(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 757 964**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.11.2013 PCT/EP2013/074873**

(87) Fecha y número de publicación internacional: **12.06.2014 WO14086640**

(96) Fecha de presentación y número de la solicitud europea: **27.11.2013 E 13802297 (5)**

(97) Fecha y número de publicación de la concesión europea: **30.10.2019 EP 2929665**

(54) Título: **Procedimiento, configuración para procesar informaciones en un aparato doméstico así como aparato doméstico**

(30) Prioridad:

04.12.2012 DE 102012222248

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.04.2020

(73) Titular/es:

BSH HAUSGERÄTE GMBH (100.0%)
CARL-WERY-STRASSE 34
81739 MÜNCHEN, DE

(72) Inventor/es:

GAUGLER, JOHANNES;
KOLBE, ANDREAS;
LEITL-NOBEL, MARTIN;
RANCK, SHARON y
SIPPEL, MATTHIAS

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Procedimiento, configuración para procesar informaciones en un aparato doméstico así como aparato doméstico

La invención se refiere a un procedimiento y a una configuración para procesar informaciones en un aparato doméstico, así como a un aparato doméstico que puede ser adecuado para ejecutar el procedimiento y/o que puede ser parte integrante de la configuración.

La creciente integración en red de aparatos domésticos mediante una red de comunicación establecida dentro de un hogar (también denominada entorno de red domestica o bien “Smart Home”), que además está conectada con una red de comunicación global de orden superior (también denominada Internet) abre nuevas posibilidades y servicios para el mantenimiento de aparatos domésticos asociados a un hogar. Por ejemplo pueden ofrecer los fabricantes de aparatos domésticos “servicios a distancia al cliente” o “servicios de mantenimiento a distancia”, que pueden controlarse a distancia, que permiten tanto al cliente como también al respectivo operador del servicio al cliente un ahorro en tiempo y en costes. A modo de ejemplo citemos en cuanto a tales funciones de mantenimiento (también denominadas transacción de servicio al cliente) la instalación en cuanto a software de nuevas características de proceso y/o programa, la ejecución de actualizaciones (update) de firmware, diagnósticos de faltas y protocolos de prueba de servicio al cliente, así como adaptaciones específicas de ajustes del aparato mediante un servicio remoto al cliente (service). El documento US 2009/0156193 A1 por ejemplo describe un enfoque en el que se conecta acústicamente un terminal mediante una red de voz a un ofertante de servicios.

Un inconveniente que implica un tal servicio remoto al cliente son peligros que comprometen la seguridad tanto de las redes establecidas por parte del cliente como también de los aparatos domésticos instalados conectados a las redes o redes domésticas, como consecuencia de lo cual podría verse afectada la aceptación general por parte de los clientes.

Un peligro consiste en el abuso de la utilización de posibilidades privilegiadas de acceso y funciones para tareas del servicio al cliente en un aparato doméstico, por ejemplo mediante criminalidad de Internet. Otro aspecto de peligro es la ejecución de funciones que pueden modificar el estado o el funcionamiento del aparato doméstico, así como la captación de informaciones en el aparato doméstico mediante un servicio remoto al cliente sin el control directo y vigilante por parte del propio cliente (es decir, el temor a ceder la prioridad del dominio sobre el aparato doméstico de forma incontrolada y sin acompañamiento).

Se prevé el comienzo de una amplia introducción en el mercado de masas de todo el campo de la conexión de aparatos domésticos, la integración en entornos de una red doméstica, así como su conexión a Internet. Esto se refiere en particular al ámbito especial de la aportación y utilización de prestaciones de servicio remoto al cliente o el llamado remote service para el cliente. Actualmente no se conoce aún ninguna solución en el ámbito de los aparatos domésticos que esté orientada al tema de los citados peligros.

El objetivo de la invención consiste en evitar los inconvenientes antes citados y en particular en indicar un procedimiento de mantenimiento, en particular un procedimiento de mantenimiento remoto, que logre una amplia aceptación por parte de los clientes que tienen aparatos domésticos.

Este objetivo se logra mediante las características de las reivindicaciones independientes. Perfeccionamientos de la invención resultan de las reivindicaciones dependientes.

Para lograr el objetivo se transmiten desde al menos un aparato doméstico un mensaje a una unidad central, así como desde la unidad central primeras informaciones a través de una primera vía de comunicación al aparato doméstico. Desde la unidad central se transmiten segundas informaciones a un aparato terminal de comunicación y desde el aparato terminal de comunicación las segundas informaciones a través de una segunda vía de comunicación al aparato doméstico. El aparato doméstico comprueba las primeras informaciones con ayuda de las segundas informaciones.

El procedimiento propuesto posibilita en particular un servicio al cliente remoto o a distancia, asegurado y autorizado, mediante una comunicación de dos vías, basándose en la utilización de una primera vía de comunicación entre el aparato doméstico y la unidad central (como por ejemplo el servicio al cliente a distancia o servicio remoto al cliente) y una segunda vía de comunicación mediante un aparato terminal de comunicación. A un cliente de un aparato doméstico se le proporciona así una vía de comunicación o bien enlace de comunicación (que opcionalmente puede estar realizada/o asegurada/o por sí misma/o) entre el aparato doméstico a mantener y el servicio a distancia al cliente (servicio remoto al cliente o bien centro remoto de servicio al cliente) del fabricante del aparato doméstico, a través de los cuales pueden también por ejemplo ejecutarse funciones privilegiadas y sensibles, en particular funciones de mantenimiento, como por ejemplo funciones de telecontrol y mantenimiento a distancia.

Tales funciones pueden incluir entonces toda clase de funciones específicas del servicio al cliente, inclusive toda clase de actualización, ejecución y liberación de tales funciones, así como acciones, órdenes o secuencias de órdenes. En particular pueden transmitirse al aparato doméstico a través de la primera vía de comunicación datos (actualizaciones,

ampliaciones del volumen funcional, etc.). La activación o bien “conversión en útiles” de los datos se realiza con preferencia sólo mediante la segunda vía de comunicación, que proporciona las segundas informaciones.

