(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 589 050**

(51) Int. CI.:

G06F 21/31	(2013.01)	***G06Q 20/34***	(2012.01)
G06F 21/34	(2013.01)		
G06F 21/43	(2013.01)		
H04L 29/06	(2006.01)		
H04L 9/32	(2006.01)		
G07F 7/10	(2006.01)		
G06F 21/33	(2013.01)		
G06F 21/35	(2013.01)		
G06F 21/44	(2013.01)		
G06Q 20/40	(2012.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.11.2008 PCT/EP2008/065470**

(87) Fecha y número de publicación internacional: **23.07.2009 WO09089943**

(96) Fecha de presentación y número de la solicitud europea: **13.11.2008 E 08870896 (1)**

(97) Fecha y número de publicación de la concesión europea: **27.07.2016 EP 2245573**

(54) Título: **Procedimiento para leer atributos de un testigo de ID**

(30) Prioridad:

16.01.2008 DE 102008000067

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.11.2016

(73) Titular/es:

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

(72) Inventor/es:

DIETRICH, FRANK;
BYSZIO, FRANK y
PAESCHKE, MANFRED

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento para leer atributos de un testigo de ID

La invención concierne a un procedimiento para leer al menos un atributo de un testigo de ID, a un producto de programa informático, a un testigo de ID y a un sistema informático.

Se conocen por el estado de la técnica diferentes procedimientos para la administración de la llamada identidad digital de un usuario:

Microsoft Windows CardSpace es un sistema de identidad digital basado en el cliente que debe hacer posible que los usuarios de internet comuniquen su identidad digital con respecto a servicios online. En este caso, es desventajoso, entre otras cosas, que el usuario pueda manipular su identidad digital.

Por el contrario, el OPENID en un sistema basado en servidor. Un denominado servidor de identidad almacena un banco de datos con las identidades digitales de los usuarios registrados. Entre otras cosas, es desventajosa aquí una protección de datos insuficiente, dado que los datos de identidad digitales de los usuarios se almacenan de manera centralizada y se puede registrar y el comportamiento de los usuarios.

Por el documento US 2007/0294431A1 se conoce un procedimiento adicional para la administración de las identidades digitales que requiere también una operación de registro de usuario.

Por el documento US 2001/0045451 A1 se conoce un procedimiento para realizar una autentificación basada en testigo. En este caso, se lee una ID lógica de una tarjeta inteligente por un navegador del PC del usuario y a continuación se la transmite por medio de una conexión SSL, a través de una red, a un servidor de acceso.

Por el contrario, la invención se basa en el problema de crear un procedimiento mejorado para leer al menos un atributo, así como un producto de programa informático correspondiente, un testigo de ID y un sistema informático.

Los problemas en los que se basa la invención se resuelven respectivamente con las características de las reivindicaciones independientes. Formas de realización de la invención se implican en las reivindicaciones subordinadas.

Según la invención, se crea un procedimiento para leer al menos un atributo almacenado en un testigo de ID, en el que el testigo de ID está asociado a un usuario. El procedimiento contiene las siguientes etapas: autentificar al usuario con respecto al testigo de ID; autentificar un primer sistema informático con respecto al testigo de ID; tras la autentificación exitosa del usuario y del primer sistema informático con respecto al testigo de ID, hacer que el primer sistema informático acceda a la lectura del al menos un atributo almacenado en el testigo de ID para la transmisión del al menos un atributo a un segundo sistema informático. Por tanto, puede crearse un “anclaje de confianza”.

La invención hace posible la lectura de uno o varios de los atributos almacenados en un testigo de ID por el primer sistema informático, pudiendo establecerse la conexión entre el testigo de ID y el primer sistema informático a través de una red, en particular internet. El al menos un atributo puede ser una indicación con respecto a la identidad del usuario asociado al testigo de ID, en particular con respecto a su denominada identidad digital. Por ejemplo, a través del sistema informático se leen los atributos nombre, apellido, dirección para reenviar estos atributos a un segundo sistema informático, por ejemplo de un servicio en línea.

No obstante, puede también leerse, por ejemplo, solamente un atributo individual que no sirva para la determinación de la identidad del usuario, sino, por ejemplo, para la comprobación de la autorización del usuario a la utilización de un determinado servicio online, tal como, por ejemplo, la edad del usuario, cuando éste quiera utilizar un servicio online que está reservado a un determinado grupo de edad, u otro atributo que documente la pertenencia del usuario a un determinado grupo que esté autorizado para el uso del servicio online.

El testigo de ID puede ser un aparato electrónico portátil, tal como, por ejemplo, un denominado lápiz USB, o un documento, en particular un documento de valor o de seguridad.

Por “documento” se entienden según la invención documentos basados en papel y/o en plástico, como, por ejemplo, documentos de identificación, en particular pasaportes, carnés de identidad, visados así como carnés de conducir, permisos de circulación, documentación del vehículo, tarjetas de identidad de empresas, tarjetas sanitarias u otros documentos de ID, así como tarjetas con chip, medios de pago, en particular tarjetas bancarias y tarjetas de crédito, pólizas de carga u otros comprobantes de autorización en los que esté integrada una memoria de datos para almacenar el al menos un atributo.

Por tanto, algunas formas de realización de la invención son especialmente ventajosas debido a que el al menos un atributo se lee de un documento especialmente fiable, por ejemplo un documento oficial. Además, es especialmente ventajoso que no sea necesario un almacenamiento centralizado de los atributos. Por tanto, la invención hace posible un grado de fiabilidad especialmente alto con respecto a la comunicación de los atributos correspondientes a una identidad digital, ligado a una protección óptima de los datos junto con un manejo extremadamente cómodo.

Según una forma de realización de la invención, el primer sistema informático tiene al menos un certificado que se utiliza para autentificar el primer sistema informático con respecto al testigo de ID. El certificado contiene una indicación de aquellos atributos para los que el primer sistema informático tiene una autorización de lectura. El testigo de ID comprueba, con ayuda de este certificado, si el primer sistema informático tiene la autorización de lectura necesaria para el acceso a la lectura del atributo antes de que pueda realizarse un acceso de lectura a través del primer sistema informático.

Según una forma de realización de la invención, el primer sistema informático envía el al menos un atributo leído por el testigo de ID directamente a un segundo sistema informático. El segundo sistema informático puede ser, por ejemplo, un servidor para proporcionar un servicio online u otro servicio, como, por ejemplo, un servicio bancario, o para pedir un producto. Por ejemplo, el usuario puede abrir una cuenta online, para lo cual se transmiten atributos que contienen la identidad del usuario, desde el primer sistema informático hasta el segundo sistema informático de un banco.

Según una forma de realización de la invención, la transmisión de los atributos leídos del testigo de ID por el primer sistema informático se realiza en primer lugar hacia un tercer sistema informático del usuario. Por ejemplo, el tercer sistema informático tiene un navegador de internet usual con el que el usuario puede abrir una página web del segundo sistema informático. El usuario puede introducir en la página web una solicitud o pedido de un servicio o de un producto.

