(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 573 692**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)
G06F 21/34 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.09.2009 E 09782622 (6)**

(97) Fecha y número de publicación de la concesión europea: **27.04.2016 EP 2332313**

(54) Título: **Procedimiento para el almacenamiento de datos, producto de programa informático, ficha de ID y sistema informático**

(30) Prioridad:

22.09.2008 DE 102008042262
02.10.2008 DE 102008042582

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.06.2016

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
Oranienstrasse 91
10958 Berlin, DE

(72) Inventor/es:

FISCHER, JÖRG;
DIETRICH, FRANK y
PAESCHKE, MANFRED

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento para el almacenamiento de datos, producto de programa informático, ficha de ID y sistema informático

La invención se refiere a un procedimiento para el almacenamiento de datos, un producto de programa informático, una ficha de ID, en particular un documento de valor o de seguridad, así como un sistema informático.

Por el estado de la técnica son conocidos diferentes procedimientos para la gestión de la llamada identidad digital de un usuario.

Windows CardSpace de Microsoft es un sistema de identidad digital basado en cliente, que debe permitir a los usuarios de Internet comunicar su identidad digital frente a servicios en línea. Un inconveniente del mismo es, entre otras cosas, que el usuario puede manipular su identidad digital.

OPENID es, por el contrario, un sistema basado en servidor. Un denominado servidor de identidad almacena una base de datos con las identidades digitales de los usuarios registrados. En este caso es desfavorable, entre otras cosas, que se trata de una protección pobre de los datos, ya que las identidades digitales de los usuarios son almacenadas de forma central y el comportamiento del usuario se puede grabar.

Por el documento US 2007/0294431 A1 es conocido otro procedimiento para la gestión de las identidades digitales que requiere igualmente un registro del usuario.

En la solicitud de patente DE 2008 000067.1-31 no publicada en el momento de la solicitud de la misma solicitante, se da a conocer un procedimiento para la lectura de al menos un atributo almacenado en una ficha de ID, en el que se requiere tanto una autenticación del usuario como de un sistema informático con respecto a la ficha de ID para permitir un acceso de lectura a un atributo almacenado en la ficha de ID, de manera que este puede ser reenviado a un sistema informático para proporcionar un servicio.

Por el documento US 2003/0023858 A1 es conocido un procedimiento para la generación de un conjunto de datos que sirva como pasaporte electrónico. El conjunto de datos es descargado por un usuario y almacenado, por ejemplo, en un teléfono móvil.

Por el documento EP 1802155 es conocido un procedimiento para la autenticación de un usuario. El procedimiento incluye el envío de una demanda de autenticación a un aparato de autenticación, así como la generación de una primera información de autenticación. Un aparato móvil del usuario recibe esta información y en función de la primera información de autenticación genera una segunda información de autenticación. La segunda información de autenticación es enviada al aparato de autenticación y validada. En caso de una validación con éxito es generada una señal de autenticación.

Por el documento US 2005/071282 A es conocido un sistema y un procedimiento correspondiente para posibilitar transacciones seguras a través de una red informática que impide el robo de identidad en ordenadores que no sean dignos de confianza. Un ordenador cliente unido a la red proporciona una interfaz de usuario para un usuario, así como una conexión segura para la transmisión de informaciones de confianza del usuario a un ordenador servidor.

Por el documento US 2008/083827 A1 es conocido un procedimiento de seguridad para su uso en un terminal de comunicación. El procedimiento incluye las etapas de proporcionar una primera tarjeta, la combinación de la primera tarjeta con una segunda tarjeta para formar una tarjeta doble, la inicialización de la primera o segunda tarjeta, así como una etapa de verificación que sirve para que la tarjeta doble sea desactivada cuando de la etapa de verificación resulte que, por ejemplo, la primera o la segunda tarjeta fue sustituida por otra.

Frente a esto, la invención se propone el objeto de conseguir un procedimiento mejorado para el almacenamiento de datos, así como un producto de programa informático correspondiente, una ficha de ID y un sistema informático.

Los objetos que se propone la invención se llevan a cabo, respectivamente, con las características de las reivindicaciones independientes. Formas de realización de la invención se especifican en las reivindicaciones dependientes.

Según formas de realización de la invención se consigue un procedimiento para el almacenamiento de datos. Se establece una primera conexión entre una primera ficha de ID y un primer sistema informático a través de un segundo sistema informático. En cuanto al primer sistema informático puede tratarse de un sistema informático servidor, que en lo sucesivo será denominado también sistema informático proveedor de ID, y que está conectado al segundo sistema informático a través de una red, por ejemplo Internet. En cuanto al segundo sistema informático puede tratarse de un ordenador personal (PC) de un usuario, que en lo sucesivo será denominado también sistema informático de usuario. Por el primer sistema informático es leído al menos un primer atributo de la primera ficha de ID a través de la primera conexión.

Además es establecida una segunda conexión entre una segunda ficha de ID y el primer sistema informático a través del segundo sistema informático, para leer por lo menos un segundo atributo de la segunda ficha de ID. Para ello, el segundo sistema informático puede recibir del primer sistema informático una orden, según la cual debe ser establecida una conexión, respectivamente, para la primera y segunda fichas de ID, esto es, debe tener lugar una llamada sesión múltiple. De esta forma se evita que el segundo sistema informático interrumpa la primera conexión, después de que hayan sido leídos los primeros atributos de la primera ficha de ID.

Los primeros y segundos atributos son enviados por el primer sistema informático a un tercer sistema informático. En cuanto al tercer sistema informático puede tratarse de un sistema informático servidor, que está conectado al primer y/o al segundo sistema informático a través de la red. En cuanto al tercer sistema informático puede tratarse de un sistema informático servidor de un proveedor de servicios, que en lo sucesivo es denominado también sistema informático de servicio. Preferentemente, los primeros y segundos atributos del primer sistema informático son firmados digitalmente antes del reenvío al tercer sistema informático, de modo que el tercer sistema informático puede comprobar la fiabilidad de los primeros y segundos atributos.

Preferentemente, los primeros atributos del primer sistema informático son reenviados al tercer sistema informático inmediatamente después de la lectura de la primera ficha de ID, de manera que el primer atributo no tiene que ser almacenado de forma permanente por el primer sistema informático. Es suficiente, por el contrario, almacenar el primer atributo en el primer sistema informático solo durante el tiempo que sea necesario para reenviar el primer atributo al tercer sistema informático, después de que ha sido leído de la primera ficha de ID. Del mismo modo se procede preferentemente en relación con el segundo atributo, que igualmente es reenviado por el primer sistema informático al tercer sistema informático inmediatamente después de la lectura de la segunda ficha de ID. Una copia temporal de los primeros o segundos atributos eventualmente necesaria para el propósito del reenvío de los atributos desde el primer sistema informático al tercer sistema informático es borrada del primer sistema informático inmediatamente después del envío. Esto tiene la ventaja de que el primer sistema informático puede ser configurado sin estado, y que los datos que necesitan protección, que pueden incluir los primeros y segundos atributos, no son almacenados por el primer sistema informático.

El tercer sistema informático utiliza los primeros y segundos atributos recibidos por el primer sistema informático para la determinación de datos. Esto puede realizarse de manera que el tercer sistema informático calcula los datos a partir de los primeros y segundos atributos o mediante el acceso a una base de datos, con ayuda de los primeros y segundos atributos, consulta los datos de una base de datos. El primer sistema informático recibe entonces los datos del tercer sistema informático, por ejemplo a través de la red. La transferencia de los datos desde el tercer sistema informático al primer sistema informático se lleva a cabo preferiblemente a través de una conexión segura.

El primer sistema informático escribe después los datos en la segunda ficha de ID a través de la segunda conexión para almacenar los datos en la segunda ficha de ID. Un prerrequisito para ello es que también siga existiendo la primera conexión a la primera ficha de ID, y concretamente durante todo el período del proceso de escritura. Para ello se asegura que entretanto el usuario ha revocado su autorización para la escritura de la primera ficha de ID por parte del primer sistema informático, habiendo retirado su primera ficha de ID de un aparato de lectura del primer sistema informático, con lo que interrumpiría la primera conexión. Puesto que la escritura de los datos se realiza a través de la segunda conexión, se asegura además que la segunda conexión entretanto no ha sido interrumpida, de modo que la segunda ficha de ID haya sido sustituida por una ficha de ID por ejemplo manipulada, es decir, falseada o falsificada.

Esto es debido al hecho de que la primera y segunda conexiones son establecidas y mantenidas, respectivamente, con ayuda de un protocolo orientado a la conexión. Tal protocolo orientado a la conexión registra cuando uno de los dos participantes en la conexión es eliminado. De este modo, durante todo el periodo entre el establecimiento de la primera conexión y el establecimiento de la segunda conexión hasta la escritura de los datos es comprobada la condición necesaria de que tanto la primera como la segunda conexión no hayan sido interrumpidas hasta la finalización del proceso de escritura. Para el caso de que se interrumpa la primera o la segunda conexión antes de la terminación del proceso de escritura, los datos no son almacenados en la segunda ficha de ID.

Las formas de realización de la invención son particularmente ventajosas, ya que la invención permite describir de forma segura las segundas fichas de ID con datos individuales del documento, sirviendo la primera ficha de ID como "ancla de confianza". El propietario de la primera ficha de ID será puesto en situación de poder describir por primera vez su segunda ficha de ID con datos individuales del documento o actualizar tales datos individuales del documento y concretamente en línea, sin que el propietario de la primera ficha de ID deba por ejemplo buscar personalmente una autoridad.

Por ejemplo, la primera ficha de ID es asignada al usuario autorizado, es decir, al propietario de la ficha de identificación. Por ejemplo, en cuanto a la primera ficha de ID se trata de una tarjeta de identidad electrónica. Sin embargo, la segunda ficha de ID puede estar asociada a un objeto, por ejemplo a un automóvil. En cuanto a la segunda ficha de ID se trata, por ejemplo, de un permiso de circulación de automóvil electrónico o de un certificado de registro de automóvil electrónico. La invención permite actualizar el permiso de circulación de automóvil o certificado de registro de automóvil electrónico en línea, por ejemplo cuando cambia el titular del automóvil y/o la matrícula del vehículo.

Por un "documento" se entienden según la invención documentos basados en papel y/o basados en plástico, como por ejemplo documentos de identidad, en particular pasaportes, tarjetas de identidad, visados, así como permisos de conducir, permisos de circulación, certificados de registro de vehículos, tarjetas de identificación de empresa, tarjetas de salud u otros documentos de ID, así como tarjetas inteligentes, medios de pago, en particular tarjetas bancarias y tarjetas de crédito, cartas de porte u otras credenciales, en las que está integrada una memoria de datos para el almacenamiento de al menos un atributo.

De acuerdo con una forma de realización de la invención, en cuanto al protocolo orientado a la conexión de la primera y/o segunda conexiones se trata de un protocolo de transporte que transmite paquetes para el establecimiento de una conexión de extremo a extremo en modo dúplex completo, como por ejemplo el Protocolo de Control de Transmisión (TCP).

Las formas de realización de la invención son, pues, particularmente ventajosas, ya que es leído el al menos un atributo de un documento especialmente digno de confianza, por ejemplo un documento oficial. Especialmente ventajoso es además que no es necesario un almacenamiento central de los atributos. Por tanto, la invención permite un grado particularmente elevado de fiabilidad con respecto a la comunicación de los atributos pertenecientes a una identidad digital, unido a una óptima protección de los datos con un manejo extremadamente cómodo.

De acuerdo con una forma de realización de la invención, el primer sistema informático tiene al menos un certificado, que es utilizado para la autenticación del primer sistema informático con respecto a la primera y/o segunda ficha de ID. El certificado contiene una indicación de aquellos atributos para los que el primer sistema informático tiene una autorización de lectura. La ficha de ID en cuestión comprueba en base a este certificado si el primer sistema informático tiene la autorización de lectura necesaria para el acceso a la lectura del primer o segundo atributo, antes de que tal acceso de lectura pueda ser realizado por el primer sistema informático.

De acuerdo con una forma de realización de la invención, el primer sistema informático envía directamente al tercer sistema informático el al menos un primer o segundo atributo leído de la ficha de ID. En cuanto al tercer sistema informático puede tratarse, por ejemplo, de un servidor de una administración, por ejemplo de una oficina de registro de automóviles.

De acuerdo con una forma de realización de la invención, la transferencia de los atributos leídos de la ficha de ID del primer sistema informático es realizada en primer lugar al segundo sistema informático del usuario. Por ejemplo, el segundo sistema informático tiene un navegador estándar de Internet, con el que el usuario puede abrir una página web del tercer sistema informático. El usuario puede introducir en la página web una demanda para un servicio, por ejemplo la actualización de su certificado de registro de automóvil electrónico.

El tercer sistema informático a continuación especifica aquellos atributos, por ejemplo del usuario y/o de su primera y/o segunda ficha de ID, que son necesarios para la prestación del servicio o la aceptación del pedido. La especificación de atributo correspondiente, que incluye la especificación de estos atributos, es enviada entonces por el tercer sistema informático al primer sistema informático. Esto se puede realizar con o sin la interposición del segundo sistema informático. En este último caso, el usuario puede especificar el primer sistema informático deseado con respecto al tercer sistema informático, por ejemplo mediante la introducción de la URL del primer sistema informático en una página web del tercer sistema informático por el segundo sistema informático.

