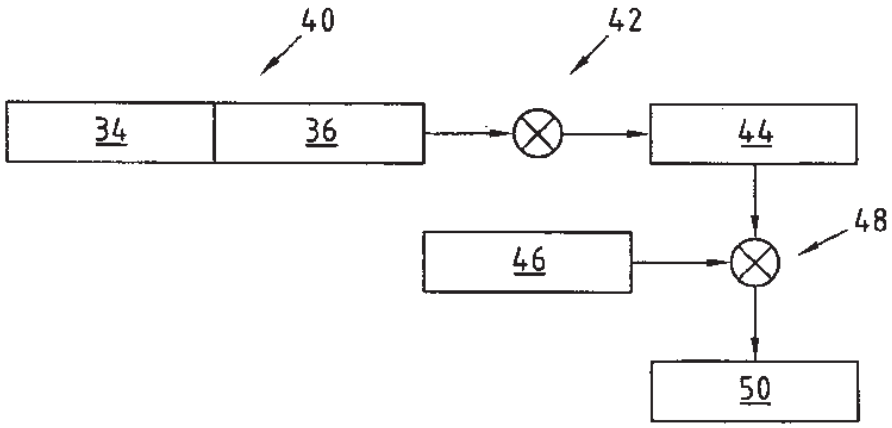

Fig. 2c

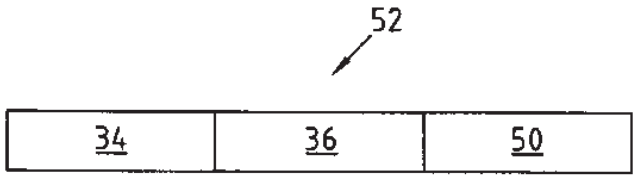

Fig. 2d

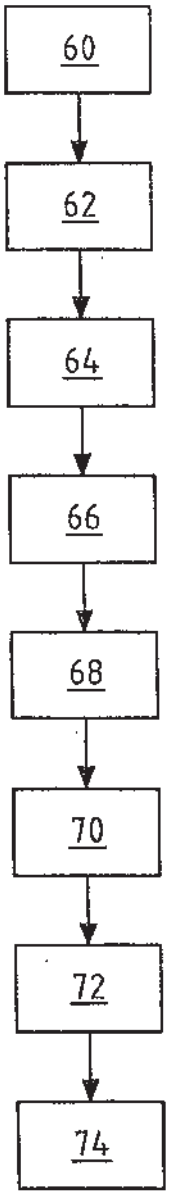

Fig.3