Seguidamente, el segundo sistema informático especifica aquellos atributos, por ejemplo del usuario o de su testigo de ID, que él necesita para la provisión del servicio o la aceptación del pedido. La especificación de atributo correspondiente, que contiene la especificación de estos atributos, se envía a continuación desde el segundo sistema informático al primer sistema informático. Esto puede realizarse con o sin intercalación del tercer sistema informático. En el último caso, el usuario puede especificar el primer sistema información deseado con respecto al segundo sistema informático, por ejemplo por la introducción de la URL del primer sistema informático en una página web del segundo sistema informático por el tercer sistema informático.

Según una forma de realización de la invención, la solicitud de servicio del usuario al segundo sistema informático contiene la indicación de un identificador, en donde el identificador identifica el primer sistema informático. Por ejemplo, el identificador es un enlace, por ejemplo una URL del primer sistema informático.

Según una forma de realización de la invención, la especificación de atributo no se envía directamente desde el segundo sistema informático hasta el primer sistema informático, sino primero desde el segundo sistema informático hasta el tercer sistema informático. El tercer sistema informático tiene varios conjuntos de datos de configuración predefinidos, en donde el tercer ordenador presenta varios conjuntos de datos de configuración predefinidos, en donde cada uno de los conjuntos de datos de configuración especifica una cantidad parcial de los atributos, al menos una fuente de datos y un primer sistema informático de una cantidad de primeros sistemas informáticos, en donde la especificación de atributo se transmite primero del el segundo sistema informático al tercer sistema informático, de modo que, por medio del tercer sistema informático, se elija al menos uno de los grupos de datos de configuración que especifica una cantidad parcial de los atributos que contiene el al menos un atributo especificado en la especificación de atributo, y en donde el tercer ordenador reenvía la especificación de atributo al primer sistema informático, y se establece la conexión con el testigo de ID especificado por la indicación de la fuente de datos en el conjunto de datos de configuración seleccionado.

Según una forma de realización de la invención, el primer sistema informático firma los atributos leídos del testigo de ID y éstos se transmiten entonces al tercer sistema informático. Por tanto, el usuario el tercer sistema informático puede leer los atributos sin que, no obstante, estos puedan modificarse. Solamente después de la liberación por el usuario, los atributos se reenvían del tercer sistema informático al segundo sistema informático.

Según una forma de realización de la invención, el usuario puede complementar los atributos con datos adicionales antes de su reenvío.

Según una forma de realización de la invención, el primer sistema informático tiene varios certificados con diferentes derechos de lectura. Debido a la recepción de la especificación de atributo, el primer sistema informático selecciona uno o varios de estos certificados para leer los atributos correspondientes del testigo de ID o de varios testigos de ID diferentes.

Según una forma de realización de la invención, el tercer sistema informático tiene al menos un conjunto de datos de configuración que especifica una fuente de datos externa para la consulta de un atributo adicional por el tercer sistema informático a través de la red.

Según una forma de realización de la invención, la consulta del atributo adicional se realiza después de que se haya leído el al menos un atributo del testigo de ID, y después de que el tercer sistema informático haya recibido el al menos un atributo del primer sistema informático, conteniendo la consulta el al menos un atributo.

En otro aspecto, la invención concierne a un producto de programa informático, en particular un medio de memoria digital, con instrucciones de programa ejecutables para realizar un procedimiento según la invención.

En otro aspecto, la invención concierne a un testigo de ID con una zona de almacenamiento protegida para almacenar al menos un atributo, con medios para autentificar a un usuario asociado al testigo de ID con respecto al testigo de ID, medios para autentificar un primer sistema informático con respecto al testigo de ID, medios para establecer una conexión protegida con el primer sistema informático, a través de la cual el primer sistema informático puede leer el al menos un atributo, en donde una condición necesaria para la lectura del al menos un atributo del testigo de ID por el primer sistema informático es la autentificación exitosa del usuario y del primer sistema informático con respecto al testigo de ID.

Por tanto, además de la autentificación del primer sistema informático con respecto al testigo de ID, tal como la que es en sí conocida, por ejemplo, como el denominado Control de Acceso Extendido para documentos de viaje legibles por máquina (machine-readable travel documents – MRTD) y se ha especificado por la Organización Internacional de Aviación Civil ICAO, debe autentificarse el usuario con respecto al testigo de ID. Por ejemplo, gracias a una autentificación exitosa del usuario con respecto al testigo de ID, se activa éste, de modo que pueden concluirse las etapas adicionales, concretamente la autentificación del primer sistema informático con respecto al testigo de ID y/o el establecimiento de una conexión protegida para leer los atributos.

Según una forma de realización de la invención, el testigo de ID tiene medios para una encriptación de extremo a extremo. Esto hace posible establecer la conexión entre el testigo de ID y el primer sistema informático a través de un tercer sistema informático del usuario, dado que el usuario, debido a la encriptación de extremo a extremo, no puede realizar ninguna modificación de los datos transmitidos por la conexión.

En otro aspecto, la invención concierne a un primer sistema informático con sistema informático con medios para recibir una especificación de atributo a través de una red, en donde la especificación de atributo especifica al menos un atributo, medios de autentificación con respecto a un testigo de ID, medios para leer al menos un atributo del testigo de ID por medio de una conexión segura, en donde la lectura del al menos un atributo implica que se ha autentificado un usuario asociado al testigo de ID con respecto al testigo de ID.

Según una forma de realización de la invención, el primer sistema informático puede contener medios para generar un requerimiento al usuario. Después de que el primer sistema informático haya recibido la especificación de atributo, por ejemplo del segundo sistema informático, envía a continuación un requerimiento al tercer sistema informático del usuario, de modo que se requiera al usuario para que se autentifique con respecto al testigo de ID. Después de que se haya realizado con éxito la autentificación del usuario con respecto al testigo de ID, el primer sistema informático recibe una confirmación del tercer sistema informático. A continuación, el primer sistema informático se autentifica con respecto al testigo de ID y se establece una conexión segura entre el testigo de ID y el primer sistema informático con una encriptación de extremo a extremo.

Según una forma de realización de la invención, el primer sistema informático tiene varios certificados que especifican respectivamente diferentes derechos de lectura. Tras la recepción de la especificación de atributo, el primer sistema informático elige al menos uno de estos certificados con los derechos de lectura suficientes para leer los atributos especificados.

Algunas formas de realización del primer sistema informático según la invención son especialmente ventajosas debido a que, en combinación con la necesidad de la autentificación del usuario con respecto al testigo de ID, éstas forman un anclaje de confianza para la identidad digital auténtica del usuario. En este caso, es especialmente ventajoso que esto no requiera ningún registro previo del usuario con respecto al sistema informático ni tampoco un almacenamiento centralizado de los atributos de los usuarios que forman las identidades digitales.