.

Al respecto existe la ventaja de que por ejemplo se transmiten datos de actualización (por ejemplo un update) para el aparato doméstico a través de la primera vía de comunicación desde la unidad central al aparato doméstico, lo cual, en función del volumen de datos, puede durar un tiempo considerable. La actualización propiamente dicha sólo se realiza tras recibir las segundas informaciones a través de la segunda vía de comunicación.

Ventajosamente, en cada transacción individual de servicio remoto al cliente en el aparato doméstico - es decir, transmisión de informaciones de mantenimiento y dado el caso ejecución de otras acciones o funciones establecidas en base a ello por parte del aparato doméstico - sigue manteniendo el cliente el control directo y el control en el tiempo de la ejecución propiamente dicha de las funciones de mantenimiento. Al mantener así el usuario o cliente el control y evitarse a la vez posibles puntos de ataque mediante criminalidad de Internet, se logra una mayor aceptación general por parte de los clientes.

Las primeras informaciones transmitidas en el marco del procedimiento propuesto al aparato doméstico constituyen por ejemplo la base de información para la ejecución de funciones de mantenimiento en el aparato doméstico. Como mejora, tras realizarse la ejecución de las funciones de mantenimiento pueden transmitirse informaciones sobre resultados específicos del mantenimiento o adicionalmente otras informaciones a transmitir a la unidad central o bien al centro de servicio al cliente.

No hay limitaciones en cuanto a la clase de aparato doméstico considerada, en particular aparato doméstico eléctrico y pueden quedar incluidos grandes aparatos domésticos y/o pequeños aparatos domésticos. El aparato doméstico podría incluir en particular al menos un aparato para cocinar, por ejemplo un horno para cocinar, un microondas, un aparato para cocer al vapor, etc. El aparato doméstico podría también incluir al menos un aparato refrigerador, por ejemplo un armario frigorífico o un arcón frigorífico. El aparato doméstico podría también incluir al menos un aparato para el tratamiento de la colada, por ejemplo una máquina lavadora o una secadora de ropa. El aparato doméstico podría incluir además un aparato para enjuagar, por ejemplo un lavavajillas. El aparato doméstico podría en particular incluir al menos una máquina de café y/o tostadora.

Un perfeccionamiento consiste en que la comprobación incluya una autentificación de las primeras informaciones.

Por ejemplo pueden utilizar el aparato doméstico y la unidad central un procedimiento de encriptado asimétrico (criptografía de clave pública o public key), para firmar alternadamente los datos transmitidos, autentificar la firma y/o encriptar y desencriptar los datos. El otorgamiento de claves y/o la gestión de las claves puede realizarlas por ejemplo el fabricante de los aparatos domésticos.

Otro perfeccionamiento consiste en que tras realizarse la comprobación con éxito, se ejecute al menos una acción predeterminada.

En particular consiste un perfeccionamiento en que la acción predeterminada incluya

- una actualización de un software del aparato doméstico,
- una ampliación de una funcionalidad del aparato doméstico,
- una realización de una acción de mantenimiento o aplicación de mantenimiento,
- una transmisión de una información de mantenimiento a un destinatario,
- una realización de una prueba,
- una ejecución de informaciones relativas a órdenes para el control del diagnóstico,
- una ejecución de las primeras informaciones o bien
- una utilización de las primeras informaciones.

También consiste un perfeccionamiento en que las segundas informaciones se transmitan a través de un enlace de telefonía móvil al aparato terminal de comunicaciones. El enlace de telefonía móvil incluye por ejemplo cualquier enlace de comunicación móvil, por ejemplo un enlace a través de una red móvil de telecomunicaciones

Además, un perfeccionamiento consiste en que las segundas informaciones se transmitan mediante

- un MMS, o
- un SMS, o
- un e-mail.

En el marco de un perfeccionamiento adicional, está configurada la segunda vía de comunicación como

- enlace de comunicación de zona próxima
- enlace Bluetooth o bien
- enlace de infrarrojos.

Mediante la variante de configuración de la segunda vía de comunicación como solamente un enlace punto a punto que dispone de un alcance limitado, ha de entenderse el establecimiento o bien organización de una vía de comunicación configurada de esta manera entre el aparato doméstico y el aparato terminal de comunicación como conformidad del cliente (tanto del aparato doméstico como también del aparato terminal de comunicación) para ejecutar una acción inminente prescrita, por ejemplo una transacción específica de servicio al cliente. Esto otorga al usuario del aparato doméstico el control sobre la ejecución de un servicio remoto al cliente o remote customer service en su aparato doméstico.

Un siguiente perfeccionamiento consiste en que las segundas informaciones incluyan al menos parcialmente informaciones sobre claves.

Las informaciones de encriptado son claves o informaciones que pueden utilizarse como claves. Básicamente pueden utilizarse mecanismos de encriptado asimétricos o simétricos en relación con la solución aquí descrita. Con ayuda de las informaciones de encriptado pueden encriptarse y/o firmarse informaciones a transmitir al aparato doméstico, por ejemplo informaciones de mantenimiento. Alternativamente puede suprimirse el encriptado o firma. Así pueden por ejemplo insertarse las informaciones de encriptado o bien una clave de prueba formada por las mismas en las informaciones de mantenimiento a transmitir al aparato doméstico, o bien anexarse a las mismas.

Según otra variante de configuración, pueden transmitirse las informaciones de encriptado separadamente a través del primer enlace de comunicación, por ejemplo una vez realizada la transmisión de las informaciones de mantenimiento, al aparato doméstico y asociarse en el mismo a las informaciones de mantenimiento ya recibidas para una comprobación siguiente. La transmisión separada de las informaciones de encriptado puede realizarse también ya antes de la transmisión de las informaciones de mantenimiento o junto con las mismas.