De acuerdo con una forma de realización de la invención, la demanda de servicio del usuario al tercer sistema informático incluye la indicación de un identificador, de modo que el identificador identifica al primer sistema informático. Por ejemplo, en cuanto al identificador se trata de un enlace, por ejemplo una URL del primer sistema informático.

De acuerdo con una forma de realización de la invención, la especificación de atributo no es enviada directamente por el tercer sistema informático al primer sistema informático, sino que en primer lugar es enviada por el tercer sistema informático al segundo sistema informático.

De acuerdo con una forma de realización de la invención, los atributos leídos de la primera o segunda ficha de ID son firmados por el primer sistema informático y transmitidos a continuación al segundo sistema informático. El usuario del segundo sistema informático puede por tanto leer los atributos, pero sin poder cambiarlos. Solo después del desbloqueo por el usuario los atributos son reenviados por el segundo sistema informático al tercer sistema informático.

De acuerdo con una forma de realización de la invención, el usuario puede completar los primeros y/o segundos atributos con otros datos antes de su reenvío.

De acuerdo con una forma de realización de la invención, el primer sistema informático tiene varios certificados con diferentes derechos de lectura. En base a la recepción de la especificación de atributo, el primer sistema informático selecciona uno o varios de estos certificados para leer los atributos correspondientes de las fichas de ID.

En otro aspecto, la invención se refiere a un producto de programa informático, en particular un medio de almacenamiento digital, con instrucciones de programa ejecutables para la realización de un procedimiento según la invención.

En otro aspecto, la invención se refiere a una ficha de ID con un área de memoria protegida para el almacenamiento de al menos un atributo, y para el almacenamiento de datos, medios para la autenticación de un primer sistema informático con respecto a la ficha de ID, medios para el establecimiento de una conexión con el primer sistema informático de acuerdo con un protocolo orientado a la conexión, mediante el cual el primer sistema informático puede leer el al menos un atributo, siendo un prerrequisito necesario para la lectura del al menos un atributo de la ficha de ID por el primer sistema informático, la autenticación con éxito del primer sistema informático con respecto a ficha de ID y en el que los datos pueden ser escritos en el área de memoria a través de la conexión.

Por ejemplo, en cuanto a la ficha de ID se trata de un permiso de circulación de vehículo electrónico, que está asignado fijamente solo a un automóvil, pero no a un usuario. Una autenticación del usuario con respecto a la ficha de ID puede entonces suprimirse.

Además de la autenticación del primer sistema informático con respecto a la ficha de ID, como es conocido en sí, por ejemplo por el denominado control de acceso ampliado para documentos de viaje legibles por máquina (documentos de viaje de lectura mecánica - MRTD) y está especificado por la Autoridad de Aviación Civil Internacional, ICAO, según la forma de realización puede ser necesario que también el usuario sea autenticado con respecto a la ficha de ID. Por ejemplo, por una autenticación con éxito del usuario con respecto a la ficha de ID se produce un desbloqueo, de modo que pueden desarrollarse las siguientes etapas, concretamente, la autenticación del primer sistema informático con respecto a la ficha de ID y/o el establecimiento de una conexión protegida para la lectura de los atributos.

De acuerdo con una forma de realización de la invención, la ficha de ID tiene medios para un cifrado de extremo a extremo. Esto hace que sea posible establecer la conexión entre la ficha de ID y el primer sistema informático a través de un tercer sistema informático del usuario, ya que el usuario no puede acometer cambios de los datos transmitidos a través de la conexión debido al cifrado de extremo a extremo.

En otro aspecto, la invención se refiere a un primer sistema informático con un sistema informático con medios para el establecimiento de una primera conexión entre una primera ficha de ID y un primer sistema informático a través de un segundo sistema informático para la lectura de al menos un primer atributo de la primera ficha de ID, medios para el establecimiento de una segunda conexión entre una segunda ficha de ID y el primer sistema informático a través del segundo sistema informático para la lectura de al menos un segundo atributo de la segunda ficha de ID, medios para el envío de los primeros y segundos atributos del primer sistema informático a un tercer sistema informático, medios para la recepción de los datos del tercer sistema informático por el primer sistema informático, medios para la escritura de los datos del primer sistema informático en la segunda ficha de ID a través de la segunda conexión para almacenar los datos en la segunda ficha de ID, siendo un prerrequisito para la escritura de los datos que también siga existiendo la primera conexión, de modo que en cuanto a la primera y segunda conexiones se trata, respectivamente, de conexiones con cifrado de extremo a extremo y con un protocolo orientado a la conexión.

De acuerdo con formas de realización de la invención, el primer sistema informático tiene medios para la recepción de una especificación de atributo a través de una red, en el que la especificación de atributo especifica al menos un atributo, medios para la autenticación con respecto a una ficha de ID, medios para la lectura de al menos un atributo de la ficha de ID a través de una conexión segura, en el que la lectura del al menos un atributo presupone que un usuario asignado a la ficha de ID ha sido autenticado con respecto a la ficha de ID.

De acuerdo con una forma de realización de la invención, el primer sistema informático puede incluir medios para la generación de un requerimiento al usuario. Después de que el primer sistema informático ha recibido la especificación de atributo, por ejemplo del tercer sistema informático, este envía a continuación un requerimiento al segundo sistema informático del usuario, de manera que al usuario se le requiere que se autentifique con respecto a la primera y/o segunda ficha de ID. Después de que haya sido realizada con éxito la autenticación del usuario con respecto a la primera y/o segunda ficha de ID, el primer sistema informático recibe del segundo sistema informático una confirmación. Acto seguido, el primer sistema informático se autentica con respecto a la ficha de ID en cuestión y se establece la primera o segunda conexión segura entre la ficha de ID y el primer sistema informático con un cifrado de extremo a extremo.

De acuerdo con una forma de realización de la invención, el primer sistema informático tiene varios certificados que especifican, respectivamente, diferentes derechos de lectura y/o derechos de escritura. Tras la recepción de la especificación de atributo, el primer sistema informático selecciona al menos uno de estos certificados con los derechos de lectura suficientes para la lectura de los atributos especificados. Además, el primer sistema informático selecciona aquel certificado que especifica los derechos necesarios para la escritura de los datos en la segunda ficha de ID para comprobar su autorización correspondiente con respecto a la segunda ficha de ID.

Las formas de realización del primer sistema informático según la invención son particularmente ventajosas, ya que en combinación con la necesidad de la autenticación del usuario con respecto a la ficha de ID constituyen un ancla

de confianza para la identidad digital no falsificada del usuario. Aquí es particularmente ventajoso que esto no requiere registro previo del usuario con respecto al primer sistema informático, así como tampoco un almacenamiento central de los atributos del usuario que constituyen las identidades digitales.

De acuerdo con una forma de realización de la invención, en cuanto al primer sistema informático se trata de un centro de confianza certificado por una autoridad, en particular un centro de confianza conforme a la ley de firma electrónica.

A continuación se explicarán en detalle formas de realización de la invención con referencia a los dibujos. Muestran:

Figura 1, un diagrama de bloques de una forma de realización de sistemas informáticos y fichas de ID según la invención,

Figura 2, un diagrama de flujo de una forma de realización de un procedimiento según la invención,

Figura 3, un diagrama de bloques de otra forma de realización de sistemas informáticos y fichas de ID según la invención,

Figura 4, un diagrama de flujo de otra forma de realización de un procedimiento según la invención,

Figura 5, un diagrama UML de otra forma de realización de un procedimiento según la invención, y

Figura 6, un diagrama de bloques de otra forma de realización de sistemas informáticos y fichas de ID según la invención.

Los elementos de las siguientes formas de realización que se corresponden entre sí están caracterizados por los mismos símbolos de referencia.

La figura 1 muestra un diagrama de bloques de una forma de realización de un sistema de procesamiento de datos según la invención. El sistema de procesamiento de datos tiene un sistema informático de usuario 100. En cuanto al sistema informático de usuario 100 puede tratarse de un PC, un ordenador transportable, por ejemplo un ordenador portátil o un ordenador de bolsillo, un asistente digital personal (PDA), un aparato de telecomunicación móvil, en particular un teléfono inteligente, o similares.

El sistema informático de usuario 100 sirve para la comunicación con la ficha de ID A 106 y la ficha de ID B 107. La comunicación entre las fichas de ID A y B, por un lado, y el sistema informático de usuario 100, por otro lado, puede realizarse con contacto o sin contacto, en particular, de acuerdo con un procedimiento RFID. En cuanto a la ficha de ID A puede tratarse de una tarjeta de identidad electrónica, es decir, una tarjeta de identidad que incluye un chip de RFID, en el que están almacenados los atributos del usuario.

La ficha de ID B puede en principio estar formada como la ficha de ID A, de modo que la ficha de ID B no está asignada al usuario, sino a un objeto, por ejemplo a un automóvil. Por ejemplo, en cuanto a la ficha de ID B se trata de un permiso de circulación de automóvil electrónico o de un certificado de registro de automóvil electrónico, en el que están almacenados atributos del automóvil.

Un aparato lector adecuado (no representado en la figura 1) está conectado al sistema informático de usuario 100 o integrado en el sistema informático de usuario 100, de modo que el sistema informático de usuario 100 puede comunicarse con las fichas de ID A y B. El aparato lector está diseñado en este caso para que pueda existir al mismo tiempo una primera conexión A 101 entre la ficha de ID A y el sistema informático de usuario 100, así como una segunda conexión B 103 entre la ficha de ID B y el sistema informático de usuario 100.

En la ficha de ID B está almacenado al menos un atributo que establece la asignación de la ficha de ID B al objeto, por ejemplo al automóvil. En cuanto a este atributo puede tratarse de un llamado identificador único del objeto, como por ejemplo el número de bastidor del vehículo o similar.

El sistema informático de usuario 100 está unido a una red 116, por ejemplo Internet, con un sistema informático de servicio 150. En cuanto al sistema informático de servicio 150 puede tratarse de un sistema informático servidor de una institución, por ejemplo una oficina de registro de vehículos.

Además, el sistema informático de usuario 100 está unido al sistema informático proveedor de ID 136 a través de la red 116. El sistema informático proveedor de ID 136 sirve para la lectura de los atributos de las fichas de ID A y B, para el reenvío de estos atributos al sistema informático de servicio 150, para la recepción de datos desde el sistema informático de servicio 150 y para un acceso de escritura sobre la base de estos datos a la ficha de ID B para actualizar la ficha de ID B. En cuanto a los datos puede tratarse, por ejemplo, de valores de atributo actualizados.

Si, por ejemplo, debido a un cambio del usuario, cambia la matrícula de su automóvil, entonces la ficha de ID B puede ser actualizada con la nueva matrícula de la siguiente manera, sin que el usuario tenga que buscar una autoridad para este propósito.

Entre la ficha de ID A y el sistema informático proveedor de ID 136 es establecida una primera conexión A 101. En cuanto a la conexión 101 se trata de una conexión con cifrado de extremo a extremo, de modo que los datos sustituidos a través de la conexión 101 no son desencriptados ni por el sistema informático de usuario 100 ni por otros miembros de la red 116. La conexión 101 es establecida y mantenida con ayuda de un protocolo orientado a la conexión.

Se procede de forma similar con respecto a la ficha de ID B. Entre la ficha de ID B y el sistema informático proveedor de ID 136 es establecida una segunda conexión B 103, y concretamente de igual modo a través del sistema informático de usuario 100 y la red 116 con cifrado de extremo a extremo e igualmente con el protocolo orientado a la conexión.

El sistema informático proveedor de ID 136 a través de la conexión 101 lee al menos un primer atributo A de la ficha de ID A o varios de tales atributos A, por medio de los cuales es identificado el usuario de forma única. Por ejemplo, puede tratarse en este caso del nombre, la fecha de nacimiento y el lugar de residencia del usuario.

Los atributos A son firmados digitalmente por el sistema informático proveedor de ID 136 y reenviados al sistema informático de servicio 150. Esto se realiza preferiblemente, de manera que el sistema informático proveedor de ID 136 no conserve copia de los atributos A después de que los atributos A, con la firma, hayan sido enviados al sistema informático de servicio 150.

Del mismo modo se procede con respecto al segundo atributo B que está almacenado en la ficha de ID B. El atributo B, por ejemplo el número de bastidor del vehículo, es leído por el sistema informático proveedor de ID 136 a través de la conexión 103 de la ficha de ID B, es firmado y reenviado al sistema informático de servicio 150.También preferentemente del atributo B no es almacenada copia en el sistema informático proveedor de ID 136 después del envío al sistema informático de servicio 150.

El sistema informático de servicio 150, con ayuda de los atributos A y del atributo B, determina la matrícula actualizada del automóvil que es identificada por el atributo B. Por ejemplo, el sistema informático de servicio 150 determina esta nueva matrícula por una consulta de base de datos en una base de datos en la que están almacenadas tales matriculas. Para la consulta de base de datos pueden ser empleados los atributos A y/o el atributo B.

El sistema informático de servicio 150 envía al sistema informático proveedor de ID 136 datos que contienen la nueva matrícula. Preferiblemente, el sistema informático de servicio 150 firma los datos, de manera que el sistema informático proveedor de ID 136 puede comprobar esta firma, para proporcionar seguridad en cuanto a la autenticidad de estos datos.

Los datos con la nueva matrícula son enviados después por el sistema informático proveedor de ID 136 a través de la conexión 103 a la ficha de ID B, de modo que la nueva matrícula es almacenada allí. Además, el sistema informático proveedor de ID 136 puede escribir la dirección actualizada del usuario de esta manera en la ficha de ID B. Para ello, puede ser necesario que el sistema informático proveedor de ID 136 acceda de nuevo a través de la conexión 101 a la ficha de ID A para leer los atributos con la dirección modificada.