Según una forma de realización de la invención, el primer sistema informático, junto con la especificación de atributo, recibe un identificador del segundo sistema informático. Con ayuda del identificador, el sistema informático identifica el segundo sistema informático que querría emplear el servicio de identificación para facturar este servicio con respecto al segundo sistema informático.

Según una forma de realización, el sistema informático es un centro de confianza oficialmente certificado, en particular un centro de confianza conforme con la ley de firma.

En lo que sigue se explican con más detalle formas de realización de la invención con referencia a los dibujos. Muestran:

La figura 1, un diagrama de bloques de una primera forma de realización de sistemas informáticos según la invención,

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

La figura 3, un diagrama de bloques de formas de realización adicionales de sistemas informáticos según la invención, y

La figura 4, un diagrama de UML de otra forma de realización de un procedimiento según la invención.

Los elementos de las siguientes formas de realización que corresponden uno a otro se indican con los mismos símbolos de referencia.

La figura 1 muestra un sistema informático 100 de un usuario 102. El sistema informático de usuario 100 puede ser un ordenador personal, un ordenador portátil, como, por ejemplo, un Laptop o un ordenador Palmtop, un asistente digital personal, un aparato de telecomunicaciones móviles, en particular un teléfono inteligente, o similares. El sistema informático de usuario 100 tiene una interfaz 104 para la comunicación con un testigo de ID 106 que presenta una interfaz correspondiente 108.

El sistema informático de usuario 100 tiene al menos un procesador 110 para ejecutar instrucciones de programa 112, así como una interfaz de red 114 para la comunicación a través de una red 116. La red puede ser una red informática, como, por ejemplo, internet.

El testigo de ID 106 tiene una memoria electrónica 118 con zonas de memoria protegidas 120, 122 y 124. La zona de memoria protegida 120 sirve para almacenar un valor de referencia que se necesita para la autentificación del usuario 102 con respecto al testigo de ID 106. Este valor de referencia es, por ejemplo, un indicativo, en particular un denominado número de identificación personal (PIN), o datos de referencia para una característica biométrica del usuario 102 que pueda utilizarse para la autentificación del usuario con respecto al testigo de ID 106.

La zona protegida 122 sirve para almacenar una clave privada y la zona de memoria protegida 124 sirve para almacenar atributos, por ejemplo del usuario 102, como, por ejemplo, su nombre, domicilio, fecha de nacimiento, sexo y/o atributos que conciernen al propio testigo de ID, como, por ejemplo, la institución que ha fabricado o emitido el testigo de ID, la vigencia del testigo de ID, un identificador del testigo de ID, como, por ejemplo, un número de pasaporte o un número de tarjeta de crédito.

La memoria electrónica 118 puede presentar además una zona de memoria 126 para almacenar un certificado. El certificado contiene una clave pública que está asociada a la clave privada almacenada en la zona de memoria 122 protegida. El certificado puede elaborarse según una norma de infraestructura de clave pública (PKI), por ejemplo según la norma X.509.

El certificado no debe almacenarse obligatoriamente en la memoria electrónica 118 del testigo de ID 106. Alternativa o adicionalmente, el certificado puede almacenarse también en un servidor de directorio público.

El testigo de ID 106 tiene un procesador 128. El procesador 128 sirve para ejecutar instrucciones de programa 130, 132 y 134. Las instrucciones de programa 130 sirven para la autentificación del usuario, es decir, para autentificar al usuario 102 con respecto al testigo de ID.

En una forma de realización con PIN, el usuario 102 introduce su PIN en el testigo de ID 106 para su autentificación, por ejemplo por medio del sistema informático de usuario 100. Ejecutando instrucciones de programa 130 se accede a continuación a la zona de memoria 120 protegida para comparar el PIN introducido con el valor de referencia del PIN allí almacenado. En caso de que el PIN introducido coincida con el valor de referencia del PIN, el usuario 102 se considera como autentificado.

Alternativamente, se registra una característica biométrica del usuario 102. Por ejemplo, el testigo de ID 106 tiene para ello un sensor de huella dactilar o un sensor de huella dactilar está conectado al sistema informático de usuario 100. En esta forma de realización, los datos biométricos registrados por el usuario 102 se comparan con los datos de referencia biométricos almacenados en la zona de memoria 120 protegida mediante la ejecución de las instrucciones de programa 130. Si hay una coincidencia suficiente de los datos biométricos registrados por el usuario 102 con los datos de referencia biométricos, el usuario 102 se considera como autentificado.

Las instrucciones de programa 134 sirven para realizar las etapas de un protocolo criptográfico concernientes al testigo de ID 106 para la autentificación de un sistema informático de proveedor de ID 136 con respecto al testigo de ID 106. El protocolo criptográfico puede ser un protocolo de reto-respuesta basado en una clave simétrica o un par de claves asimétricas.

Por ejemplo, por medio del protocolo criptográfico se implementa un procedimiento de control de acceso extendido como el que se especifica para documentos de viaje legibles por máquina (machine-readable travel documents – MRTD) de la Organización Internacional de Aviación Civil (ICAO). Gracias a la ejecución exitosa del protocolo criptográfico se autentifica el sistema informático de proveedor de ID 136 con respecto al testigo de ID y, por tanto, éste demuestra su autorización de lectura para leer los atributos almacenados en la zona de memoria 124 protegida. La autentificación puede ser también recíproca, es decir, también el testigo de ID 106 debe autentificarse entonces con respecto al sistema informático de proveedor de ID 136 según el mismo u otro protocolo criptográfico.

Las instrucciones de programa 132 sirven para la encriptación de extremo a extremo de datos transmitidos entre el testigo de ID 106 y el sistema informático de proveedor de ID 136, pero al menos de los atributos leídos de la zona de memoria 124 protegida por el sistema informático de proveedor de ID 136. Para la encriptación de extremo a extremo puede utilizarse una clave simétrica que se puede estipular, por ejemplo, con ocasión de la ejecución del protocolo criptográfico entre el testigo de ID 106 y el sistema informático de proveedor de ID 136.

Alternativamente a la forma de realización representada en la figura 1, el sistema informático de usuario 100 con su interfaz 104 puede comunicarse con la interfaz 108 no directamente, sino a través de un aparato de lectura conectada a la interfaz 104 para el testigo de ID 106. Gracias a este aparato de lectura, como, por ejemplo, un denominado terminal de tarjetas con chip de clase 2, puede realizarse también la introducción del PIN.

El sistema informático de proveedor de ID 136 tiene una interfaz de red 138 para la comunicación a través de la red 116. El sistema informático de proveedor de ID 136 tiene además una memoria 140 en la que se almacenan una clave privada 142 del sistema informático de proveedor de ID 136, y el certificado correspondiente 144. Asimismo, este certificado puede ser, por ejemplo, un certificado según una norma PKI, como, por ejemplo, X.509.