Por ejemplo pueden presentar las informaciones sobre claves sólo una validez limitada en el tiempo, con lo que en el aparato doméstico la comprobación ha de realizarse dentro de un periodo de tiempo predeterminado. La duración de la validez en el tiempo (por ejemplo a partir de la transmisión del mensaje que representa una solicitud de mantenimiento) puede archivarse en el aparato doméstico o transmitirse al aparato doméstico mediante otra información adicional.

Una variante de configuración consiste en que el mensaje sea firmado por el aparato doméstico antes de la transmisión con ayuda de un procedimiento de encriptado asimétrico.

Otra forma de ejecución más consiste en que las segundas informaciones transmitidas a través del aparato terminal de comunicaciones se firmen antes de la transmisión mediante la unidad central con ayuda de un procedimiento de encriptado asimétrico.

La aplicación opcional de un procedimiento de encriptado asimétrico al transmitir el mensaje, así como también de las segundas informaciones, significa una seguridad adicional para la ejecución de transacciones de servicio remoto al cliente.

Una siguiente variante de configuración consiste en que las segundas informaciones firmadas transmitidas a través de la segunda vía de comunicación sean autentificadas por el aparato doméstico.

También consiste una variante de configuración en que las segundas informaciones firmadas transmitidas sean autentificadas por el aparato terminal de comunicación.

Esto significa una medida adicional de seguridad, ya que la autentificación de las segundas informaciones firmadas puede realizarse bien en el aparato doméstico o en el aparato terminal de comunicación o en ambos aparatos citados.

Un perfeccionamiento consiste en que el establecimiento o bien la formación de la segunda vía de comunicación esté asegurado/a mediante la introducción de un código personal de identificación (PIN).

La introducción local de informaciones de código, como por ejemplo un número de PIN, en el aparato terminal de comunicación, significa una medida adicional ventajosa para asegurar el procedimiento propuesto. La comprobación de las informaciones de código introducidas puede realizarse entonces localmente mediante el aparato terminal de comunicación o mediante un equipo central fuera del aparato terminal de comunicación, como por ejemplo el aparato doméstico que representa el aparato contrapuesto de la segunda vía de comunicación. Alternativamente puede realizar la comprobación de las informaciones de código el aparato contrapuesto del enlace de telefonía móvil, es decir, la unidad central, como por ejemplo el servicio remoto al cliente.

Una variante de configuración adicional consiste en que la primera vía de comunicación esté configurada como enlace de datos asegurado criptográficamente a través de Internet.

El enlace de Internet asegurado criptográficamente provoca una mejora adicional de la seguridad del procedimiento propuesto.

El objetivo antes mencionado se logra también mediante una configuración para procesar informaciones en un aparato doméstico, con medios de transmisión asociados al aparato doméstico para transmitir un mensaje a una unidad central y al menos un equipo asociado a la unidad central para transmitir primeras informaciones a través de una primera vía de comunicación al aparato doméstico, así como para transmitir segundas informaciones a un aparato terminal de comunicación. Al respecto están asociados al aparato terminal de comunicación medios emisores para transmitir las segundas informaciones a través de una segunda vía de comunicación al aparato doméstico. Al aparato doméstico están asociados medios de comprobación para comprobar las primeras informaciones con ayuda de las segundas informaciones.

El objetivo antes citado se logra también mediante un aparato doméstico que es parte integrante de la configuración antes descrita.

Las etapas del procedimiento aquí descrito pueden aplicarse a la configuración, así como al aparato doméstico correspondientemente.

A continuación se presentarán y describirán ejemplos de ejecución de la invención en base a un dibujo.

Se muestra en:

figura 1 en forma de una representación esquemática, un escenario de aplicación del procedimiento propuesto.

La figura 1 muestra una red de comunicación local o red doméstica 110 establecida en un aparato doméstico 100, a la cual están conectados varios aparatos domésticos 101 a 103 asociados al hogar 100, mediante respectivas interfaces de red o bien una interfaz de red 105. Con preferencia es la respectiva interfaz de red 105 parte integrante del correspondiente aparato doméstico 101 a 103. Según el escenario de aplicación representado, está configurado un primer aparato doméstico 101 como armario frigorífico, un segundo aparato doméstico 102 como horno para cocinar y un tercer aparato doméstico 103 como máquina lavadora. El enlace de comunicación de los respectivos aparatos domésticos con la red local de comunicación 110 puede basarse por ejemplo en tecnología de transmisión WLAN (Wireless Local Area Network, red inalámbrica de área local), LAN o Powerline.

La red doméstica 110 del hogar 100 puede conectarse o está conectada (mediante un enlace 130 representado simbólicamente) mediante una conexión doméstica no representada con una red de comunicación global 200 de orden superior. La red de comunicación 200 puede ser Internet o incluirla. A la red de comunicación global 200 está conectada mediante un enlace 320 una red de comunicación local 310 de un centro de servicio al cliente 300, que está configurada como centro remoto de servicio al cliente para proporcionar servicios de mantenimiento a distancia. El centro de servicio al cliente 300 incluye un equipo de mantenimiento 301 (por ejemplo en forma de al menos un servidor) para recibir solicitudes de servicio al cliente y para generar las correspondientes informaciones de mantenimiento, así como un equipo de encriptado 302 para generar informaciones de clave para el encriptado y firma de informaciones específicas del mantenimiento. Adicionalmente está equipado el equipo de encriptado 302 para autentificar y/o verificar solicitudes de servicio al cliente que llegan al centro de servicio al cliente 300 o bien otras informaciones específicas del mantenimiento.

La red de comunicación local 310 del centro de servicio al cliente 300 puede conectarse además mediante un enlace 420 representado simbólicamente con una red de comunicación móvil 400 operada por un ofertante de telefonía móvil, que por ejemplo está configurada según al menos un estándar de telefonía móvil como GSM, UMTS, LTE. La red de comunicación móvil 400 está equipada, entre otros, para transmitir mensajes de texto y/o mensajes breves, como SMS o MMS/QDR.