Para un acceso de escritura del sistema informático proveedor de ID 136 a través de la conexión 103 a la ficha de ID B, es un prerrequisito necesario que siga existiendo la conexión 101 a la ficha de ID A. Con ello se asegura que el "ancla de confianza" está todavía presente, cuando los datos, es decir por ejemplo la nueva matrícula, son escritos en la ficha de ID B a través de la conexión 103.

La figura 2 muestra un diagrama de flujo correspondiente.

En la etapa 10 se establece la conexión A entre el proveedor de ID y la ficha de ID A, y concretamente con un protocolo orientado a la conexión, y con cifrado de extremo a extremo. En la etapa 12 son leídos los atributos A de la ficha de ID A por el proveedor de ID, y concretamente a través de la conexión A. Los atributos A son entonces reenviados por el proveedor de ID en la etapa 14 al servicio (véase el sistema informático proveedor de ID 136 y el sistema informático de servicio 150 en la forma de realización de la figura 1).

De forma análoga se procede en las etapas 16, 18 y 20 con respecto a la ficha de ID B y los atributos B almacenados en la ficha de ID B, que son por tanto igualmente recibidos por el servicio.

En la etapa 22, con ayuda de los atributos A y B, el servicio determina los datos que deben ser utilizados para la actualización de la ficha de ID B. Estos datos pueden incluir por ejemplo la matrícula del automóvil que está asignada a la ficha de ID B.

En la etapa 24 estos datos son enviados por el servicio al proveedor de ID. Si la ficha de ID B debe ser actualizada también con los atributos A, entonces estos atributos A son leídos de nuevo en la etapa 26 por el proveedor de ID a través de la conexión A. En la etapa 28, el proveedor de ID, a partir de los atributos A y de los datos recibidos por el servicio, genera los datos de escritura, es decir, un conjunto de datos que incluye los datos que se van a escribir en la ficha de ID B.

En la etapa 30, el proveedor de ID comprueba si sigue existiendo la conexión A. Si este es el caso, en la etapa 32 los datos de escritura son escritos en la ficha de ID B por el proveedor de ID a través de la conexión B y almacenados allí, de modo que la ficha de ID B está actualizada. En caso contrario, el proveedor de ID interrumpe el proceso en la etapa 34, ya que no es posible una escritura segura de los datos de escritura en la ficha de ID B debido a la ruptura de la conexión A.

La figura 3 muestra un sistema informático de usuario 100 de un usuario 102. El sistema informático de usuario 100 tiene una interfaz 104 para la comunicación con la ficha de ID 106 A, que presenta una interfaz 108 correspondiente.

El sistema informático de usuario 100 tiene al menos un procesador 110 para la ejecución de las instrucciones del programa 112, así como una interfaz de red 114 para la comunicación a través de una red 116. En cuanto a la red puede tratarse de una red informática, como por ejemplo Internet.

La ficha de ID 106 tiene una memoria electrónica 118 con áreas de memoria protegida 120, 122 y 124. El área de memoria protegida 120 sirve para el almacenamiento de un valor de referencia que es necesario para la autenticación del usuario 102 con respecto a la ficha de ID 106. En cuanto a este valor de referencia se trata, por ejemplo, de un identificador, en particular un denominado Número de Identificación Personal (PIN), o de datos de referencia para una característica biométrica del usuario 102, que puede ser empleada para la autenticación del usuario con respecto a la ficha de ID 106.

El área protegida 122 sirve para el almacenamiento de una clave privada y el área de almacenamiento protegida 124 sirve para el almacenamiento de atributos, por ejemplo del usuario 102, como por ejemplo su nombre, lugar de residencia, fecha de nacimiento, sexo y/o atributos que se refieren a la propia ficha de ID, como por ejemplo la institución que ha creado o emitido la ficha de ID, la validez de la ficha de ID, un identificador de la ficha de ID, como por ejemplo un número de pasaporte o un número de tarjeta de crédito.

La memoria electrónica 118 puede presentar además un área de memoria 126 para el almacenamiento de un certificado. El certificado contiene una clave pública que ha sido asignada a la clave privada almacenada en el área de memoria protegida 122. El certificado puede haber sido creado de acuerdo con un estándar de infraestructura de clave pública (PKI), por ejemplo, de acuerdo con el estándar X.509.

El certificado no tiene necesariamente que estar almacenado en la memoria electrónica 118 de la ficha de ID 106. Alternativa o adicionalmente, el certificado puede también estar almacenado en un servidor de directorio público.

La ficha de ID 106 tiene un procesador 128. El procesador 128 sirve para la ejecución de instrucciones de programa 130, 132 y 134. Las instrucciones de programa 130 sirven para la autenticación del usuario, es decir, para la autenticación del usuario 102 con respecto a la ficha de ID.

En una forma de realización con PIN, el usuario introduce su PIN 102 en la ficha de ID 106 para su autenticación, por ejemplo a través del sistema informático de usuario 100. Por la ejecución de las instrucciones del programa 130 a continuación se accede al área de memoria protegida 120 para comparar el PIN introducido con el valor de referencia del PIN almacenado allí. En el caso de que el PIN introducido coincida con el valor de referencia del PIN, el usuario 102 es considerado como autenticado.

Alternativamente, es detectada una característica biométrica del usuario 102. Por ejemplo, la ficha de ID 106 tiene para ello un sensor de huella dactilar o un sensor de huella digital está conectado al sistema informático de usuario 100. En esta forma de realización los datos biométricos detectados del usuario 102 son comparados con los datos de referencia biométricos almacenados en el área de memoria protegida 120 mediante la ejecución de las instrucciones del programa 130. En caso de suficiente coincidencia de los datos biométricos detectados del usuario 102 con los datos de referencia biométricos, el usuario 102 es considerado autenticado.

Las instrucciones de programa 134 sirven para la ejecución de las etapas referentes a la ficha de ID 106 de un protocolo criptográfico para la autenticación de un sistema informático proveedor de ID 136 con respecto a la ficha de ID 106. En cuanto al protocolo criptográfico puede tratarse de un protocolo desafío-respuesta basado en una clave simétrica o un par de claves asimétricas.

Por ejemplo, por el protocolo criptográfico es implementado un procedimiento de control de acceso ampliado como está especificado para documentos de viaje legibles a máquina (documentos de viaje de lectura mecánica - MRTD) por la Autoridad de Aviación Civil Internacional (ICAO). Por la ejecución con éxito del protocolo criptográfico el sistema informático proveedor de ID 136 se autentica con respecto a la ficha de ID y, por tanto, comprueba su autorización de lectura para leer los atributos almacenados en el área de memoria protegida 124. La autenticación también puede ser mutua, es decir, también la ficha de ID 106 debe autenticarse con respecto al sistema informático proveedor de ID 136 de acuerdo con el mismo u otro protocolo criptográfico.

Las instrucciones de programa 132 sirven para el cifrado de extremo a extremo de datos transmitidos entre la ficha de ID 106 y el sistema informático proveedor de ID 136, pero al menos de los atributos leídos por el sistema informático proveedor de ID 136 del área de memoria protegida 124. Para el cifrado de extremo a extremo puede ser

utilizada una clave simétrica que pueda ser acordada entre la ficha de ID 106 y el sistema informático proveedor de ID 136, por ejemplo, con ocasión de la ejecución del protocolo criptográfico.

Las instrucciones del programa 131 sirven para la realización del protocolo orientado a la conexión por parte de la ficha de ID 106. Por ejemplo, en cuanto al protocolo orientado a la conexión puede tratarse de un TCP. Por "protocolo orientado a la conexión" se entiende cualquier protocolo para la formación de un canal virtual entre dos puntos finales, aquí entre una ficha de ID y el sistema informático proveedor de ID 136. En este canal se puede transmitir en ambas direcciones. Por ejemplo, se utiliza para ello un protocolo propietario o un protocolo estándar, como por ejemplo TCP. TCP está establecido en la etapa 4d el modelo de referencia OSI y se puede disponer sobre el protocolo de Internet.

Como alternativa a la forma de realización representada en la figura 3, el sistema informático de usuario 100 con su interfaz 104 puede comunicar no directamente con la interfaz 108, sino a través de un aparato lector para las fichas de ID 106 conectado a la interfaz 104. Mediante este aparato lector, por ejemplo un llamado terminal de tarjetas inteligentes clase 2, puede realizarse también la introducción del PIN.

La interfaz 104 y eventualmente el aparato lector están diseñados de tal manera que pueden mantenerse al mismo tiempo las conexiones 101 y 103 (véase la Fig.1). Por ejemplo, en el aparato lector están previstas dos ranuras para las fichas de ID A y B o es posible una comunicación simultánea con las fichas de ID A y B a través de un canal de RF.

En la forma de realización considerada aquí la ficha de ID B 107 está formada básicamente de la misma forma o similar a la ficha de ID A 106. Para la descripción de los componentes individuales de la ficha de ID B107 se remite, por tanto, a la descripción anterior de los componentes de la ficha de ID A 106. En contraste con la ficha de ID A puede realizarse un acceso de escritura a la zona de memoria protegida 124' a través de la conexión B para actualizar los valores de atributo allí almacenados con los datos de escritura. Aquí hay que considerar la excepción del valor del atributo con el identificador único, es decir, por ejemplo, el número de bastidor del vehículo, que es invariable.

Las instrucciones de programa 130' pueden omitirse en caso de que para la ficha de ID 107 no esté prevista la autenticación del usuario.

El sistema informático proveedor de ID 136 tiene una interfaz de red 138 para la comunicación a través de la red 116. El sistema informático proveedor de ID 136 tiene además una memoria 140, en la que está almacenada una clave privada 142 del sistema informático proveedor de ID 136, así como el certificado 144 correspondiente.

También en cuanto a este certificado puede tratarse, por ejemplo, de un certificado según un estándar PKI, como por ejemplo X.509.

El sistema informático proveedor de ID 136 tiene además al menos un procesador 145 para la ejecución de instrucciones de programa 146 y 148. Por la ejecución de las instrucciones de programa 146 son ejecutadas las etapas del protocolo criptográfico relativas al sistema informático proveedor de ID 136. En conjunto, por tanto, el protocolo criptográfico es implementado mediante la ejecución de las instrucciones de programa 134 por el procesador 128 de la ficha de ID 106 o de la ficha de ID 107, así como mediante la ejecución de las instrucciones de programa 146 por el procesador 145 del sistema informático proveedor de ID 136.

Las instrucciones de programa 148 sirven para la implementación del cifrado de extremo a extremo en el lado del sistema informático proveedor de ID 136, por ejemplo basado en la clave simétrica que fue acordada entre la ficha de ID 106 o 107 y el sistema informático proveedor de ID 136 con ocasión de la ejecución del protocolo criptográfico. En principio, puede ser empleado cualquiera de los procedimientos conocidos en sí para el acuerdo de la clave simétrica para el cifrado de extremo a extremo, como por ejemplo el intercambio de claves Diffie-Hellman.

Las instrucciones de programa 147 sirven para la implementación del protocolo orientado a la conexión, y concretamente de tal manera que puedan ser mantenidas simultáneamente las dos conexiones 101 y 103.

Las instrucciones del programa 151 sirven para la implementación de un programa de control para el control de proceso.

El sistema informático proveedor de ID 136 se encuentra preferiblemente en un entorno especialmente protegido, en particular en un denominado centro de confianza, de modo que el sistema informático proveedor de ID 136 en combinación con la necesidad de la autenticación del usuario 102 con respecto a la ficha de ID 106 constituye el ancla de confianza para la autenticidad de los atributos leídos de la ficha de ID 106.

El sistema informático de servicio 150 puede estar realizado para la recepción de una demanda de servicio para la inicialización, en particular para la actualización de la ficha de ID B.

El sistema informático de servicio 150 tiene para ello una interfaz de red 152 para la conexión a la red 116. Además, el sistema informático de servicio 150 tiene al menos un procesador 154 para la ejecución de instrucciones de

programa 156. Mediante la ejecución de las instrucciones del programa 156 son generadas, por ejemplo, páginas HTML dinámicas mediante las cuales el usuario 102 puede introducir su demanda de servicio.

Dependiendo del tipo de la demanda de servicio, el sistema informático de servicio 150 debe recibir uno o varios atributos de la ficha de ID 106 y de la ficha de ID 107 desde el sistema informático proveedor de ID 136 para poder ejecutar la demanda de servicio.

Para proporcionar el servicio puesto a disposición por el sistema informático de servicio 150 se procede, por ejemplo, como sigue:

1. Autenticación del usuario 102 con respecto a la ficha de ID 106.

   El usuario 102 se autentica con respecto a la ficha de ID 106. En el caso de una implementación con PIN, el usuario 102 introduce para ello su PIN, por ejemplo a través del sistema informático de usuario 100 o de un terminal de tarjetas inteligentes conectado al mismo. Mediante la ejecución de las instrucciones de programa 130 a continuación, la ficha de ID 106 comprueba la corrección del PIN introducido. Si el PIN introducido coincide con el valor de referencia del PIN almacenado en el área de memoria protegida 120, entonces el usuario 102 es considerado como autenticado. De forma análoga se puede proceder cuando es empleada una característica biométrica del usuario 102 para su autenticación, como se describió anteriormente.