El sistema informático de proveedor de ID 136 tiene además al menos un procesador 145 para ejecutar instrucciones de programa 146 y 148. Gracias a la ejecución de las instrucciones de programa 146 se realizan las etapas del protocolo criptográfico que conciernen al sistema informático de proveedor de ID 136. Por tanto, en total se implementa el protocolo criptográfico por medio de la ejecución de las instrucciones de programa 134 por el procesador 128 del testigo de ID 106, así como por la ejecución de las instrucciones de programa 146 por el procesador 145 del sistema informático de proveedor de ID 136.

Las instrucciones de programa 148 sirven para implementar la encriptación de extremo a extremo al lado del sistema informático de proveedor de ID 136, por ejemplo sobre la base de la clave simétrica que se ha estipulado con ocasión de la ejecución del protocolo criptográfico entre el testigo de ID 106 y el sistema informático de proveedor de ID 136. En principio, puede utilizarse cualquier procedimiento en sí conocido para estipular la clave simérica para la encriptación de extremo a extremo, tal como, por ejemplo, un intercambio de claves Diffie-Hellman.

El sistema informático de 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 de proveedor de ID 136, en combinación con la necesidad de la autentificación del usuario 102 con respecto al testigo de ID 106, forma el anclaje de confianza para la autenticidad de los atributos leídos del testigo de ID 106.

Un sistema informático de servicio 150 puede configurarse para la recepción de un pedido o una orden de un servicio o un producto, en particular un servicio online. Por ejemplo, el usuario 102 puede abrir online, a través de la red 116, una cuenta en un banco o emplear otro servicio financiero o bancario. El sistema informático de servicio 150 puede configurarse también como unos grandes almacenes online, de modo que el usuario 102 puede adquirir, por ejemplo, online un teléfono móvil o similar. Además, el sistema informático de servicio 150 puede estar configurado también para el suministro de contenidos digitales, por ejemplo para la descarga de música y/o datos de vídeo.

El sistema informático de servicio 150 tiene para ello una interfaz de red 152 para la conexión con la red 116. Además, el sistema informático de servicio 150 tiene al menos un procesador 154 para ejecutar instrucciones de programa 156. Ejecutando las instrucciones de programa 156 se generan, por ejemplo, páginas HTML dinámicas, a través de las cuales el usuario 102 puede introducir su orden o su pedido.

Según el tipo del producto encargado o pedido o el servicio, el sistema informático de servicio 150 debe comprobar uno o varios atributos del usuario 102 y/o su testigo de ID 106 con ayuda de uno o varios criterios predeterminados. Sólo si se pasa esta prueba, se acepta y/o se ejecuta el pedido o la orden del usuario 102.

Por ejemplo, para la apertura de una cuenta bancaria o la compra de un teléfono móvil con un contrato asociado es necesario que el usuario 102 revele su identidad con respecto al sistema informático de servicio 150 y que se compruebe esta identidad. En el estado de la técnica, el usuario 102 debe presentar para ello, por ejemplo, su documento de identidad. Este proceso se sustituye por la lectura de la identidad digital del usuario 102 en su testigo de ID 106.

Sin embargo, según el caso de aplicación, el usuario 102 no debe revelar su identidad con respecto al sistema informático de servicio 150, sino que es suficiente la notificación de, por ejemplo, sólo uno de los atributos. Por ejemplo, el usuario 102 puede producir, por medio de uno de los atributos, un comprobante de que pertenece a un determinado grupo de personas que está autorizado para el acceso a datos contenidos en el sistema informático de servicio 150 y preparados para su descarga. Por ejemplo, un criterio de este tipo puede ser una edad mínima del usuario 102 o la pertenencia del usuario 102 a un círculo de personas que tiene una autorización de acceso a determinados datos confidenciales.

Para la utilización del servicio facilitado por el sistema informático de servicio 150 se procede como sigue:

1. Autentificación del usuario 102 con respecto al testigo de ID 106.

El usuario 102 se autentifica con respecto al testigo de ID 106. En una implementación con PIN, el usuario 102 introduce para ello su PIN, por ejemplo a través del sistema informático de usuario 100 o un terminal de tarjeta de chip conectado a él. Ejecutando las instrucciones de programa 130, el testigo de ID 106 comprueba entonces la corrección del PIN introducido. Cuando el PIN introducido coincide con el valor de referencia del PIN almacenado en la zona de memoria 120 protegida, el usuario 102 se considera como autentificado. Puede procederse de manera

análoga cuando se utiliza una característica biométrica del usuario 102 para su autentificación, tal como se describe anteriormente.

2. Autentificación del sistema informático de proveedor de ID 136 con respecto al testigo de ID 106.

Para ello se establece una conexión entre el testigo de ID 106 y el sistema informático de proveedor de ID 136 a través del sistema informático de usuario 100 y la red 116. Por ejemplo, el sistema informático de proveedor de ID 136 transmite su certificado 144 al testigo de ID 106 a través de esta conexión. Gracias a las instrucciones de programa 134 se genera un denominado reto, es decir, por ejemplo un número aleatorio. Este número aleatorio se encripta con la clave pública contenida en el certificado 144 del sistema informático de proveedor de ID 136. El cifrado resultante se envía desde el testigo de ID 106, a través de la conexión, hasta el sistema informático de proveedor de ID 136. El sistema informático de proveedor de ID 136 desencripta el cifrado con ayuda de su clave privada 142 y obtiene así el número aleatorio. El sistema informático de proveedor de ID 136 reenvía el número aleatorio al testigo de ID 106 a través de la conexión. Ejecutando las instrucciones de programa 134 se comprueba allí si el número aleatorio recibido del sistema informático de proveedor de ID 136 coincide con el número aleatorio generado originariamente, es decir, el reto. Si éste es el caso, entonces el sistema informático de proveedor de ID 136 se autentifica como válido con respecto al testigo de ID 106. El número aleatorio puede utilizarse como clave simétrica para la encriptación de extremo a extremo.

3. Después de que el usuario 102 se ha autentificado con éxito con respecto al testigo de ID 106 y después de que el sistema informático de proveedor de ID 136 se ha autentificado con éxito con respecto al testigo de ID 106, el sistema informático de proveedor de ID 136 recibe una autorización de lectura para leer uno, varios o todos los atributos almacenados en la zona de memoria 124 protegida. Basándose en una orden de lectura correspondiente que envía el sistema informático de proveedor de ID 136 al testigo de ID 106 a través de la conexión, los atributos requeridos se leen en la zona de memoria 124 protegida y se encriptan por la ejecución de las instrucciones de programa 132. Los atributos encriptados se transmiten, a través de la conexión, al sistema informático de proveedor de ID 136 y se desencriptan allí por la ejecución de las instrucciones de programa 148. Por tanto, el sistema informático de proveedor de ID 136 adquiere conocimiento de los atributos leídos del testigo de ID 106.

Estos atributos se firman por el sistema informático de proveedor de ID con ayuda de su certificado 144 y se transmiten al sistema informático de servicio 150 a través del sistema informático de usuario 100 o bien directamente. Por tanto, el sistema informático de servicio 150 es puesto en conocimiento de los atributos leídos del testigo de ID 106, de modo que el sistema informático de servicio 150 puede comprobar estos atributos con ayuda de los uno o varios criterios predeterminados para, eventualmente, proporcionar después el servicio requerido por el usuario 102.