Para las siguientes explicaciones supongamos que la máquina lavadora 103 dispuesta en el hogar 100 está equipada y configurada correspondientemente para un posible “mantenimiento a distancia o remoto” por parte del centro de servicio al cliente 300 del fabricante de la máquina lavadora, en el sentido del procedimiento correspondiente a la invención. Para ello lleva asociada la máquina lavadora 103 un equipo de encriptado 120, que posibilita un encriptado asimétrico y/o simétrico. Señalemos que también los otros aparatos domésticos dispuestos en la red doméstica 110, como el armario frigorífico 101 y el horno para cocinar 102, pueden estar equipados y configurados correspondientemente, igualmente para un mantenimiento remoto. La secuencia de la solución descrita se explicará no obstante en el escenario de aplicación representado en la figura 1 a modo de ejemplo en base a la máquina lavadora 103. Los aparatos domésticos 101 a 103 dispuestos en el hogar 100 pueden proceder de diversos fabricantes y correspondientemente puede realizarse opcionalmente el mantenimiento remoto para cada aparato doméstico también en función de cada fabricante desde distintos centros de servicio al cliente.

Cuando se utiliza un procedimiento de encriptado simétrico, se realiza el encriptado y desencriptado de informaciones con la misma clave (secreta). Por el contrario se basa un procedimiento de encriptado asimétrico en un par de claves, que está compuesto por una parte secreta (“secreto”, clave privada o private key) y una parte no secreta (clave pública o public key). La clave pública permite a cualquier tercero encriptar datos para el poseedor de la clave privada, cuya

firma digital ha de comprobarse o bien ha de autentificarse el poseedor. La clave privada permite a su poseedor desencriptar datos encriptados con la correspondiente clave pública, generar firmas digitales o autentificarse.

En base a una configuración realizada ya desde el proceso de fabricación de la máquina lavadora 103, está memorizada por ejemplo en el equipo de encriptado 120 por un lado una clave privada 140, que en el marco de un procedimiento de encriptado asimétrico está asociada a la máquina lavadora 103. La clave pública 141 correspondiente al respecto está memorizada en el equipo de encriptado 302 del centro de servicio al cliente 300. Además está memorizada en el equipo de encriptado 120 una clave pública 351, que en el marco de otro procedimiento de encriptado asimétrico quedó asociada al centro de servicio al cliente 300 del fabricante de la máquina lavadora 103. Una clave privada 350 que corresponde a la misma del centro de servicio al cliente 300 está memorizada en el equipo de encriptado 302.

Además, en el sentido de la invención está memorizada una información de dirección 145 inequívoca de un aparato terminal de comunicación móvil 150 (smartphone) asociado al hogar 100 o bien al usuario de la máquina lavadora 103 en el equipo de encriptado 302 del centro de servicio al cliente 300. El aparato terminal de comunicación móvil 150 representado en la figura 1 está constituido por ejemplo como smartphone, que en base a su número de telefonía móvil 145 puede identificarse como información de dirección inequívoca en la red de comunicación móvil 400. Alternativamente puede estar constituido el smartphone por ejemplo como un Tablet-PC con cualesquiera otras informaciones de dirección 145 asociadas inequívocamente.

El número de telefonía móvil 145 del smartphone 150 asociado al hogar 100 puede transmitirse por ejemplo en el marco de la realización de un registro de la máquina lavadora 103 al centro de servicio al cliente 300, con lo que se registra o archiva un acceso de telefonía móvil específico del correspondiente hogar 100 en el centro de servicio al cliente 300 del fabricante del correspondiente aparato doméstico (como aquí la máquina lavadora 103).

La interfaz de red 105 dispuesta en la máquina lavadora 103 está equipada además con una pila (stack) de protocolos configurada según TCP/IP, que puede basarse en cualquier tecnología de transmisión de la red allí dispuesta, como por ejemplo WiFi (Wireless LAN), ZigBee (Wireless Mesh Network, red inalámbrica mallada, basándose en la norma IEEE 802.15.4), Ethernet (IEEE 802.3), PLC Powerline Communication, comunicación por líneas de suministro eléctrico), LTE (Long Term Evolution, evolución a largo plazo), GSM (Global System for Mobile Communications, sistema global para comunicaciones móviles). La interfaz de red 105 de la máquina lavadora 103 está entonces equipada tal que se utiliza un enlace de comunicación asegurado criptográficamente, por ejemplo mediante SSL/TLS (Secure Socket Layer, capa de puertos seguros/TLS, Transport Layer Security, seguridad de la capa de transporte) para relaciones de comunicación o enlaces de comunicación a establecer a través de la red de comunicación global 200. Igualmente está memorizada mediante configuración previa una dirección de red conforme con la pila de protocolos o bien un nombre de host (ordenador anfitrión) del servidor de servicio al cliente 301 del fabricante de la máquina lavadora 103 en la interfaz de red 105.

Tal como ya se ha señalado pueden proceder los aparatos domésticos 101 a 103 representados en la figura 1 y conectados a la red doméstica 110 de distintos fabricantes. Correspondientemente presentan los aparatos domésticos 101 a 103 diversas claves públicas individuales de los respectivos fabricantes de los aparatos domésticos, así como diversas direcciones de red individuales o bien nombres de host de los correspondientes servidores de servicio al cliente de los distintos fabricantes.

Alternativamente pueden estar memorizadas las informaciones almacenadas en el equipo de encriptado 120 o en la correspondiente interfaz de red 105 directamente en la máquina lavadora 103 o bien en un equipo de control (no representado) de la máquina lavadora.