2. Autenticación del sistema informático proveedor de ID 136 con respecto a la ficha de ID 106.

   Para ello se establece la conexión 101 entre la ficha de ID 106 y el sistema informático proveedor de ID 136 a través del sistema informático de usuario 100 y la red 116. Por ejemplo, el sistema informático proveedor de ID 136 transmite su certificado 144 a través de esta conexión 101 a la ficha de ID 106. Mediante las instrucciones de programa 134 es generado después un denominado desafío, es decir, por ejemplo, un número aleatorio. Este número aleatorio es encriptado con la clave pública del sistema informático proveedor de ID 136 contenida en el certificado 144. El texto cifrado resultante es enviado desde la ficha de ID 106 a través de la conexión al sistema informático proveedor de ID 136. El sistema informático proveedor de ID 136 desencripta el texto cifrado con ayuda de su clave privada 142 y obtiene así el número aleatorio. El número aleatorio es enviado de vuelta a la ficha de ID 106 por el sistema informático proveedor de ID 136 a través de la conexión. Mediante la ejecución de las instrucciones de programa 134 se comprueba allí si el número aleatorio recibido desde el sistema informático proveedor de ID 136 coincide con el número aleatorio generado originalmente, es decir, el desafío. Si este es el caso, el sistema informático proveedor de ID 136 es considerado autenticado con respecto a la ficha de ID 106. El número aleatorio puede ser utilizado como clave simétrica para el cifrado de extremo a extremo.

3. Después de que el usuario 102 se haya autenticado con éxito con respecto a la ficha de ID 106, y después de que el sistema informático proveedor de ID 136 se haya autenticado con éxito con respecto a la ficha de ID 106, el sistema informático proveedor de ID 136 obtiene una autorización de lectura para leer uno, varios o la totalidad de los atributos A almacenados en el área de memoria protegida 124. Debido a una orden de lectura correspondiente, que envía el sistema informático proveedor de ID 136 a través de la conexión a la ficha de ID 106, son leídos los atributos A requeridos del área de memoria protegida 124 y cifrados mediante la ejecución de las instrucciones de programa 132. Los atributos A cifrados son transmitidos a través de la conexión al sistema informático proveedor de ID 136 y allí son desencriptados mediante la ejecución de las instrucciones de programa 148. De esta forma el sistema informático proveedor de ID 136 tiene conocimiento de los atributos leídos de la ficha de ID 106.

   Estos atributos A son firmados por el sistema informático proveedor de ID con la ayuda de su certificado 144 y transmitidos al sistema informático de servicio 150 directamente o a través del sistema informático de usuario 100. De este modo, el sistema informático de servicio 150 es informado de los atributos A leídos de la ficha de ID 106. Por la necesidad de la autenticación del usuario 102 con respecto a la ficha de ID 106 y la autenticación del sistema informático proveedor de ID 136 con respecto a la ficha de ID 106 se consigue el ancla de confianza necesaria, de modo que el sistema informático de servicio 150 puede estar seguro de que los atributos del usuario 102 comunicados a él por el sistema informático proveedor de ID 136 son verdaderos y no han sido falsificados.

4. Para la transmisión de al menos un atributo B al sistema informático de servicio 150 se procede de manera análoga, es decir, son ejecutadas las etapas 1 a 3 mencionadas anteriormente con referencia a la ficha de ID 107, estableciéndose para ello la conexión 103. Como resultado, el sistema informático de servicio 150 recibe entonces los atributos A y B de una manera segura y fiable. La autenticación del usuario con respecto a la ficha de ID B puede omitirse, en contraste con la primera realización de las etapas 1-3.

5. Con la ayuda de los atributos A y B, el sistema informático del servicio determina a continuación los datos que deben servir en la ficha de ID B por ejemplo para la actualización o inicialización de uno de los valores de atributo almacenados en la zona protegida 124'. Si la ficha de ID B es asignada, por ejemplo, a un

automóvil 172 y en cuanto al sistema informático de servicio 150 se trata de una oficina de registro de automóviles en línea, el sistema informático de servicio puede determinar la matrícula actual del automóvil 172 accediendo con ayuda de los atributos de A y/o B a una base de datos 174 que está conectada al sistema informático de servicio 150. Esto se puede hacer de manera que mediante la ejecución de las instrucciones del programa 156 con ayuda de los atributos A y/o B es realizada una consulta de base de datos a la base de datos 174 para solicitar la matrícula actual del automóvil allí almacenada. El sistema informático de servicio firma entonces con su clave privada los datos que incluyen la matrícula actual, y envía los datos firmados través de la red 116 al sistema informático proveedor de ID 136. El sistema informático proveedor de ID 136, a continuación, comprueba la validez de la firma. Si la firma es válida, el programa de control 151 comprueba si aún existen las dos conexiones 101 y 103. Si este es el caso, el programa de control 151 escribe entonces los datos recibidos desde el sistema informático de servicio 150 a través de la conexión 103 en la ficha de ID B, por ejemplo, para actualizar el valor del atributo de la matrícula, que está almacenado en el área de memoria protegida 124' de la ficha de ID B.

Dependiendo de la forma realización, la secuencia de la autenticación puede ser diferente. Por ejemplo, puede estar previsto que en primer lugar deba autenticarse el usuario 102 con respecto a la ficha de ID 106 y, posteriormente, el sistema informático proveedor de ID 136. Pero también es posible esencialmente que en primer lugar deba autenticarse el sistema informático proveedor de ID 136 con respecto a la ficha de ID 106 y luego a continuación el usuario 102. Lo mismo se aplica a la ficha de ID 107.

En el primer caso, la ficha de ID 106 o 107 está diseñada, por ejemplo, de modo que solo sea desbloqueada mediante la introducción de un PIN correcto o de una característica biométrica correcta por el usuario 102. Solo este desbloqueo permite el inicio de las instrucciones de programa 132 y 134 y, por tanto, la autenticación del sistema informático proveedor de ID 136.

En el segundo caso es posible también ya un inicio de las instrucciones de programa 132 y 134 cuando el usuario 102 aún no se ha autenticado con respecto a la ficha de ID 106. En este caso, por ejemplo, las instrucciones de programa 134 están realizadas de manera que el sistema informático proveedor de ID 136 puede realizar un acceso de lectura al área de memoria protegida 124 para la lectura de uno o varios de los atributos, solo después de que por las instrucciones de programa 130 haya sido señalada la autenticación con éxito también del usuario 102. Lo mismo se aplica a la ficha de ID 107.

De particular ventaja es la utilización de las fichas de ID 106 y 107 para, por ejemplo, aplicaciones de e-gobierno, y concretamente sin cambio de medios y legalmente segura debido al ancla de confianza constituida por la necesidad de la autenticación del usuario 102 y del sistema informático proveedor de ID 136 con respecto a la ficha de ID 106. De particular ventaja es además que no es necesario un almacenamiento central de los atributos de diferentes usuarios 102, por lo que se resuelven así los problemas de protección de datos existentes en el estado de la técnica. En lo que se refiere a la comodidad de uso del procedimiento, es particularmente ventajoso que no es necesario un registro previo del usuario 102 para la puesta en funcionamiento del sistema informático proveedor de ID 136.

La figura 4 muestra una forma de realización de un procedimiento según la invención. En la etapa 200 es enviada una demanda de servicio desde el sistema informático de usuario al sistema informático de servicio. Por ejemplo, el usuario inicia para ello un navegador de Internet del sistema informático de usuario e introduce una URL para llamar a una página web del sistema informático de servicio. En la página web invocada, el usuario introduce después su demanda de servicio, por ejemplo, para la actualización de su ficha de ID B.

Para esta actualización es necesario por tanto que se establezca, respectivamente, una conexión A o B, tanto entre la ficha de ID A y el proveedor de ID, como entre la ficha de ID B y el proveedor de ID, mediante las cuales el proveedor de ID puede leer atributos de las fichas de ID A y B. En la forma de realización considerada aquí el establecimiento de las conexiones A y B se realiza secuencialmente, estableciendo por ejemplo en primer lugar la conexión A. Para ello, en la etapa 201 la ficha de ID empleada actualmente es igualada a la ficha de ID A.

En la etapa 202, el sistema informático de servicio 150 especifica entonces uno o varios atributos que necesita para comprobar la autorización del usuario para la demanda de servicio. En particular, el sistema informático de servicio puede especificar aquellos atributos que determinan la identidad digital del usuario 102. Esta especificación de los atributos por el sistema informático de servicio 150 puede estar predeterminada fijamente o ser determinada en el caso particular dependiendo de la demanda de servicio por el sistema informático de servicio 150 en base a reglas predefinidas.

En la etapa 204, la especificación de atributo, es decir, la especificación realizada en la etapa 202 de uno o varios de los atributos, es transmitida por el sistema informático de servicio al sistema informático proveedor de ID, y concretamente, o bien directamente o bien a través el sistema informático de usuario.

Para dar al sistema informático proveedor de ID la posibilidad de leer los atributos de su ficha de ID, en la etapa 206 el usuario se autentica con respecto a la ficha de ID.

En la etapa 208 es establecida una conexión entre la ficha de ID y el sistema informático proveedor de ID. En este caso, preferiblemente, se trata de una conexión segura, por ejemplo, según un llamado procedimiento de mensajería segura.

En la etapa 210 se realiza al menos una autenticación del sistema informático proveedor de ID con respecto a la ficha de ID a través de la conexión establecida en la etapa 208. Además puede estar prevista una autenticación también de la ficha de ID con respecto al sistema informático proveedor de ID.

Después de que tanto el usuario como el sistema informático proveedor de ID se hayan autenticado con éxito con respecto a la ficha de ID, el sistema informático proveedor de ID recibe de la ficha de ID la autorización de acceso para la lectura de los atributos. En la etapa 212 el sistema informático proveedor de ID envía una o varias órdenes de lectura para la lectura de los atributos necesarios según la especificación de atributo de la ficha de ID. Los atributos son después transmitidos por medio de un cifrado de extremo a extremo a través de la conexión segura al sistema informático proveedor de ID y allí son desencriptados.

Los valores de atributo leídos son firmados en la etapa 214 por el sistema informático proveedor de ID. En la etapa 216, el sistema informático proveedor de ID envía los valores de atributos firmados a través de la red. Los valores de atributo firmados llegan al sistema informático de servicio, o bien directamente o bien a través del sistema informático de usuario. En este último caso, el usuario puede tener la posibilidad de conocer los valores de atributo firmados y/o completarlos con otros datos. Puede estar previsto que los valores de atributo firmados sean reenviados desde el sistema informático de usuario al sistema informático de servicio eventualmente con los datos completados tras el desbloqueo por el usuario. Con esto se produce la mayor transparencia posible para el usuario en cuanto a los atributos enviados desde el sistema informático proveedor de ID al sistema informático del servicio.

A continuación, en la etapa 218 la ficha de ID procesada actualmente se iguala a la ficha de ID B y el control del proceso vuelve a la etapa 202. Alternativamente también se retrocede a la etapa 206 cuando el sistema informático de servicio en la etapa 202 también ha especificado los atributos B leídos de la ficha de ID B y cuando esta especificación en la etapa 204 ya ha sido transmitida al proveedor de ID y ha sido allí almacenada de forma intermedia. No obstante, preferiblemente, se prescinde de tal almacenamiento intermedio, para poder realizar el proveedor de ID sin estado.

La etapa 206 puede omitirse con respecto a la ficha de ID B.

Después de la ejecución repetida de las etapas 202 a 216 con respecto a la ficha de ID B, el sistema informático de servicio ha recibido, por tanto, los atributos A y B.

En la etapa 220 el sistema informático de servicio determina entonces en base a los atributos A y/o B, los datos para la actualización o inicialización de la ficha de ID B. Esto se puede realizar de manera que el sistema informático de servicio genere estos datos, consulte una base de datos o desbloquee la base de datos para el acceso por el sistema informático proveedor de ID para la lectura de estos datos a través de la red.

En la etapa 220, el sistema informático de servicio envía una señal de desbloqueo para la escritura de los datos en la ficha de ID B al proveedor de ID. A continuación, en la etapa 224 el proveedor de ID lee los datos determinados por el sistema informático en la etapa 220, accediendo el sistema informático proveedor de ID, por ejemplo a través de la red, al sistema informático de servicio. A continuación, el sistema informático proveedor de ID escribe los datos en la etapa 226 en la ficha de ID B a través de la conexión B y de hecho con el prerrequisito de que también siga existiendo la conexión A.

La figura 5 muestra otra forma de realización de un procedimiento de acuerdo con la invención. Por una entrada de usuario de un usuario 102 en un sistema informático de usuario 100, el usuario 102 especifica un servicio de un sistema informático de servicio, que él o ella desea utilizar. Esto se realiza, por ejemplo, llamando a una página de internet del sistema informático de servicio y una selección de uno de los servicios que allí se ofrecen. La demanda de servicio del usuario 102 es transmitida desde el sistema informático de usuario 100 al sistema informático de servicio 150.

Por ejemplo, el sistema informático de servicio 150 incluye un servicio web 176, especialmente según una arquitectura de servicios web especificada W3C. El servicio web 176 sirve como interfaz del sistema informático de servicio 150 con respecto al sistema informático de usuario 100 y/o el sistema informático proveedor de ID 136.

El sistema informático de servicio 150 responde a la demanda de servicio con una especificación de atributo de los atributos A, es decir, por ejemplo una lista de nombres de atributo. Tras la recepción de la especificación de atributo, el sistema informático de usuario 100 requiere al usuario 102 una autenticación con respecto a la ficha de ID 106, por ejemplo, por una petición de entrada.