Gracias a la necesidad de autentificación del usuario 102 con respecto al testigo de ID 106 y de autentificación del sistema informático de proveedor de ID 136 con respecto al testigo de ID 106 se crea el anclaje de confianza necesario, de modo que el sistema informático de servicio 150 puede estar seguro de que los atributos del usuario 102 comunicados por el sistema informático de proveedor de ID 136 son auténticos y no se han falsificado.

Según la forma de realización, la secuencia de la autentificación puede ser diferente. Por ejemplo, puede preverse que el usuario 102 deba autentificarse primero con respecto al testigo de ID 106 y a continuación tenga que autentificarse el sistema informático de proveedor de ID 136. No obstante, es básicamente posible también que el sistema informático de proveedor de ID 136 deba autentificarse primero con respecto al testigo de ID 106 y sólo con posterioridad tenga que autentificarse el usuario 102.

En el primer caso, el testigo de ID 106 está configurado de tal modo que se active por el usuario 102 únicamente por la introducción de un PIN correcto o una característica biométrica correcta. Solamente esta activación hace posibles la puesta en marcha de las instrucciones de programa 132 y 134 y, por tanto, la autentificación del sistema informático de proveedor de ID 136.

En el segundo caso, se posible iniciar ya también las instrucciones de programa 132 y 134 cuando el usuario 102 no se ha autentificado aún con respecto al testigo de ID 106. En este caso, las instrucciones de programa 134 están configuradas, por ejemplo, de tal modo que el sistema informático de proveedor de ID 136 pueda realizar un acceso de lectura a la zona de memoria protegida 124 para leer uno varios atributos únicamente cuando se haya señalizado también la autentificación exitosa del usuario 102 por las instrucciones de programa 130.

Es especialmente ventajoso el aprovechamiento del testigo de ID 106 para, por ejemplo, aplicaciones de comercio electrónico y administración electrónica, concretamente sin interrupción de medios y con certeza jurídica debido al anclaje de confianza formado por la necesidad de la autentificación del usuario 102 y del sistema informático de proveedor de ID 136 con respecto al testigo de ID 106. Además, es especialmente ventajoso que no se necesite un almacenamiento central de los atributos de diferentes usuarios 102, de modo que se resuelven con ello los problemas de protección de datos existentes en el estado de la técnica. En lo que concierne a la comodidad de la aplicación del procedimiento, es especialmente ventajoso que no sea necesario un registro previo del usuario 102 para el uso del sistema informático de proveedor de ID 136.

La figura 2 muestra una forma de realización de un procedimiento según la invención. En la etapa 200 se envía una solicitud de servicio del sistema informático de usuario al sistema informático de servicio. Por ejemplo, el usuario pone en marcha para ello un navegador de internet del sistema informático del usuario e introduce una URL para recuperar una página web del sistema informático de servicio. En la página web recuperada, el usuario introduce entonces su solicitud de servicio, por ejemplo para el pedido o la orden de encargo de un servicio o un producto.

En la etapa 202, el sistema informático de servicio 150 especifica seguidamente uno o varios atributos que son necesarios para comprobar la autorización del usuario para la solicitud 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 del servicio 150 puede predefinirse firmemente o, según la solicitud de servicio, puede determinarse en cada caso individual a través del sistema informático de servicio 150 con ayuda de reglas predeterminadas.

En la etapa 204, la especificación de atributo, es decir, la especificación realizada en la etapa 202 de los uno o varios atributos, se transmite desde el sistema informático del servicio hasta el sistema informático del proveedor de ID, concretamente de manera directa o a través del sistema informático del usuario.

Para dar la posibilidad al sistema informático del proveedor de ID de leer atributos de su testigo de ID, el usuario se autentifica en la etapa 206 con respecto al testigo de ID.

En la etapa 208 se establece una conexión entre el testigo de ID y el sistema informático del proveedor de ID. En este caso, se trata preferiblemente de una conexión segura, por ejemplo según un denominado procedimiento de mensajería segura.

En la etapa 210 se realiza al menos una autentificación del sistema informático del proveedor de ID con respecto al testigo de ID a través de la conexión establecida en la etapa 208. Adicionalmente, puede preverse también una autentificación del testigo de ID con respecto al sistema informático del proveedor de ID.

Después de que tanto el usuario como también el sistema informático del proveedor de ID se hayan autentificado con éxito con respecto al testigo de ID, el sistema informático del proveedor de ID recibe del testigo de ID la autorización de acceso para leer los atributos. En la etapa 212, el sistema informático del proveedor de ID envía una o varias órdenes de lectura para leer en el testigo de ID los atributos necesarios según la especificación de atributo. Los atributos se transmiten entonces al sistema informático del proveedor de ID a través de la conexión securizada por medio de una encriptación de extremo a extremo y se desencriptan allí.

Los valores de atributo leídos se firman en la etapa 214 por el sistema informático del proveedor de ID. En la etapa 216 el sistema del proveedor de ID envía a través de la red los valores de atributo firmados. Los valores de atributo firmados alcanzan el sistema informático del servicio directamente o a través del sistema informático del usuario. En el último caso, el usuario puede tener la posibilidad de tomar nota de los valores de atributo firmados y/o complementarlos con datos adicionales. Puede preverse que los valores de atributo firmados se reenvíen eventualmente con los datos complementados al sistema informático del servicio desde el sistema informático del usuario únicamente después de su liberación por el usuario. Por tanto, se establece la mayor transparencia posible para el usuario con respecto a los atributos enviados al sistema informático del servicio por el sistema informático del proveedor de ID.

La figura 3 muestra otras formas de realización de un testigo de ID según la invención y sistemas informáticos según la invención. En la forma de realización de la figura 3, el testigo de ID 106 está configurado como un documento, tal como, por ejemplo, un documento basado en papel y/o basado en plástico con un circuito de mando electrónico integrado, a través del cual se forman la interfaz 108, la memoria 118 y el procesador 128. El circuito de mando electrónico integrado puede ser, por ejemplo, una denominada etiqueta de radio que se designa también como etiqueta RFID o RIFD-label. No obstante, la interfaz 108 puede configurarse también como etiqueta de contacto o como la denominada interfaz de doble modo.

En particular, el documento 106 puede ser un documento de valor o de seguridad, como, por ejemplo, un documento de viaje legible por máquina (MRTD), tal como, por ejemplo, un pasaporte electrónico o un carné de identidad electrónico, o un medio de pago, como, por ejemplo, una tarjeta de crédito.

En la forma de realización aquí contemplada están almacenados en la zona de memoria 124 protegida los atributos i, en donde $1 \leq i \leq n$. Además, sin limitar la generalidad, se parte de que el testigo de ID 106 mostrado a modo de ejemplo en la figura 3 es un carné de identidad electrónico. Por ejemplo, el atributo i = 1 es el nombre, el atributo i = 2 es el apellido, el atributo i = 3 es la dirección y el atributo i = 4 es la fecha de nacimiento, etc.