En el presente ejemplo de ejecución está configurada la máquina lavadora 103 tal que en un caso que se presente de mantenimiento y/o de servicio al cliente se establece mediante la máquina lavadora 103 autónomamente a través de la red doméstica local 110, así como de la conexión doméstica del aparato doméstico 100, un enlace bidireccional asegurado a través de Internet 200 con el centro de servicio al cliente 300 o bien con el correspondiente servidor de servicio al cliente 301 del fabricante de la máquina lavadora; ello se representa mediante un enlace con trazo discontinuo 500. Tras establecerse en enlace de Internet 500, genera la máquina lavadora 103 un mensaje o solicitud de servicio al cliente 510, inclusive una identificación del aparato que identifica la máquina lavadora 103, así como informaciones adjuntas sobre faltas, se firma con ayuda de la clave privada 140 asociada y a continuación se retransmite a través del enlace de Internet 500 al servidor de servicio al cliente 301.

Mediante el servidor de servicio al cliente 301 se verifica la solicitud de servicio al cliente 510 firmada recibida con ayuda de la clave pública 141 de la máquina lavadora 103 memorizada en el equipo de encriptado 302, es decir, se comprueba la identidad de la máquina lavadora 103 como punto de partida de la solicitud de servicio al cliente 510. La verificación de la solicitud de servicio al cliente 510 puede realizarse también mediante el equipo de encriptado 302. Un resultado positivo de la comprobación o bien una autorización con éxito se considera como autorización digital para utilizar el número de telefonía móvil 145 archivado en el centro de servicio al cliente en el marco del registro del teléfono smartphone 150 asociado al hogar 100 y dado el caso otras informaciones específicas del cliente. En función de la clase de solicitud de servicio al cliente 510, se generan mediante el servidor de servicio al cliente 301 o mediante

un colaborador del centro de servicio al cliente 300 informaciones de mantenimiento específicas de la solicitud y adecuadas para realizar funciones de mantenimiento, que incluyen por ejemplo funciones de servicio al cliente y/o mantenimiento necesarias para la máquina lavadora 103 para diagnósticos a distancia y/o una prueba a distancia (remote test) y/o una actualización a distancia del firmware. Además pueden incluir las informaciones de mantenimiento datos o ficheros completos necesarios adicionalmente, así como paquetes de software completos (bundles).

Antes de la transmisión de las informaciones de mantenimiento específicas de la solicitud se dotan las mismas por ejemplo de informaciones de claves 520 generadas exclusivamente para esta solicitud de mantenimiento o transacción de servicio al cliente mediante el equipo codificador 302 - a continuación denominadas también secreto, claves o claves de prueba – y/o se firman. La clave de prueba 520 está archivada con preferencia en el equipo codificador 302 del centro de servicio al cliente 300. Las informaciones de mantenimiento 530 específicas de la solicitud y dotadas de la clave de prueba 520, se transmiten a continuación a través del enlace de Internet 500 establecido (primera vía de comunicación) a la máquina lavadora 103 y ésta las memoriza correspondientemente como informaciones de mantenimiento 530 pertenecientes a la transacción del servicio al cliente. Antes de seguir procesando las informaciones de mantenimiento 530 memorizadas, se prueban y/o verifican las mismas por ejemplo mediante la máquina lavadora 103, es decir, mediante un equipo de control (no representado) dispuesto en la máquina lavadora 103.

Señalemos que la clave de prueba 520 puede asociarse de cualquier forma a las informaciones de mantenimiento 530 específicas de la solicitud, pudiendo realizarse la asociación en este caso por ejemplo mediante encriptado o firma de las informaciones de mantenimiento 530. Opcionalmente puede evitarse el encriptado o firma, pudiendo por ejemplo insertarse la clave de prueba 520 en las informaciones de mantenimiento 530 a transmitir o bien anexarse a las mismas. Alternativamente puede transmitirse la clave de prueba 520 separadamente a través del enlace de Internet 500, es decir, una vez realizada la transmisión de las informaciones de mantenimiento 530, a la máquina lavadora 103 y asociarse en ésta a las informaciones de mantenimiento 530 ya recibidas. Así puede transmitirse al aparato doméstico, por ejemplo para procesar una solicitud de servicio al cliente, primeramente un volumen de datos muy amplio, lo cual dado el caso implica un largo tiempo de transmisión (por ejemplo varias horas o también días). Sólo una vez realizada la transmisión de los datos, lo que se indica al centro de clientes por ejemplo mediante un correspondiente retroaviso, se genera la clave de prueba 520 y se transmite a través de la primera vía de comunicación a la máquina lavadora. Según otra alternativa más, puede realizarse la transmisión de la clave de prueba 520 también antes de la transmisión de las informaciones de mantenimiento 530. Opcionalmente puede encriptarse la transmisión de la clave de prueba 520 mediante la clave privada 350 del centro de servicio al cliente 300.

Con preferencia tiene la clave de prueba 520 sólo una limitada validez en el tiempo, con lo que las informaciones de mantenimiento 530 transmitidas a la máquina lavadora y/o la clave de prueba 520 transmitida a través de la primera vía de comunicación, debe/n comprobarse dentro de un periodo de tiempo predeterminado.

Tal como ya se ha descrito, se basa el procedimiento aquí propuesto en el concepto de una comunicación por dos vías. Para ello se transmite la clave de prueba 520 generada mediante el equipo de encriptado 302 adicionalmente mediante un mensaje específico de la telefonía móvil, por ejemplo un SMS como mensaje de texto 540, al smartphone 150 direccionado mediante el número de telefonía móvil 145 archivado.

El mensaje de texto 540 recibido por el smartphone 150 se retransmite a continuación a través de un enlace punto a punto 700 inalámbrico (segunda vía de comunicación), configurado como enlace NFC (Near-Field Communication, comunicación de campo cercano), a un equipo receptor NFC 125 asociado a la máquina lavadora 103.