El usuario 102 se autentica a continuación con respecto a la ficha de ID 106, por ejemplo mediante la introducción de su PIN. Después de la autenticación con éxito, la especificación de atributo es reenviada por el sistema informático de usuario 100 a un sistema informático proveedor de ID 136. Para ello se establece la conexión A. El

sistema informático proveedor de ID 136 se autentica a continuación con respecto a la ficha de ID 106 y dirige una demanda de lectura para la lectura de los atributos de acuerdo con la especificación de atributo a la ficha de ID 106.

Bajo el prerrequisito de la autenticación con éxito previa del usuario 102 y del sistema informático proveedor de ID 136, la ficha de ID 106 responde a la demanda de lectura con los atributos A deseados. El sistema informático proveedor de ID 136 firma los atributos A y envía los atributos firmados al sistema informático de usuario 100. Después del desbloqueo por parte del usuario 102, los atributos firmados son transmitidos después al sistema informático de servicio 150.

La secuencia parcial 178 caracterizada en la figura 5 con las etapas para la transmisión de los atributos A al servicio web 176 es ejecutada otra vez a continuación y, concretamente con respecto a la ficha de ID B, para transmitir al servicio web 176 también los atributos B de acuerdo con la especificación de atributo. Aquí, las etapas para la autenticación del usuario con respecto a la ficha de ID B pueden ser omitidas.

La secuencia parcial 178' prevista para ello puede pues realizarse, por ejemplo, como sigue.

El sistema informático de servicio 150 responde a la recepción de los atributos A con una especificación de atributo de los atributos B, es decir, por ejemplo, una lista de nombres de atributo. La especificación de atributo es reenviada desde el sistema informático de usuario 100 a un sistema informático proveedor de ID 136. Para ello se establece la conexión B. El sistema informático proveedor de ID 136 se autentica a continuación con respecto a la ficha de ID 107 y dirige una demanda de lectura para la lectura de los atributos de acuerdo con la especificación de atributo a la ficha de ID 107.

Bajo el prerrequisito de autenticación con éxito previa del usuario 102 y del sistema informático proveedor de ID 136, la ficha de ID 107 responde a la demanda de lectura con los atributos B deseados. El sistema informático proveedor de ID 136 firma los atributos B, y envía los atributos firmados al sistema informático de usuario 100. Después del desbloqueo por parte del usuario 102, los atributos firmados son transmitidos después al sistema informático del servicio 150.

El servicio web 176, a continuación, reenvía los atributos A y B a un componente 180 del sistema informático de servicio 150, que sirve como proveedor de atributos, es decir, para la determinación de los valores de atributo actualizados o iniciales para la escritura en la ficha de ID B.

Esto se puede realizar de modo que el componente 180 con ayuda de los atributos A y/o B realice una consulta de base de datos a la base de datos 174. Las entradas de base de datos identificadas en la base de datos 174 a través de la consulta de base de datos, que incluyen los datos que se escriben en la ficha de ID B, pueden ser caracterizados por el componente 180 con una denominada bandera. A continuación, desde la base de datos 174 o desde el componente 180 se informa al servicio web 176 de que los datos están preparados. Esta señal es reenviada por el servicio web 176 al sistema informático proveedor de ID 136. El sistema informático proveedor de ID 136 acto seguido lee los datos a través del servicio web 176 de la base de datos 174 y luego escribe los datos en la ficha de ID B con el prerrequisito de que sigan existiendo ambas conexiones A y B hasta la finalización del proceso de escritura.

Para la seguridad de los datos proporcionados por el componente 180 frente a accesos no autorizados puede procederse de manera que por el componente 180 sea generada una clave, que sea enviada junto con la señal "datos listos" al sistema informático proveedor de ID 136. La lectura posterior de los datos por el sistema informático proveedor de ID 136 solo es posible entonces si el sistema informático proveedor de ID 136 tiene esta clave. Por ejemplo, el sistema informático proveedor de ID 136 debe en primer lugar autenticarse con respecto al servicio web con esta clave para poder acceder a los datos.

Alternativa o adicionalmente, la facilitación de datos por el componente 180 puede realizarse solo durante un período limitado. Para ello, el componente 180 inicia un temporizador después de que los datos han sido proporcionados o después de que ha sido enviada la señal "datos listos" al sistema informático proveedor de ID 136. La lectura de los datos por el sistema informático proveedor de ID 136 solo es posible entonces si esta se lleva a cabo antes de que expire el temporizador.

En la forma de realización de la figura 6, el sistema informático de usuario 100 está diseñado como ordenador cliente. En cuanto a la ficha de ID A 106 se trata aquí de una tarjeta de identidad electrónica "ePA". En cuanto a la ficha de ID B 107 se trata de un documento de automóvil electrónico, por ejemplo un permiso de circulación electrónico o un certificado de registro de vehículo electrónico "eKFZ". El servicio web 176 está diseñado aquí como servicio de autorización, es decir, el servicio web ofrece diferentes servicios para el registro o cambio de registro de automóviles en línea. El servicio web 176 y el proveedor de atributos 180 pueden estar conectados a una conexión para la lectura y/o escritura de datos.

Para la actualización de la ficha de ID 107, por ejemplo con una nueva matrícula, se procede como sigue:

1. El usuario 102 invoca por su sistema informático de usuario 100, con ayuda de una demanda de servicio, uno de los servicios disponibles en el servicio web 176.

2. El servicio web 176 responde a esta demanda de servicio con una petición de autenticación, es decir, el servicio web 106 especifica con la ayuda de una especificación de atributo A aquellos atributos que necesita con respecto al usuario 102. Esta petición de autenticación es enviada por el servicio web 176 al sistema informático de usuario 100. Además, el servicio web 176 envía al sistema informático de usuario 100 una información a la que sigue una sesión de múltiples documentos, es decir, una sesión en la que deben existir dos conexiones paralelas a las fichas de ID 106 y 107.

3. Desde el sistema informático de usuario 100 es enviada una petición de confirmación de ID de usuario al proveedor de ID 136. Esta petición incluye la especificación de atributo A, es decir, una especificación de los atributos A que deben ser leídos de la ficha de ID 106. Además, desde el sistema informático de usuario 100 es enviado al sistema informático proveedor de ID 136 la información según la cual debe ser mantenida la conexión A que se establece con la ficha de ID 106, tras la petición de los atributos A de la ficha de ID 106.

4. Entre el sistema informático proveedor de ID 136 y la ficha de ID 106 es establecida a continuación la conexión A y el sistema informático proveedor de ID 136 lee los atributos A de la ficha de ID A. Después de la lectura de los atributos A persiste la conexión A, es decir, la sesión.

5. El sistema informático proveedor de ID 136 envía los atributos A al sistema informático de usuario 100 en respuesta a la petición de la etapa 3.

6. El sistema informático de usuario 100 envía los atributos A al servicio web 176 en respuesta a la petición de autenticación de la etapa 2.

7. El servicio web 176 envía una petición de autenticación relativa a los atributos B al sistema informático de usuario 100, es decir, relativa a aquellos atributos B que están almacenados en la ficha de ID 107. La petición de autenticación incluye pues una especificación de atributo de los atributos B. Además es transmitida una información de que la sesión de múltiples documentos debe ser ampliada, es decir que debe establecerse otra conexión B.

8. El sistema informático de usuario 100 envía una petición de confirmación de ID del automóvil al sistema informático proveedor de ID 136, es decir, una petición para la entrega de los atributos B, así como están especificados en la especificación de atributo B recibida con la petición de autenticación de la etapa 7. Además, es enviada una información según la cual la conexión B que se va a establecer para ello con la ficha de ID 107 debe permanecer después de la lectura de los atributos B.

9. El sistema informático proveedor de ID 136 establece la conexión B con la ficha de ID 107 y lee de ella los atributos B. Después de la lectura de los atributos B persiste la conexión B. Por ejemplo, es realizada una llamada sesión de unión de las conexiones A y B.

10. En respuesta a la petición de la etapa 8, el sistema informático proveedor de ID 136 envía los atributos B al sistema informático de usuario 100.

11. En respuesta a la petición de autenticación de la etapa 7, el sistema informático de usuario 100 envía los atributos B al servicio web 176.

12a. El servicio web 176 envía una señal de desbloqueo para la escritura de datos, como por ejemplo la nueva matrícula, en la ficha de ID 107 al sistema informático de usuario 100.

12b. El servicio web 176 envía una señal de desbloqueo para la lectura de los datos que se van a escribir en la ficha de ID 107 por el proveedor de atributos 180.

13. El sistema informático de usuario 100 envía al sistema informático proveedor de ID 136 una demanda para describir la ficha de ID 107 en base a la señal de desbloqueo recibida en la etapa 12a.

14. El sistema informático proveedor de ID 136 lee de nuevo los atributos A de la ficha de ID 106 a través de la conexión A, ya que estos han sido almacenados de forma intermedia en el sistema informático proveedor de ID 136 después del primer proceso de lectura.

15. El sistema informático proveedor de ID 136 lee del proveedor de atributos 180 los datos para la descripción de la ficha de ID 107, lo que es posible ya que el proveedor de atributos 180 había recibido la señal de desbloqueo para la lectura en la etapa 12b.

16. El sistema informático proveedor de ID 136 genera a partir de los atributos A y los datos leídos desde el proveedor de atributos 180 un conjunto de datos para la escritura en la ficha de ID 107 y escribe este conjunto de datos después a través de la conexión B en la ficha de ID 107.

17. El sistema informático proveedor de ID 136 envía una confirmación al sistema informático de usuario 100, y concretamente como confirmación para la demanda recibida en la etapa 13.

18. El sistema informático de usuario 100 envía al servicio web 176 una confirmación relativa a la señal de desbloqueo de la etapa 12a.

19. El servicio web 176 envía al sistema informático de usuario 100 una confirmación relativa a la demanda de servicio de la etapa 1 para confirmar que la ficha de ID 107 ha sido actualizada con éxito.

De particular ventaja aquí es que el sistema informático proveedor de ID 136 actúa como intermediario entre las diferentes fuentes de datos que están sujetas a diferentes estamentos. Además, es especialmente ventajoso que el sistema informático proveedor de ID 136 constituye el punto de confianza para la unión de las diferentes sesiones.

Lista de símbolos de referencia

100 sistema informático de usuario
101 conexión A
102 usuario
103 conexión B
104 interfaz
106 ficha de ID
107 ficha de ID
108 interfaz
110 procesador
112 instrucciones de programa
114 interfaz de red
116 red
118 memoria electrónica
120 área de memoria protegida
122 área de memoria protegida
124 área de memoria protegida
126 área de memoria
128 procesador
130 instrucciones de programa
131 instrucciones de programa
132 instrucciones de programa
134 instrucciones de programa
136 sistema informático proveedor de ID
138 interfaz de red
140 memoria
142 clave privada

144 certificado

145 procesador

146 instrucciones de programa

147 instrucciones de programa

148 instrucciones de programa

149 instrucciones de programa

150 sistema informático de servicio

151 instrucciones del programa

152 interfaz de red

154 procesador

156 instrucciones de programa

158 conjunto de datos de configuración

160 conjunto de datos de configuración

161 conjunto de datos de configuración

162 entrada de usuario

166 especificación de atributo

168 demanda

170 respuesta

172 automóvil

174 base de datos

176 servicio web

178 secuencia parcial

180 componente

REIVINDICACIONES

1. Procedimiento para el almacenamiento de datos con las siguientes etapas:

- establecimiento de una primera conexión (101) entre una primera ficha de ID (106) y un primer sistema informático (136) a través de un segundo sistema informático (100) para la lectura de al menos un primer atributo de la primera ficha de ID,

- establecimiento de una segunda conexión (103) entre una segunda ficha de ID (107) y el primer sistema informático a través del segundo sistema informático para la lectura de al menos un segundo atributo de la segunda ficha de ID,

- envío de los primeros y segundos atributos por el primer sistema informático a un tercer sistema informático (150),

- recepción de los datos del tercer sistema informático por el primer sistema informático,

- escritura de los datos del primer sistema informático en la segunda ficha de ID a través de la segunda conexión para almacenar los datos en la segunda ficha de ID, siendo un prerrequisito para la escritura de los datos que también siga existiendo la primera conexión,

en el que en cuanto a la primera y segunda conexiones se trata, respectivamente, de conexiones con cifrado de extremo a extremo y con un protocolo orientado a la conexión.

2. Procedimiento según la reivindicación 1, en el que en cuanto a la primera y/o segunda ficha de ID se trata de un documento, en particular un documento de valor o de seguridad.

3. Procedimiento según la reivindicación 1 o 2, en el que en cuanto al protocolo orientado a la conexión se trata de un TCP.

4. Procedimiento según la reivindicación 1, 2 o 3, en el que para el establecimiento de cada una de las primera y segunda conexiones son realizadas, respectivamente, las siguientes etapas:

- autenticación de un usuario (102) con respecto a la ficha de ID en cuestión,

- autenticación del primer sistema informático con respecto a la ficha de ID en cuestión, en el que tras la autenticación con éxito del usuario y del primer sistema informático con respecto a la ficha de ID en cuestión se realiza un acceso de lectura del primer sistema informático hacia el al menos primer o segundo atributos almacenados en la ficha de ID en cuestión para la transmisión, después de su firma, al tercer sistema informático.