La interfaz 104 del sistema informático de usuario 100 puede estar configurada, en la forma de realización aquí contemplada como un aparato de lectura de RFID, que puede formar un componente integral del sistema informático del usuario o puede estar conectado a éste como un componente independiente.

El usuario 102 dispone de uno o varios testigos de ID que están estructurados en principio iguales, como, por ejemplo, un testigo de ID 106', que es una tarjeta de crédito.

En el sistema informático de usuario 100 pueden almacenarse varios conjuntos de datos de configuración 158, 160, ... Cada grupo de datos de configuración indica para un cantidad de atributos determinada una fuente de datos y un sistema informático de proveedor de ID que puede leer la fuente de datos especificada. En esta forma de realización, el sistema informático de usuario 100 puede operar, a través de la red 116, con diferentes sistemas informáticos de proveedor de ID 136, 136', ... que pueden pertenecer respectivamente a diferentes centros llamados de confianza. Por ejemplo, el sistema informático de proveedor de ID 136 pertenece al centro de confianza A y el sistema informático de proveedor de ID 136' estructurado en principio de la misma forma pertenece a otro centro de confianza B.

En el conjunto de datos de configuración 158, que se designa también como contenedor de ID, está definida la cantidad de atributos i = 1 a i = 4. A estos atributos están asociados respectivamente la fuente de datos "carné de identidad", es decir, el testigo de ID 106, así como el centro de confianza A, es decir, el sistema informático de proveedor de ID 136. Este puede estar especificado, por ejemplo, en forma de su URL en el conjunto de datos de configuración 158.

Por el contrario, en el conjunto de datos de configuración 116 está definida una cantidad de atributos I, II y III. Como fuente de datos para estos atributos se especifica respectivamente la tarjeta de crédito, es decir, el testigo de ID 106'. El testigo de ID 106' tiene una zona de memoria 124' protegida en la que están almacenados los atributos I, II, III, ... El atributo I puede ser, por ejemplo el nombre del titular de la tarjeta de crédito, el atributo II el número de la tarjeta de crédito y el atributo III el plazo de validez de la tarjeta de crédito, etc.

Como sistema informático del proveedor de ID está indicado en el conjunto de datos de configuración 160 el sistema informático de proveedor de ID 136' del centro de confianza B.

Alternativamente a la forma de realización mostrada en la figura 3, para diferentes atributos en el mismo conjunto de datos de configuración pueden especificarse también diferentes fuentes de datos y/o diferentes sistemas informáticos de proveedor de ID.

En la forma de realización de la figura 3, cada uno de los sistemas informáticos de proveedor de ID 136, 136', ... puede tener varios certificados correspondientes.

Por ejemplo, en la memoria 140 del sistema informático de proveedor de ID 136, que se muestra a modo de ejemplo en la figura 3, están almacenados varios certificados, como, por ejemplo, los certificados 144.1 y 144.2 con las claves privadas 142.1 y 142.2 respectivamente asociadas. En el certificado 144.1 están definidos derechos de lectura del sistema informático de proveedor de ID 136 referentes a los atributos i = 1 a i = 4, mientras que en el certificado 144.2 están definidos derechos de lectura referentes a los atributos I a III.

Para la utilización de un servicio ofrecido por el sistema informático de servicio 150, el usuario 102 efectúa primero una introducción de usuario 162 en el sistema informático de usuario 100 para introducir su solicitud para el servicio deseado, por ejemplo en una página web del sistema informático de servicio 150. Esta solicitud de servicio 164 se transmite desde el sistema informático de usuario 100, a través de la red 116, hasta el sistema informático de servicio 150. El sistema informático de servicio 150 responde a ello con una especificación de atributo 166, es decir, con una especificación de aquellos atributos que el sistema informático de servicio 150 necesita del usuario 102 para procesar la solicitud de servicio 164. La especificación de atributo puede realizarse, por ejemplo, en forma de los nombres de atributo, como, por ejemplo "nombre", "apellido", "dirección", "número de tarjeta de crédito".

La recepción de la especificación de atributo 166 se le señaliza al usuario 102 a través el sistema informático de usuario 100. El usuario 102 puede elegir seguidamente uno o, en caso necesario, varios conjuntos de datos de configuración 158, 160, ... que definen las respectivas cantidades de atributos que contienen los atributos según la especificación de atributo 166, al menos como cantidad parcial.

Si la especificación de atributo 166 requiere, por ejemplo, solamente la notificación del nombre, del apellido y de la dirección del usuario 102, entonces, el usuario 102 puede elegir el conjunto de datos de configuración 158. Por el contrario, si además se especifica el número de tarjeta de crédito en la especificación de atributo 166, entonces el usuario 102 puede elegir adicionalmente el conjunto de datos de configuración 160. Este proceso puede realizarse también de manera completamente automática por medio del sistema informático de usuario 100, por ejemplo por la ejecución de las instrucciones de programa 112.

Además, en primer lugar se parte de que sólo se elige uno de los conjuntos de datos de configuración, como, por ejemplo, el conjunto de datos de configuración 158, debido a la especificación de atributo 166.

El sistema informático de usuario 100 envía seguidamente una solicitud 168 al sistema o sistemas informáticos de proveedor de ID indicados en el conjunto de datos de configuración seleccionado, en el ejemplo contemplado al sistema informático de proveedor de ID 136 del centro de confianza A. Esta solicitud 168 contiene una indicación de los atributos según la especificación de atributo 166 a leer por el sistema informático de proveedor de ID 136 en la fuente de datos indicada en el conjunto de datos de configuración 158.

El sistema informático de proveedor de ID 136 selecciona seguidamente uno o varios de sus certificados que presentan los derechos de lectura necesarios para leer estos atributos. Cuando, por ejemplo, los atributos i = 1 a 3 deben leerse en el carné de identidad, entonces el sistema informático de proveedor de ID 136 selecciona su certificado 144.1 que define los derechos de lectura necesarios para ello. Esta selección del certificado se realiza por medio de la ejecución de instrucciones de programa 149.

Seguidamente, se inicia la ejecución del protocolo criptográfico. Por ejemplo, el sistema informático de proveedor de ID 136 envía para ello una respuesta al sistema informático de usuario 100. El sistema informático de usuario 100 requiere seguidamente al usuario 102 su autentificación con respecto a la fuente de datos especificada, es decir, aquí con respecto al carné de identidad.