Near Field Communication es una norma internacional de transmisión para el intercambio sin contacto de datos y/o informaciones a través de tramos cortos de hasta 4 cm. Al respecto señalemos que NFC sólo es un ejemplo de un enlace inalámbrico de poco alcance. Básicamente son posibles también otras posibilidades de transmisión, inalámbricamente o por hilo, desde el smartphone 150 al aparato doméstico. No obstante, para una tal transmisión con éxito al aparato doméstico ha de llevarse con preferencia el smartphone 150 a las proximidades del aparato doméstico, por ejemplo a la misma sala. Con preferencia puede estar limitada la transmisión a varios centímetros o metros. Con ello queda asegurado que no puede tener lugar ninguna liberación o transmisión de segundas informaciones (mensaje de texto) desde el smartphone 150 al aparato doméstico a lo largo de grandes distancias y con ello pueden activarse a distancia las primeras informaciones (informaciones de mantenimiento).

Mediante la inclusión del enlace NFC 700 en el tramo de comunicación entre el smartphone 150 y el aparato doméstico 103, mantiene el cliente el control prioritario y en el tiempo sobre la transacción del servicio al cliente y con ello también el control sobre la ejecución de las funciones de servicio al cliente. Sólo mediante el posicionado activo del smartphone 150 por parte del cliente hasta las proximidades (por ejemplo dentro del alcance del enlace NFC) del aparato doméstico 103, puede transmitirse la clave de prueba 520 (las segundas informaciones) para comprobar y/o verificar y ejecutar la transacción de servicio al cliente (de las primeras informaciones) a través del enlace NFC 700 al aparato doméstico 700. A continuación puede verificarse la clave de prueba 520 transmitida a través del enlace de Internet o bien primera vía de comunicación y ejecutarse una acción predeterminada. El cliente lleva por lo tanto el smartphone 150 a las proximidades del aparato doméstico 103, da lugar a la retransmisión o transmisión de la clave

de prueba 520 transmitida a través de la red de comunicación móvil 400 al smartphone 150 y da así su acuerdo para realizar la acción predeterminada.

Opcionalmente puede realizarse la consulta relativa a un PIN mediante una aplicación sobre el smartphone 150, por ejemplo antes de establecerse el enlace NFC 700 o antes de enviar la clave de prueba 520.

Alternativamente puede retransmitirse el mensaje de texto 540 recibido por el smartphone 150 y que contiene el enlace de prueba 520 a través de un enlace por hilo, por ejemplo a través de un enlace USB a establecer igualmente por parte del cliente, a la máquina lavadora 103.

Con ayuda de la clave de prueba 520 transmitida en el mensaje de texto 540 se comprueba la coincidencia de las informaciones de mantenimiento 530 específicas de la solicitud o bien de la clave de prueba 520 asociada a la misma, transmitida a través del enlace de Internet 500 a la máquina lavadora 103. Sólo cuando se detecta coincidencia ejecuta el control de la máquina lavadora 103 correspondientemente la acción prescrita, por ejemplo la transacción de servicio al cliente, es decir, las órdenes o funciones de mantenimiento contenidas en las informaciones de mantenimiento 530. En una etapa opcional que va a continuación se envían de retorno resultados de la transacción de servicio al cliente realizada a través del enlace de Internet 500 o a través de otro enlace establecido para ello al servidor de servicio al cliente 301 para la evaluación.

Según un perfeccionamiento del procedimiento propuesto, para aumentar la seguridad antes de la transmisión del mensaje de texto 540, puede firmarse el mismo en el marco de un procedimiento de encriptado asimétrico mediante la clave privada 350 del centro de servicio al cliente 300 archivada en el equipo de encriptado 302 y a continuación transmitirse el mensaje de texto 540 firmado de la forma descrita a través de la red de telefonía móvil 400, así como a través del smartphone 150 (asociado al hogar 100) a la máquina lavadora 103. La máquina lavadora 103 realiza la autentificación del centro de servicio al cliente 300 frente a la máquina lavadora 103 con ayuda de la clave pública 351 memorizada en el equipo de encriptado 120.

Alternativamente puede realizarse la autentificación del centro de servicio al cliente 300 frente a la máquina lavadora 103 también antes de la transmisión a través del enlace NFC por parte del smartphone 150.

Tal como ya se ha descrito, se transmite en el marco del procedimiento propuesto la clave de prueba 520 (también denominada secreto) tanto a través de la primera vía de comunicación 500 como también a través de la segunda vía de comunicación 700 a la máquina lavadora 103. Con preferencia se realiza en al menos una de estas vías de transmisión un encriptado de la clave de prueba 520, con lo que un atacante no puede averiguar la clave de prueba 520 en texto explicito. Mediante la inclusión del smartphone 150 en la segunda vía de transmisión queda asegurado con preferencia que la clave de prueba 520 se transmite a través de una comunicación de campo cercano 700 a la máquina lavadora 103. Sólo cuando la clave de prueba 520 transmitida a través de la primera vía de comunicación 500 o a través de la primera vía de transmisión también ha podido transmitirse y verificarse con éxito a través de la comunicación de campo cercano 700, se ejecuta la acción predeterminada.

La clave de prueba 520 puede transmitirse encriptada o firmada a través de la primera y/o segunda vía de comunicación. Para ello pueden utilizarse con preferencia las claves asimétricas 350, 141, 351, 140 archivadas en los equipos de encriptado 302, 120 del centro de mantenimiento 300 o bien de la máquina lavadora 103. Opcionalmente puede lograrse un tal mecanismo también con claves simétricas.

Mediante la sustitución de una clave de prueba 520 con validez opcionalmente limitada (por ejemplo limitada en el tiempo y/o limitada a al menos una acción predeterminada) se minimiza el peligro, citado al principio y existente debido a la creciente criminalidad en Internet, de utilización abusiva de las posibilidades privilegiadas de acceso.

Otro aseguramiento adicional consiste en la firma y/o encriptado opcional de las informaciones de mantenimiento 530 transmitidas a través de la primera vía de comunicación 500 (por parte del centro de mantenimiento 300) mediante la clave de prueba 520 generada para la transición del servicio al cliente (en el marco de un procedimiento de encriptado por ejemplo simétrico), realizándose mediante la máquina lavadora 103 la autentificación así como el desencriptado mediante la clave de prueba 520 transmitida mediante el mensaje de texto 540 a través de la segunda vía de comunicación 700.