5. Procedimiento según la reivindicación 4, en el que la autenticación del primer sistema informático con respecto a la ficha de ID en cuestión es realizada con ayuda de un certificado (144) de primer sistema informático, en el que el certificado contiene una indicación de aquellos atributos almacenados en la ficha de ID en cuestión para los que el primer sistema informático está autorizado para el acceso de lectura,

- en el que en particular la ficha de ID en cuestión comprueba la autorización de lectura del primer sistema informático para el acceso de lectura hacia el al menos el primer o segundo atributo con ayuda del certificado y/o

- en el que en particular el certificado contiene una especificación de los derechos de escritura del primer sistema informático para la escritura de los datos en la segunda ficha de ID, en el que la segunda ficha de ID comprueba la autorización de escritura del primer sistema informático para acceso de escritura para la escritura de los datos con ayuda del certificado.

6. Procedimiento según una de las reivindicaciones anteriores, con las siguientes etapas adicionales:

- firma del al menos primer y segundo atributos leídos de la ficha de ID en cuestión por el primer sistema informático,

- transmisión del sistema informático firmado del primer sistema informático al tercer sistema informático.

7. Procedimiento según una de las reivindicaciones anteriores, con las siguientes etapas adicionales:

- envío de una demanda de servicio del segundo sistema informático al tercer sistema informático,

- especificación de uno o varios atributos por el tercer sistema informático,

- envío de una especificación de atributo del tercer sistema informático al primer sistema informático, en el que se realiza el acceso de lectura del primer sistema informático a la primera o la segunda ficha de ID para leer el uno o varios atributos especificados en la especificación de atributo, en el que en particular la demanda de servicio contiene un identificador para la identificación del primer sistema informático para seleccionar el primer sistema informático para el establecimiento de la primera y segunda conexiones y la escritura de los datos.

8. Procedimiento según una de las reivindicaciones anteriores, en el que el al menos primer o segundo atributos leídos por el primer sistema informático de la ficha de ID en cuestión es enviado al segundo sistema informático, desde donde es reenviado al tercer sistema informático después del desbloqueo por el usuario, en el que en particular el usuario puede completar con otros datos el al menos primer o segundo atributo antes del reenvío al tercer sistema informático.

9. Procedimiento según una de las reivindicaciones anteriores, en el que el primer sistema informático antes de escribir los datos accede de nuevo a la primera ficha de ID a través de la primera conexión para leer de nuevo el primer atributo, y en el que el primer sistema informático a partir del primer atributo y de los datos recibidos por el tercer sistema informático genera los datos de escritura, que después son escritos por el primer sistema informático en la segunda ficha de ID.

10. Procedimiento según una de las reivindicaciones anteriores, en el que la primera ficha de ID es asignada a un usuario y en el que la segunda ficha de ID es asignada a un objeto, en particular a un automóvil, en el que segundo atributo identifica al objeto de forma única.

11. Producto de programa informático con instrucciones ejecutables por un sistema informático para la realización de un procedimiento según una de las reivindicaciones anteriores.

12. Ficha de ID con:

- un área de memoria protegida (124') para el almacenamiento de al menos un atributo y para el almacenamiento de datos de un sistema informático de servicio (150), en el que para el almacenamiento de los datos debe existir una primera conexión entre un primer sistema informático (136) y una primera ficha de ID (106) y un primer atributo ha sido leído de la primera ficha de ID;

- medios (134) para la autenticación del primer sistema informático (136) con respecto a la ficha de ID, medios (131') para el establecimiento de una segunda conexión (103) entre la ficha de ID y el primer sistema informático según un protocolo orientado a la conexión, a través del cual el primer sistema informático puede leer al menos un segundo atributo, en el que un prerrequisito necesario para la lectura del al menos un atributo de la ficha de ID por el primer sistema informático es la autenticación con éxito del primer sistema informático con respecto a la ficha de ID, y en el que los datos pueden ser escritos en el área de memoria a través de la segunda conexión, en el que el prerrequisito para la escritura de los datos es que siga existiendo la primera conexión, y en el que en particular en cuanto al protocolo orientado a la conexión se trata de un TCP, y en el que en cuanto a la ficha de ID se trata en particular de un documento, en particular un documento de valor o de seguridad.

13. Sistema informático con:

- medios (138, 147) para el establecimiento de una primera conexión (101) entre una primera ficha de ID (106) para la lectura de al menos un primer atributo de la primera ficha de ID a través de un segundo sistema informático (100),

- medios (138, 147) para el establecimiento de una segunda conexión (103) entre una segunda ficha de ID (107) para la lectura de al menos un segundo atributo de la segunda ficha de ID a través del segundo sistema informático,

- medios (138, 147) para el envío de los primeros y segundos atributos del primer sistema informático a un tercer sistema informático (150),

- medios (138) para la recepción de los datos del tercer sistema informático,

- medios (138, 147, 151) para la escritura de los datos del primer sistema informático en la segunda ficha de ID a través de la segunda conexión, para almacenar los datos en la segunda ficha de ID, en el que un prerrequisito para la escritura de los datos es que también siga existiendo la primera conexión, en el que en cuanto a la primera y segunda conexiones se trata, respectivamente, de conexiones con cifrado de extremo a extremo y con un protocolo orientado a la conexión.

14. Sistema informático según la reivindicación 13 con:

- medios (138) para la recepción de una especificación de atributo a través de una red (116), en el que la especificación de atributo especifica al menos un primer y/o segundo atributos,

- medios (142, 144, 146) para la autenticación con respecto a la primera y segunda ficha de ID, en el que la lectura del primer o segundo atributos presupone que un usuario ha sido autenticado al menos con respecto a la primera ficha de ID y el sistema informático ha sido autenticado con respecto a la primera y segunda ficha de ID.

15. Sistema informático según la reivindicación 13 o 14, en el que los medios para el establecimiento de la primera y segunda conexiones están realizados de manera que pueden mantenerse simultáneamente la primera y segunda conexiones.

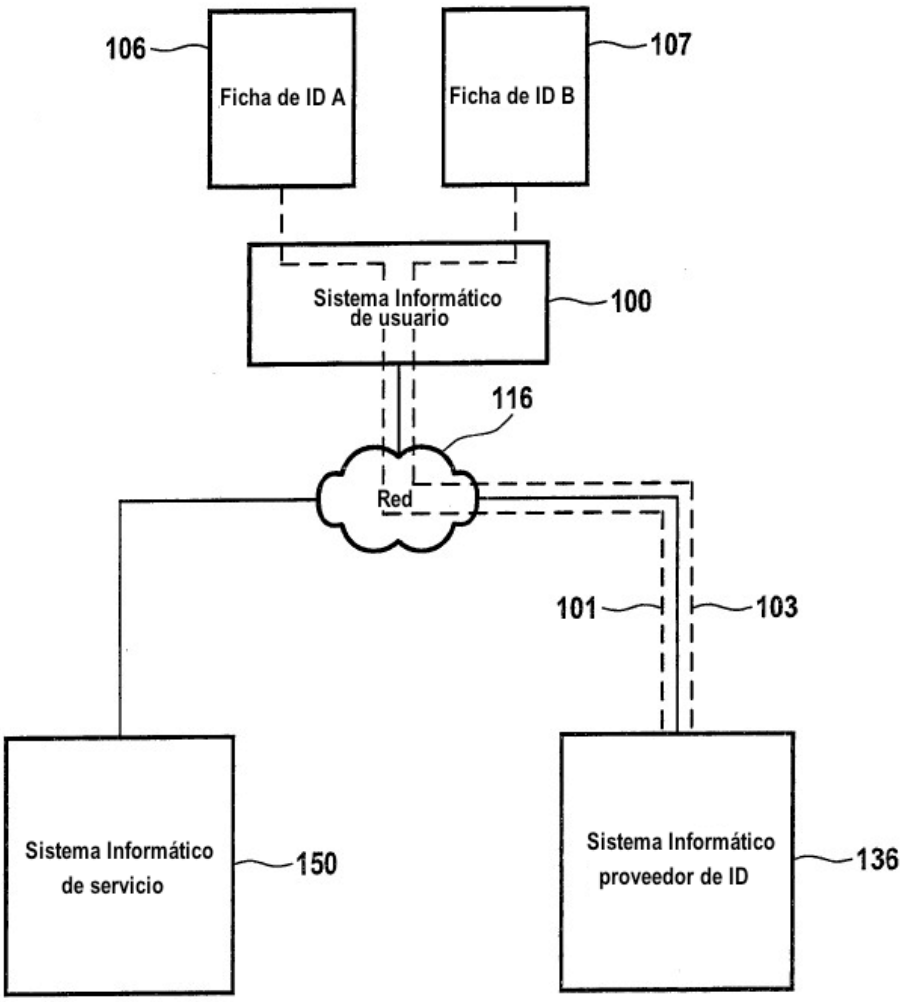
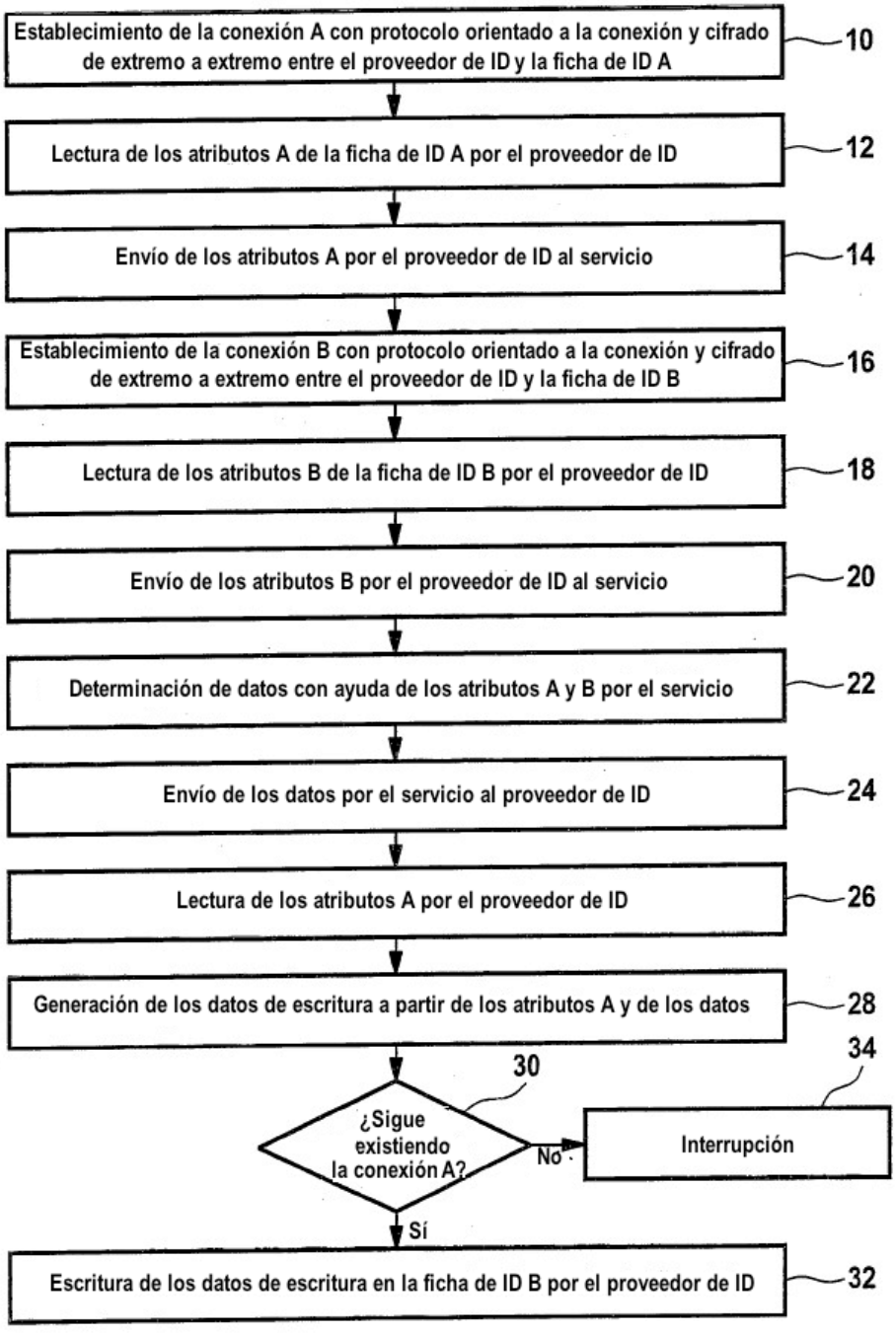
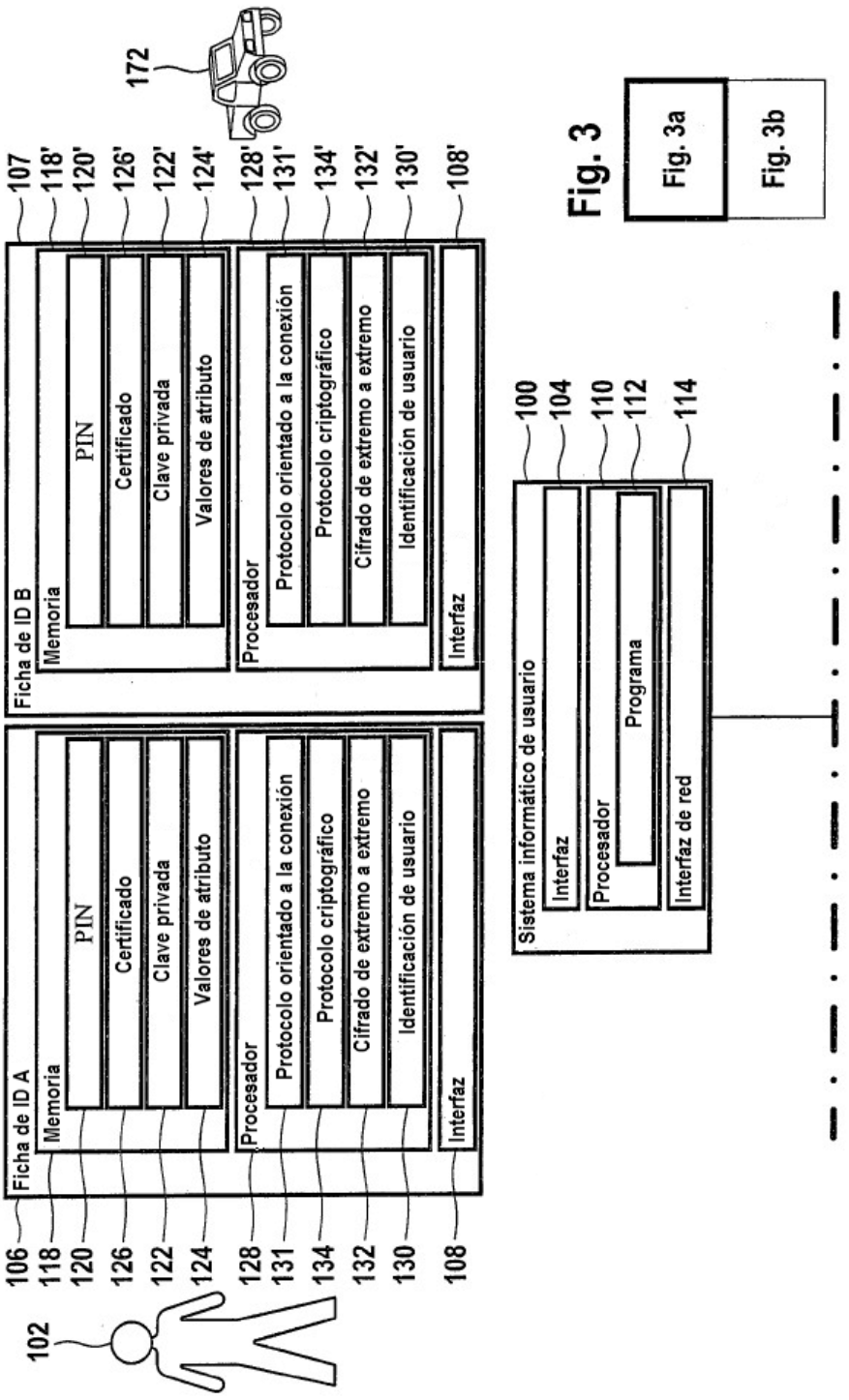