El usuario 102 pone seguidamente su carné de identidad, es decir, el testigo de ID 106, en la zona del aparato de lectura de RFID 104, e introduce, por ejemplo, su PIN para su autentificación. Gracias a la autentificación exitosa del usuario 102 con respecto al testigo de ID 106 se activa éste para la realización del protocolo criptográfico, es decir, para la ejecución de las instrucciones de programa 134. Además, se autentifica el sistema informático de proveedor de ID 136 con respecto al testigo de ID 106 con ayuda del certificado seleccionado 144.1, por ejemplo con ayuda de un procedimiento de reto-respuesta. Esta autentificación puede ser también recíproca. Tras la autentificación exitosa del sistema informático de proveedor de ID 136 con respecto al testigo de ID 106, el sistema informático de proveedor de ID dirige al sistema informático de usuario 100 una solicitud de lectura para leer los atributos necesarios, cuyo sistema reenvía esta solicitud al testigo de ID 106 a través del aparato de lectura de RFID 104. El testigo de ID 106 comprueba con ayuda del certificado 144.1 si el sistema informático de proveedor de ID 136 tiene el derecho de lectura necesario para ello. Cuando es éste el caso, los atributos deseados se leen en la zona de memoria 124 protegida y, por medio de la encriptación de extremo a extremo, se transmiten al sistema informático de proveedor de ID a través del sistema informático de usuario 100.

El sistema informático de proveedor de ID 136 envía entonces una respuesta 170, que contiene los atributos leídos, al sistema informático de servicio 150 a través de la red 116. La respuesta 170 está firmada digitalmente con el certificado 144.1.

Alternativamente, el sistema informático de proveedor de ID 136 envía la respuesta 170 al sistema informático de usuario 100. El usuario 102 adquiere seguidamente la posibilidad de leer los atributos contenidos en la respuesta 170 y decidir si querría o no reenviar realmente estos atributos al sistema informático de servicio 150. Solamente después de introducir una orden de liberación del usuario 102 en el sistema informático de usuario 100 se reenvía entonces la respuesta 170 al sistema informático de servicio 150. En esta forma de realización es posible además que el usuario 102 complemente la respuesta 170 con datos adicionales.

Cuando están implicados varios sistemas informáticos de proveedor de ID 136, 136', ..., entonces las repuestas individuales del sistema informático de proveedor de ID pueden recopilarse a través del sistema informático de usuario 100 en una única respuesta que contiene todos los atributos según la especificación de atributo 166, la cual se envía desde el sistema informático de usuario 100 al sistema informático de servicio 150.

Según una forma de realización de la invención, el usuario 102, con ocasión de la solicitud de servicio 164, puede revelar uno o varios de sus atributos con respecto al sistema informático de servicio 150, para lo cual, por ejemplo, estos atributos del usuario se transmiten a través de la red 116 al sistema informático de servicio como parte de la solicitud de servicio 164. En particular, el usuario 102 puede introducir estos atributos en la página web del sistema informático de servicio 150. La autenticidad de estos atributos se confirma entonces por la respuesta 170, es decir, el sistema informático de servicio 150 puede comparar los atributos recibidos del usuario 102 con los atributos leídos del testigo de ID 106 por el sistema informático de proveedor de ID 136 y comprobar la coincidencia.

Según una forma de realización adicional de la invención, puede estar indicado también en la especificación de atributo 166 al menos un atributo adicional que no está almacenado en uno de los testigos de ID del usuario 102, sino que puede consultarse desde una fuente de datos externa. En este caso, puede tratarse, por ejemplo, de un atributo que concierne a la solvencia del usuario 102. El sistema informático de usuario 100 puede contener para ello un conjunto de datos de configuración adicional 161 que contiene la indicación de una fuente de datos y de un sistema informático de proveedor de ID para el atributo A – por ejemplo, la solvencia. La fuente de datos puede ser una agencia de informes online, tal como, por ejemplo Schufa, Dun & Bradstreet o similares. Como sistema informático de proveedor de ID está indicado, por ejemplo, un centro de confianza C, como en la forma de realización de la figura 3. La fuente de datos puede encontrarse aquí en el centro de confianza C.

Por tanto, para consultar el atributo A, el sistema informático de usuario 100 dirige una solicitud correspondiente (no mostrada en la figura 3) al centro de confianza C, es decir, al sistema informático de proveedor de ID 136''. Éste suministra seguidamente el atributo A, el cual es reenviado por el sistema informático de usuario 100 al sistema informático de servicio 150 junto con los atributos adicionales que se hayan leído en el testigo o testigos de ID del usuario 102.

Preferiblemente, la consulta del atributo A se realiza después de que se hayan consultado ya los atributos concernientes a la identidad digital del usuario 102 en uno de los testigos de ID del usuario 102 y, por ejemplo, se

hayan recibido del sistema informático de usuario 100 como respuesta firmada 170. La consulta del atributo A por el sistema informático de proveedor de ID 136'' a través del sistema informático de usuario 100 contiene entonces la respuesta firmada 170, de modo que el sistema informático de proveedor de ID 136'' tiene una información segura con respecto a la identidad del usuario 102.

La figura 4 muestra otra forma de realización de un procedimiento según la invención. Mediante una entrada 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 querría utilizar. Esto se realiza, por ejemplo, por recuperación de una página de internet del sistema informático de servicio y una selección de uno de los servicios allí ofrecidos. La solicitud de servicio del usuario 102 se transmite desde el sistema informático de usuario 100 hasta el sistema informático de servicio 150.

El sistema informático de servicio 150 responde a la solicitud de servicio con una especificación de atributo, es decir, por ejemplo, una lista de nombres de atributos. Tras la recepción de la especificación de atributo, el sistema informático de usuario 100 requiere al usuario 102, por ejemplo a través de una invitación de introducción, a que se autentifique con respecto al testigo de ID 106.

El usuario 102 se autentifica seguidamente con respecto al testigo de ID 106, por ejemplo por la introducción de su PIN. Tras una autentificación exitosa, la especificación de atributo se reenvía por el sistema informático de usuario 100 a un sistema informático de proveedor de ID 136. Éste se autentifica seguidamente con respecto al testigo de ID 106 y dirige al testigo de ID 106 una solicitud de servicio para leer los atributos según la especificación de atributo.

Suponiendo la autentificación exitosa previa del usuario 102 y del sistema informático de proveedor de ID 136, el testigo de ID 106 responde a la solicitud de lectura con los atributos deseados. El sistema informático de proveedor de ID 136 firma los atributos y envía los atributos firmados al sistema informático de usuario 100. Tras la liberación por el usuario 102, los atributos firmados se transmiten entonces al sistema informático de servicio 150, que entonces puede producir eventualmente el servicio deseado.