Un aseguramiento adicional consiste en la exigencia de la presencia o bien actuación del cliente o bien usuario directamente in situ en el aparato doméstico en cuestión durante la ejecución de una transacción especial remota de servicio al cliente. Esto puede lograrse por ejemplo mediante operaciones interactivas (periódicas) a ejecutar por el cliente mediante una aplicación que corre por ejemplo en el aparato terminal móvil de comunicación mientras existe el enlace NFC hacia el aparato doméstico. El mando y control de las operaciones interactivas a ejecutar por el usuario puede realizarse por ejemplo mediante el centro remoto de servicio al cliente.

Mediante la utilización, necesaria para ejecutar el procedimiento propuesto, de por ejemplo un aparato terminal móvil de comunicación junto con un acceso a telefonía móvil asociado inequívocamente al usuario o bien al hogar, junto

con la transmisión de datos NFC en el marco de una comunicación de dos vías, se minimiza o elimina una pérdida potencialmente perceptible por parte del usuario del control directo y con vigilancia por parte del propio usuario.

Lista de referencias

100	aparato doméstico
101	armario frigorífico
102	horno para cocinar
103	máquina lavadora
105	interfaz de red
110	red doméstica
120	equipo de encriptado (máquina lavadora)
125	equipo NFC
130	enlace Internet
140	clave privada (máquina lavadora)
141	clave pública (máquina lavadora)
145	número de telefonía móvil
150	smartphone
200	red de comunicación global (Internet)
300	centro de servicio al cliente
301	servidor de servicio al cliente
302	equipo de encriptado (centro de servicio al cliente)
310	red de comunicación local
320	enlace Internet
350	clave privada (centro de servicio al cliente)
351	clave pública (centro de servicio al cliente)
400	red de telefonía móvil
420	enlace de red de telefonía móvil
500	enlace bidireccional de Internet
510	solicitud de servicio al cliente
520	clave de prueba
530	informaciones de mantenimiento
540	mensaje de texto
700	enlace NFC (Near Field Communication)

REIVINDICACIONES

1. Procedimiento para procesar informaciones en un aparato doméstico (101 a 103), en el que
   - se transmite desde el aparato doméstico (103) un mensaje (510) a una unidad central (300),
   - se transmiten desde la unidad central (300) primeras informaciones (520, 530) a través de una primera vía de comunicación (500) al aparato doméstico (103).
   - se transmiten desde la unidad central (300) segundas informaciones (520) a un aparato terminal de comunicación (150) y
   - desde el aparato terminal de comunicación (150) se transmiten las segundas informaciones (520) a través de una segunda vía de comunicación (700) al aparato doméstico (103),
   - comprobando el aparato doméstico (103) las primeras informaciones (520, 530) con ayuda de las segundas informaciones (520),

   caracterizado porque
   - la segunda vía de comunicación (700) está configurada como un enlace punto a punto con alcance limitado, con lo que una comprobación con éxito de las primeras informaciones (520, 530) con ayuda de las segundas informaciones (520) puede entenderse como conformidad de un usuario.

2. Procedimiento según la reivindicación 1,
   en el que la comprobación incluye una autentificación de las primeras informaciones (520, 530).

3. Procedimiento según una de las reivindicaciones precedentes,
   en el que tras una comprobación con éxito se ejecuta al menos una acción predeterminada.

4. Procedimiento según la reivindicación 3,
   en el que la acción predeterminada incluye
   - una actualización de un software del aparato doméstico,
   - una ampliación de una funcionalidad del aparato doméstico,
   - una realización de una acción de mantenimiento o aplicación de mantenimiento,
   - una transmisión de una información de mantenimiento a un destinatario,
   - una realización de una prueba,
   - una ejecución de informaciones relativas a órdenes para el control del diagnóstico,
   - una ejecución de las primeras informaciones o bien
   - una utilización de las primeras informaciones.

5. Procedimiento según una de las reivindicaciones precedentes,
   en el que las segundas informaciones (520) se transmiten a través de un enlace de telefonía móvil al aparato terminal de comunicaciones (150).

6. Procedimiento según la reivindicación 5,
   En el que las segundas informaciones (520) se transmiten mediante
   - un MMS,
   - un SMS, o
   - un e-mail.

7. Procedimiento según una de las reivindicaciones precedentes,
   en el que la segunda vía de comunicación (700) está configurada como
   - enlace de comunicación de zona próxima,
   - enlace Bluetooth o bien
   - enlace de infrarrojos.

8. Procedimiento según una de las reivindicaciones precedentes,
   en el que las segundas informaciones (520) incluyen al menos parcialmente informaciones sobre claves.

9. Procedimiento según una de las reivindicaciones precedentes,
   en el que el aparato doméstico (103) firma el mensaje (510) antes de la transmisión con ayuda de un procedimiento de encriptado asimétrico.

10. Procedimiento según una de las reivindicaciones precedentes,
    en el que las segundas informaciones (520) transmitidas a través del aparato terminal de comunicaciones (150) se firman antes de la transmisión por parte de la unidad central (300) con ayuda de un procedimiento de encriptado asimétrico.

11. Procedimiento según la reivindicación 10,

en el que las segundas informaciones (520) firmadas transmitidas a través de la segunda vía de comunicación(700) son autentificadas por el aparato doméstico (103).

12. Procedimiento según la reivindicación 10 u 11,
en el que las segundas informaciones (520) firmadas transmitidas son autentificadas por el aparato terminal de comunicación (150).

13. Procedimiento según una de las reivindicaciones precedentes,
en el que el establecimiento de la segunda vía de comunicación (700) está asegurado mediante la introducción de un código personal de identificación (PIN).

14. Procedimiento según una de las reivindicaciones precedentes,
en el que la primera vía de comunicación (500) está configurada como enlace de datos asegurado criptográficamente a través de Internet.