106
Ficha de ID A
Ficha de ID B
107
Sistema Informático de usuario
100
116
Red
101
103
Sistema Informático de servicio
150
Sistema Informático proveedor de ID
136

Fig. 1

Fig. 2


Establecimiento de la conexión A con protocolo orientado a la conexión y cifrado de extremo a extremo entre el proveedor de ID y la ficha de ID A
10
Lectura de los atributos A de la ficha de ID A por el proveedor de ID
12
Envío de los atributos A por el proveedor de ID al servicio
14
Establecimiento de la conexión B con protocolo orientado a la conexión y cifrado de extremo a extremo entre el proveedor de ID y la ficha de ID B
16
Lectura de los atributos B de la ficha de ID B por el proveedor de ID
18
Envío de los atributos B por el proveedor de ID al servicio
20
Determinación de datos con ayuda de los atributos A y B por el servicio
22
Envío de los datos por el servicio al proveedor de ID
24
Lectura de los atributos A por el proveedor de ID
26
Generación de los datos de escritura a partir de los atributos A y de los datos
28
30
¿Sigue existiendo la conexión A?
No
34
Interrupción
Sí
Escritura de los datos de escritura en la ficha de ID B por el proveedor de ID
32


172
107
118'
120'
126'
122'
124'
128'
131'
134'
132'
130'
108'
Ficha de ID B
Memoria
PIN
Certificado
Clave privada
Valores de atributo
Procesador
Protocolo orientado a la conexión
Protocolo criptográfico
Cifrado de extremo a extremo
Identificación de usuario
Interfaz
Ficha de ID A
Memoria
PIN
Certificado
Clave privada
Valores de atributo
Procesador
Protocolo orientado a la conexión
Protocolo criptográfico
Cifrado de extremo a extremo
Identificación de usuario
Interfaz
106
118
120
126
122
124
128
131
134
132
130
108
102
100
104
110
112
114
Sistema informático de usuario
Interfaz
Procesador
Programa
Interfaz de red
Fig. 3
Fig. 3a
Fig. 3b

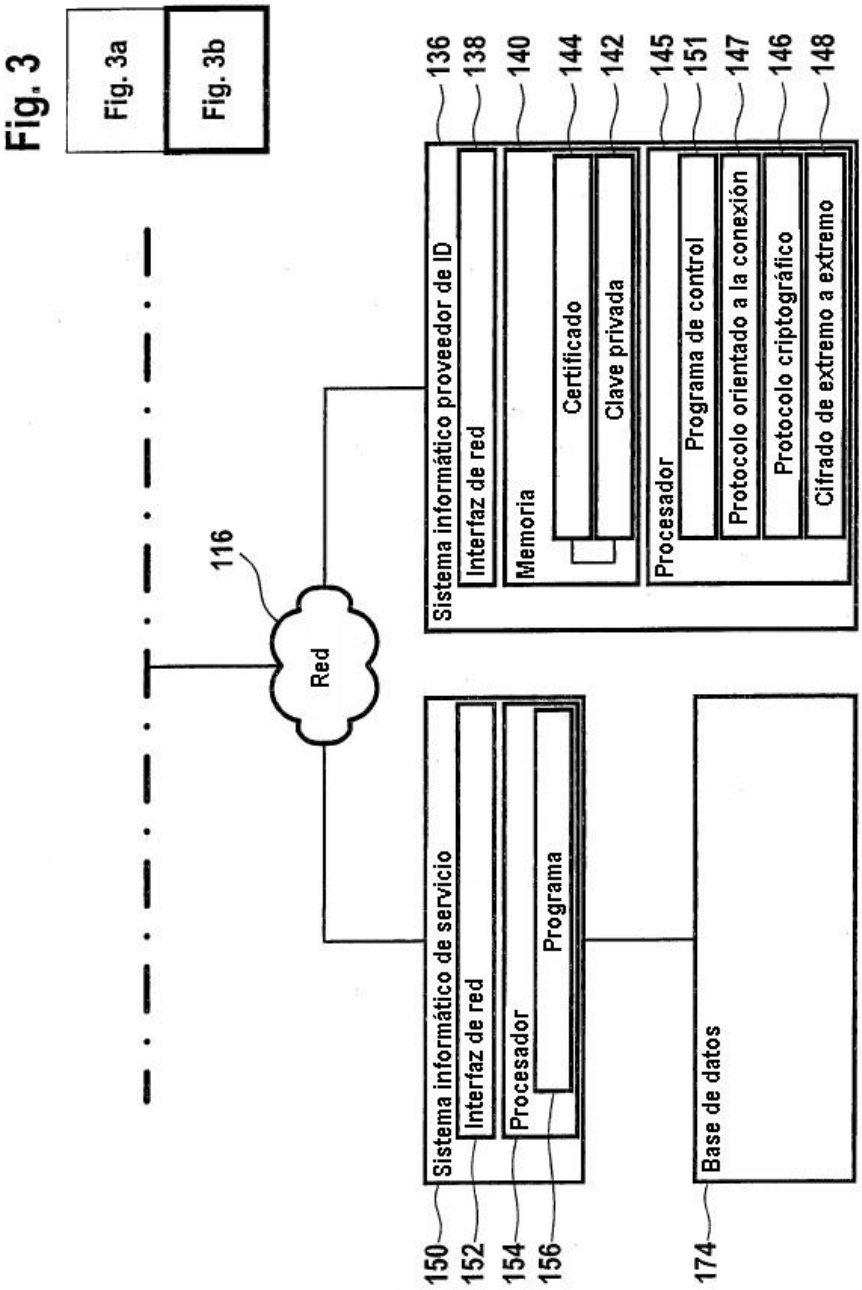


Fig. 3
Fig. 3a
Fig. 3b
116
Red
Sistema informático proveedor de ID
Interfaz de red
Memoria
Certificado
Clave privada
Procesador
Programa de control
Protocolo orientado a la conexión
Protocolo criptográfico
Cifrado de extremo a extremo
136
138
140
144
142
145
151
147
146
148
Sistema informático de servicio
Interfaz de red
Procesador
Programa
Base de datos
150
152
154
156
174

Fig. 4

Fig. 4a Fig. 4b

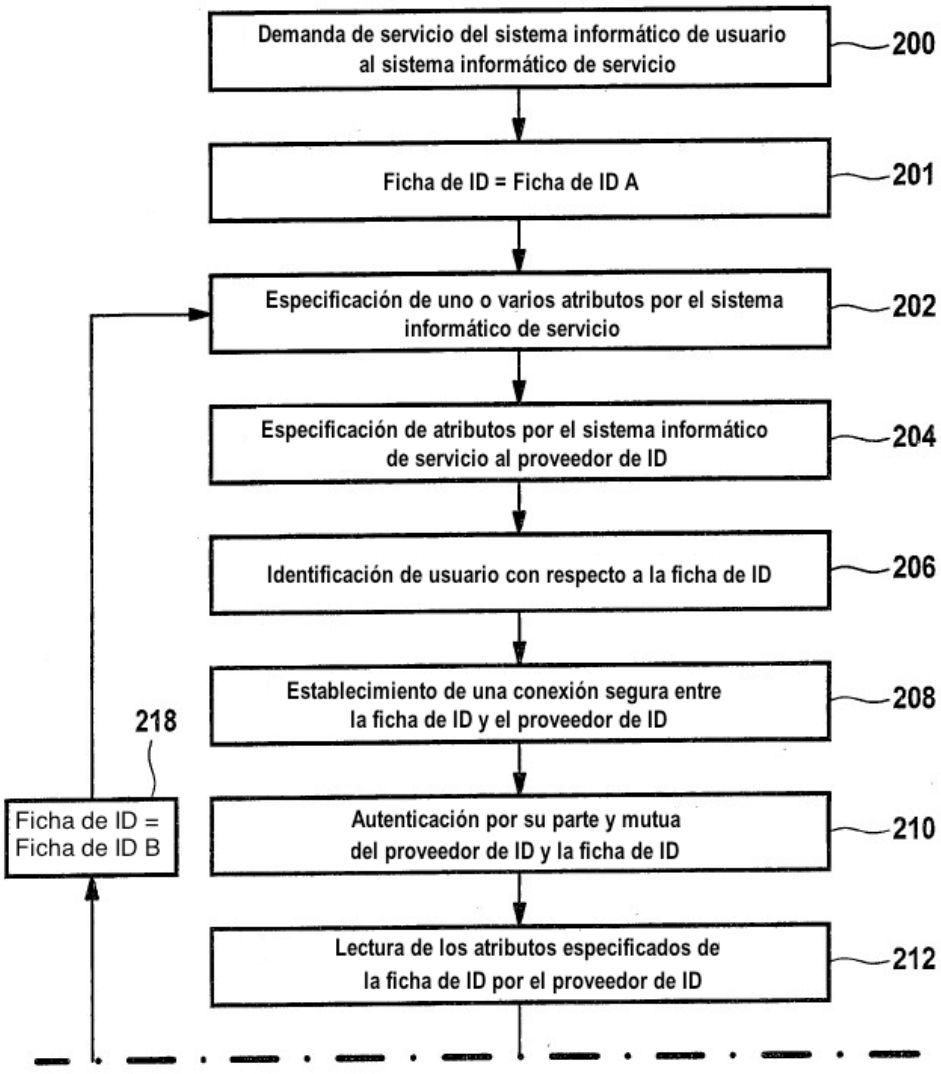
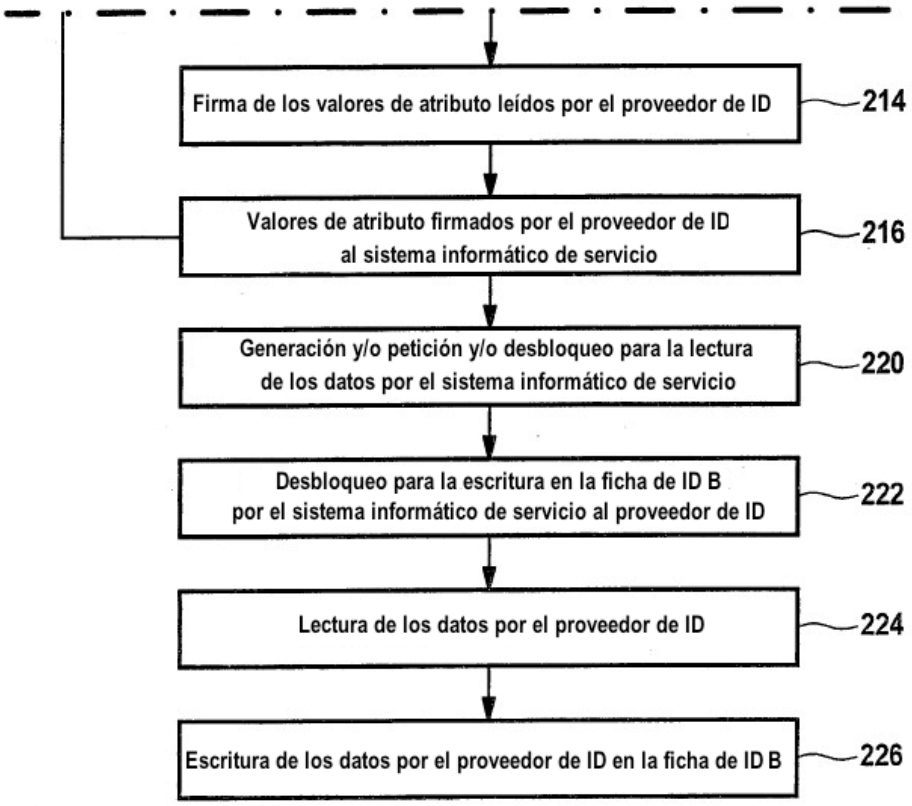