15. Configuración para procesar informaciones en un aparato doméstico (101 a 103), con
- medios de transmisión (105) asociados al aparato doméstico (103) para transmitir un mensaje (510) a una unidad central (300),
- al menos un equipo (301, 302) asociado a la unidad central (300) para
  - transmitir primeras informaciones (520, 530) a través de una primera vía de comunicación (500) al aparato doméstico (103) y
  - transmitir segundas informaciones (520) a un aparato terminal de comunicación (150) y
- medios emisores asociados al aparato terminal de comunicación (150) para transmitir las segundas informaciones (520) a través de una segunda vía de comunicación (700) al aparato doméstico (103) y
- medios de comprobación asociados al aparato doméstico (103) para comprobar las primeras informaciones (520, 530) con ayuda de las segundas informaciones (520),
- **caracterizada porque**
- la segunda vía de comunicación (700) está configurada como un enlace punto a punto con alcance limitado, con lo que una comprobación con éxito de las primeras informaciones (520, 530) con ayuda de las segundas informaciones (520) puede entenderse como conformidad de un usuario.

16. Aparato doméstico para procesar informaciones con
- medios emisores (105) para transmitir un mensaje (510) a una unidad central (300),
- medios receptores (105) para recibir
  - primeras informaciones (520, 530) transmitidas a través de una primera vía de comunicación (500) desde la unidad central (300) y
  - segundas informaciones (520) transmitidas a través de una segunda vía de comunicación (700) desde un aparato terminal de comunicación (150) y
- medios de comprobación para comprobar las primeras informaciones (520, 530) con ayuda de las segundas informaciones (520),

caracterizado porque
- la segunda vía de comunicación (700) está configurada como un enlace punto a punto con alcance limitado, con lo que una comprobación con éxito de las primeras informaciones (520, 530) con ayuda de las segundas informaciones (520) puede entenderse como conformidad de un usuario.

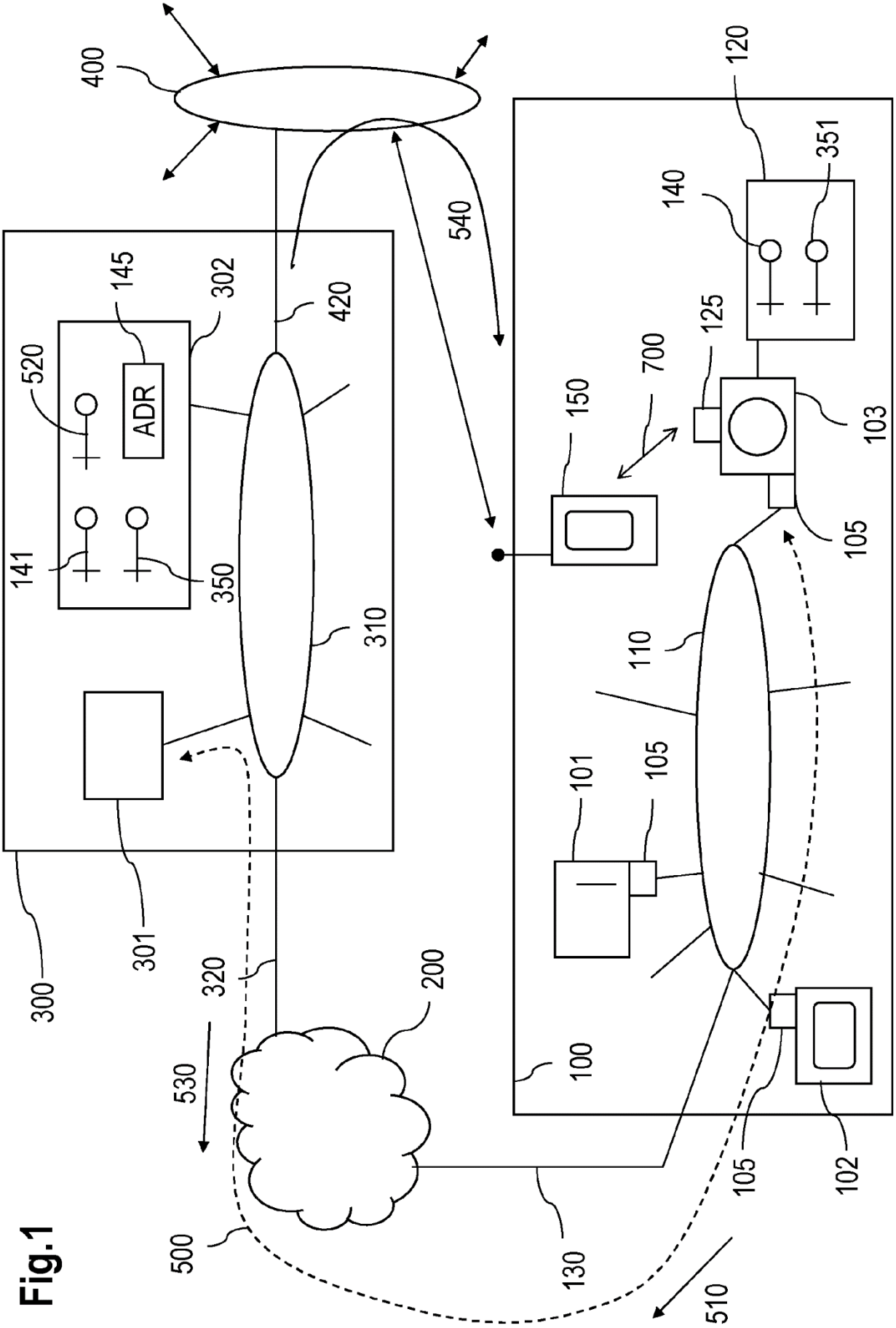
400
120
351
140
540
145
302
420
125
700
520
ADR
150
103
141
350
105
310
110
101
105
300
301
320
200
530
100
500
130
105
102
510

Fig.1