Fig. 4

Fig. 4a | Fig. 4b



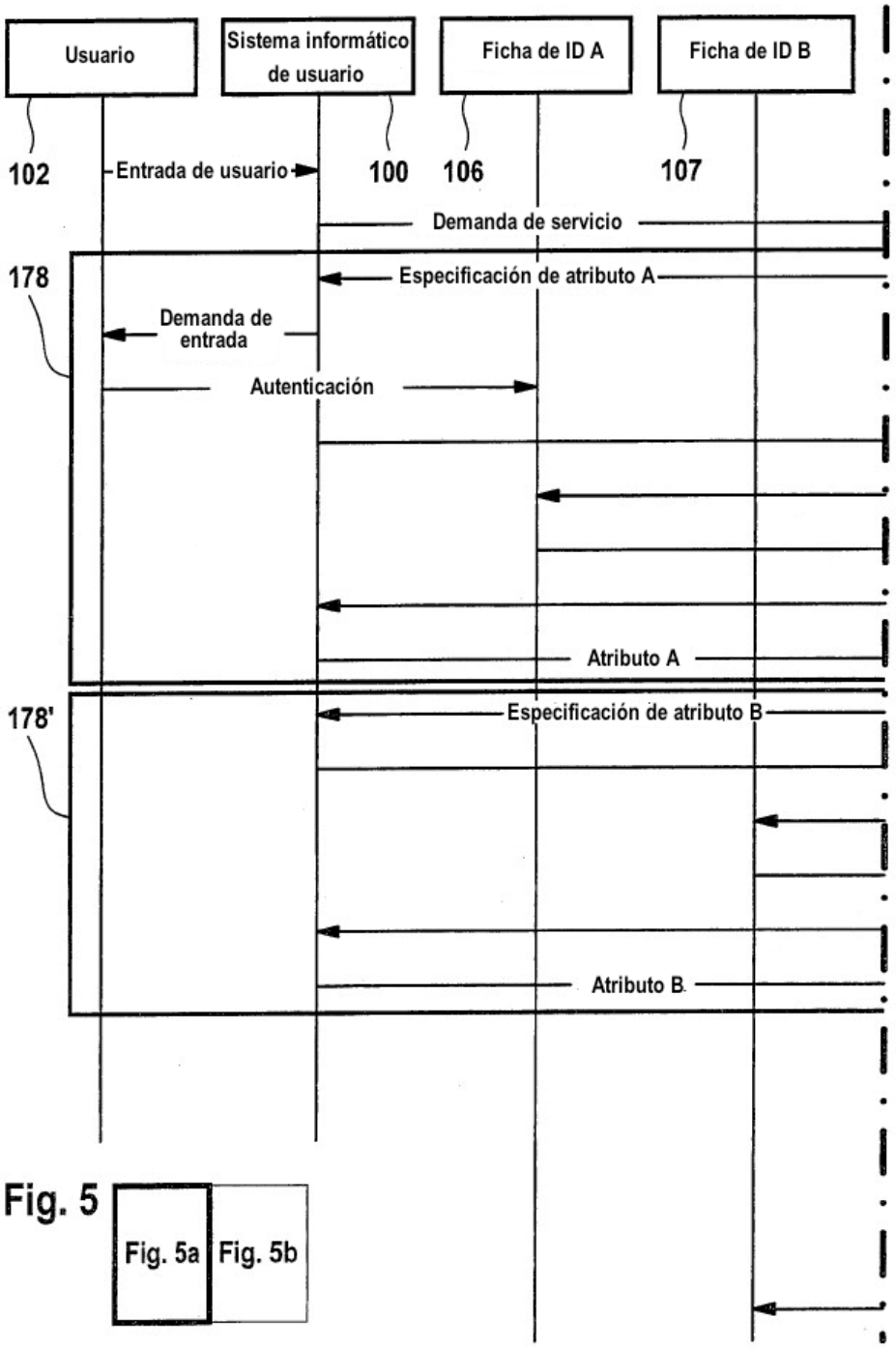

Usuario
Sistema informático de usuario
Ficha de ID A
Ficha de ID B
102
Entrada de usuario
100
106
107
Demanda de servicio
178
Especificación de atributo A
Demanda de entrada
Autenticación
Atributo A
178'
Especificación de atributo B
Atributo B

Fig. 5

Fig. 5a
Fig. 5b

Fig. 5

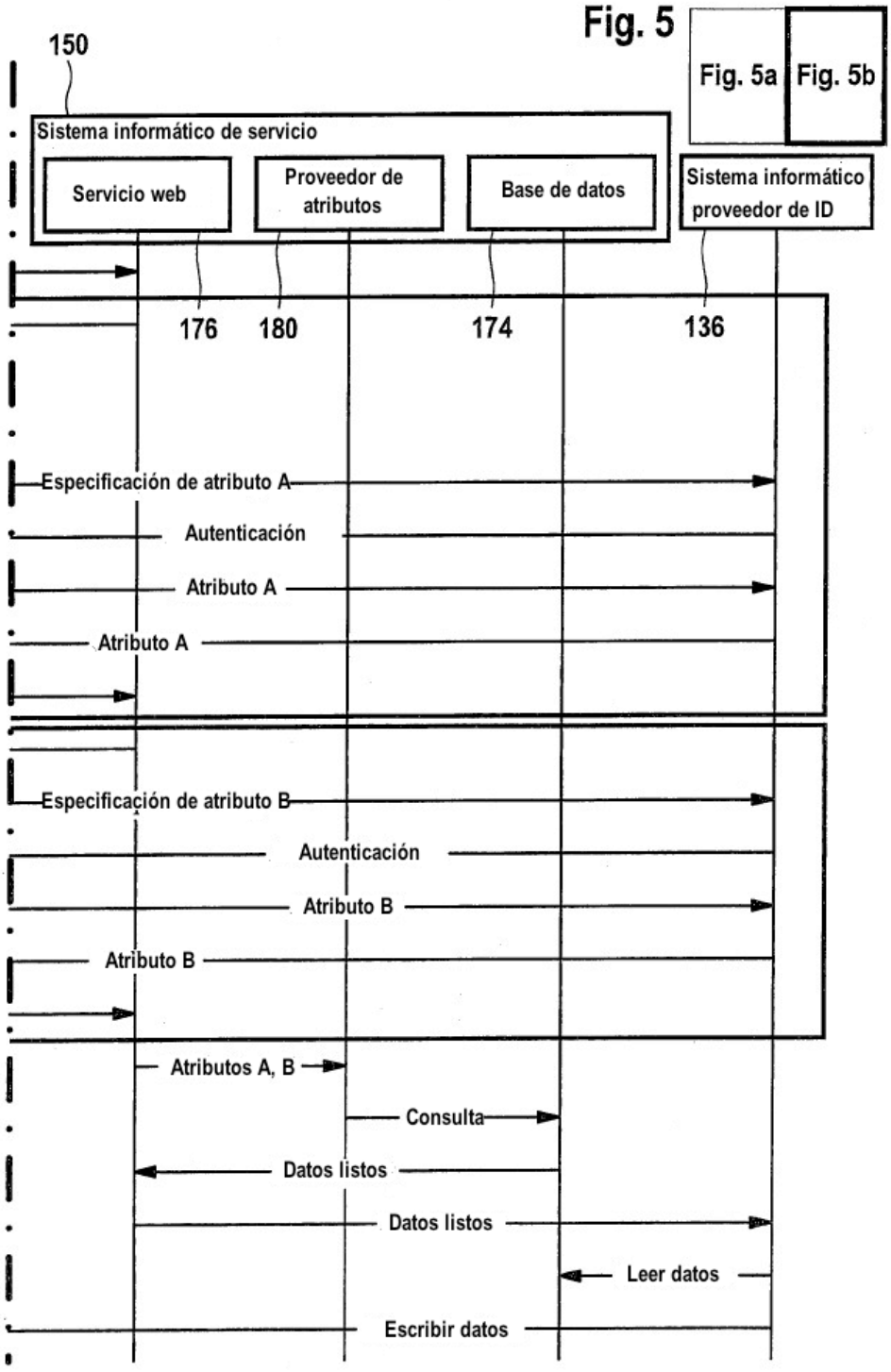


Fig. 5a
Fig. 5b
150
Sistema informático de servicio
Servicio web
Proveedor de atributos
Base de datos
Sistema informático proveedor de ID
176
180
174
136
Especificación de atributo A
Autenticación
Atributo A
Atributo A
Especificación de atributo B
Autenticación
Atributo B
Atributo B
Atributos A, B
Consulta
Datos listos
Datos listos
Leer datos
Escribir datos

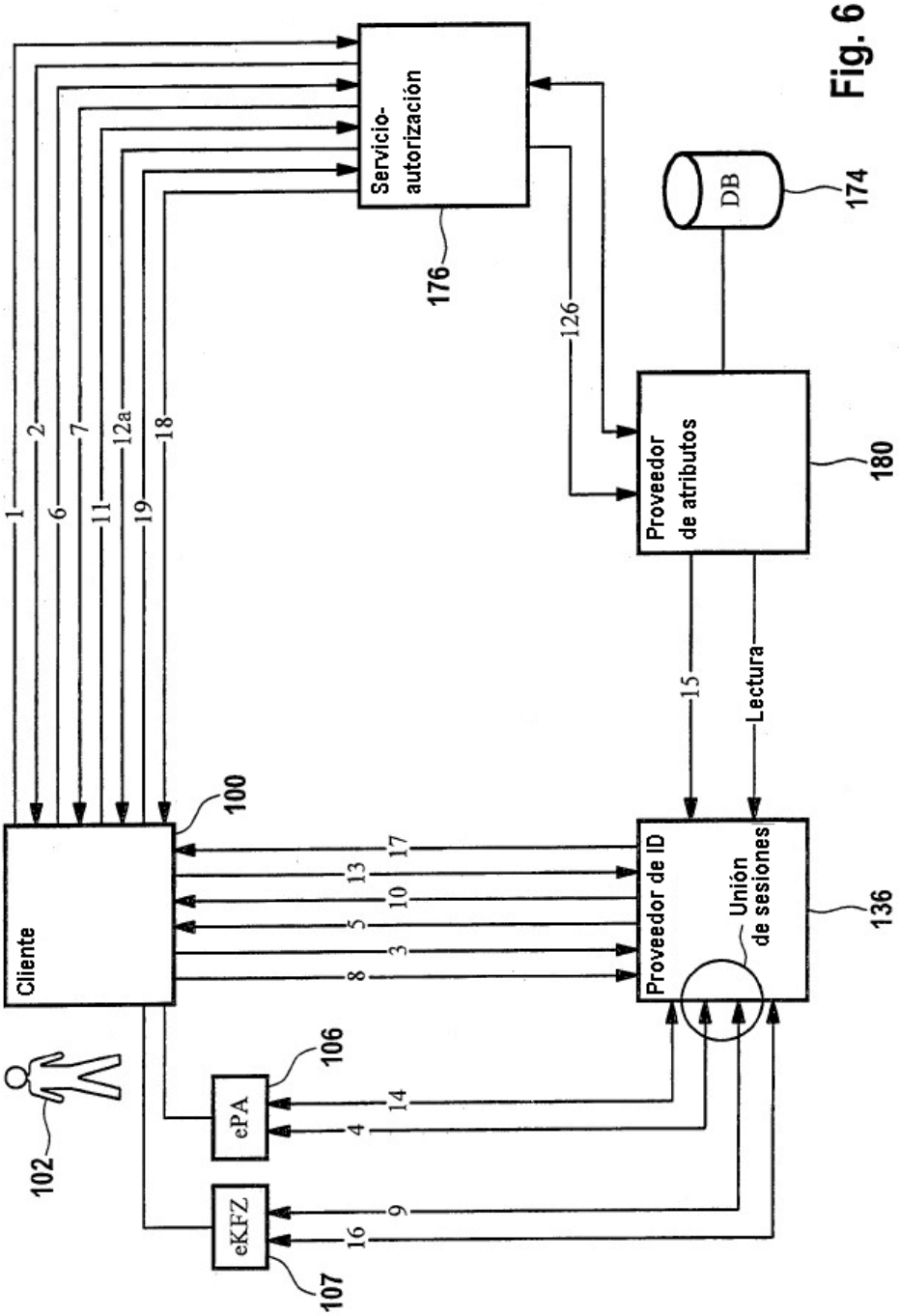

Servicio-autorización
176
DB
174
126
Proveedor de atributos
180
1
2
6
7
11
12a
19
18
15
Lectura
100
Cliente
17
13
10
5
3
8
Proveedor de ID
Unión de sesiones
136
102
106
ePA
14
4
eKFZ
9
16
107

Fig. 6