Lista de símbolos de referencia

100	Sistema informático de usuario
102	Usuario
104	Interfaz
106	Testigo de ID
108	Interfaz
110	Procesador
112	Instrucciones de programa
114	Interfaz de red
116	Red
118	Memoria electrónica
120	Zona de memoria protegida
122	Zona de memoria protegida
124	Zona de memoria protegida
126	Zona de memoria
128	Procesador
130	Instrucciones de programa
132	Instrucciones de programa
134	Instrucciones de programa
136	Sistema informático de proveedor de ID
138	Interfaz de red
140	Memoria

142 Clave privada

144 Certificado

145 Procesador

146 Instrucciones de programa

148 Instrucciones de programa

149 Instrucciones de programa

150 Sistema informático de servicio

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

164 Solicitud de servicio

166 Especificación de atributo

168 Solicitud

170 Respuesta

REIVINDICACIONES

1. Procedimiento para leer al menos un atributo almacenado en un testigo de ID (106, 106'), en el que el testigo de ID está asociado a un usuario (102), con las siguientes etapas:

- autentificar al usuario con respecto al testigo de ID,

- establecer una conexión protegida entre el testigo de ID y un primer sistema informático (136) a través de una red (116),

- autentificar el primer sistema informático (136) con respecto al testigo de ID por medio de la conexión protegida,

- después de autentificar exitosamente al usuario y al primer sistema informático con respecto al testigo de ID, hacer que el primer sistema informático acceda a la lectura del al menos un atributo almacenado en el testigo de ID por medio del envío de una o varias órdenes de lectura y la transmisión del por lo menos un atributo desde el testigo de ID por medio de una encriptación de extremo a extremo, a través de la conexión protegida, hasta el primer sistema informático, y desencriptar el al menos un atributo por medio del primer sistema informático, con las siguientes etapas adicionales:

  i. firmar el al menos un atributo leído del testigo de ID por el primer sistema informático,

  ii. transmitir el atributo firmado desde el primer sistema informático hasta un segundo sistema informático.

en el que la autentificación del primer sistema informático con respecto al testigo de ID se realiza con ayuda de un certificado (144) del primer sistema informático, en el que el certificado contiene una indicación de aquellos atributos almacenados en el testigo de ID para los cuales el primer sistema informático está autorizado para realizar el acceso de lectura, y

en el que el testigo de ID comprueba la autorización de lectura del primer sistema informático para realizar el acceso de lectura a al menos uno de los atributos con ayuda del certificado.

2. Procedimiento según la reivindicación 1, con las siguientes etapas adicionales:

- enviar una solicitud (164) de un tercer sistema informático (100) al segundo sistema informático,

- especificar uno o varios atributos por el segundo sistema informático,

- enviar la especificación de atributo (166) del segundo sistema informático al primer sistema informático,

en el que el acceso de lectura del primer sistema informático se realiza para leer uno o varios atributos del testigo de ID especificados en la especificación de atributo.

3. Procedimiento según la reivindicación 2, en el que la solicitud (164) contiene un identificador para identificar el primer sistema informático por el segundo sistema informático, y en el que la transmisión de la especificación de atributo del segundo sistema informático al primer sistema informático se realiza sin intercalación del tercer sistema informático.

4. Procedimiento según la reivindicación 2, en el que el tercer sistema informático presenta varios conjuntos de datos de configuración predefinidos (158, 160, ...), en el que cada uno de los conjuntos de datos de configuración especifica una cantidad parcial de los atributos, al menos una fuente de datos y un primer sistema informático de una cantidad de primeros sistemas informáticos (136, 136',...), en el que la especificación de atributo se transmite primero del segundo sistema informático al tercer sistema informático, de modo que, por medio del tercer sistema informático, se selecciona al menos uno de los conjuntos de datos de configuración que especifica una cantidad parcial de los atributos que contiene el al menos un atributo especificado en la especificación de atributo, y en el que el tercer sistema informático reenvía la especificación de atributo al primer sistema informático, y en el que una conexión entre el primer sistema informático y el testigo de ID especificado por la indicación de la fuente de datos en el conjunto de datos seleccionado se establece por medio del tercer sistema informático.

5. Procedimiento según una de las reivindicaciones anteriores, en el que el al menos un atributo leído del testigo de ID por el primer sistema informático se envía al tercer sistema informático, desde donde se le reenvía al segundo sistema informático tras su liberación por el usuario.

6. Procedimiento según una de las reivindicaciones anteriores, en el que el tercer sistema informático tiene al menos un conjunto de datos de configuración (161) que especifica una fuente de datos externa para la consulta de un atributo adicional (A) por el tercer sistema informático a través de la red (116), en el que se efectúa la consulta del atributo adicional después de que se haya leído el al menos un atributo en el testigo de ID y después de que el tercer sistema informático haya recibido del primer sistema informático el al menos un atributo firmado, conteniendo la consulta el al menos un atributo firmado.

7. Producto de programa informático con instrucciones ejecutables por un sistema informático para realizar un procedimiento según una de las reivindicaciones anteriores.

8. Sistema informático con al menos un primer sistema informático (136) y un testigo de ID (106, 106') que pueden ser unidos por medio de una conexión protegida a través de una red (116), en el que el primer sistema informático presenta lo siguiente:

- unos medios (138) para recibir una especificación de atributo (166) a través de la red (116), especificando la especificación de atributo al menos un atributo,

- unos medios (142, 144, 146) de autentificación con respecto a un testigo de ID (106), efectuándose la autentificación del primer sistema informático con respecto al testigo de ID con ayuda de un certificado (144) del primer sistema informático, conteniendo el certificado una indicación de aquellos atributos almacenados en el testigo de ID para los cuales el primer sistema informático está autorizado para realizar el acceso de lectura,

- unos medios para leer al menos un atributo en el testigo de ID por medio de la conexión protegida, presuponiendo la lectura del al menos un atributo que un usuario asociado al testigo de ID y el sistema informático se han autentificado con respecto al testigo de ID,

- unos medios para firmar el atributo leído del testigo de ID,

- unos medios para transmitir el atributo firmado a un segundo sistema informático,

en donde el testigo de ID presenta:

- una zona de almacenamiento protegida (124) para almacenar al menos un atributo,

- unos medios (120, 130) para autentificar un usuario (102) asociado al testigo de ID con respecto al testigo de ID,

- unos medios (134) para autentificar el primer sistema informático (136) con respecto al testigo de ID,

- unos medios (132) para establecer una conexión protegida con el primer sistema informático, a través de la cual el primer sistema informático puede leer el al menos un atributo,

- unos medios para la encriptación de extremo a extremo de la conexión para una transmisión protegida del al menos uno de los atributos al primer sistema informático por medio de la conexión,

en el que el testigo de ID comprueba la autorización de lectura del primer sistema informático para realizar el acceso de lectura a al menos uno de los atributos con ayuda del certificado.

9. Sistema informático según la reivindicación 8, en el que los medios (138) para la recepción de la especificación de atributo están formados por un segundo sistema informático, y con unos medios (138) para enviar el al menos un atributo leído del testigo de ID a un tercer sistema informático (100) para su reenvío al segundo sistema informático.

10. Sistema informático según una de las reivindicaciones 8 o 9 con varios de los certificados (144.1; 144.2) de derechos de lectura diferentes, en el que el sistema informático está configurado para, debido a la recepción de la especificación de atributo, seleccionar al menos uno de los certificados que presenta los derechos de lectura suficientes para leer los atributos especificados en la especificación de atributo.

11. Sistema informático según la reivindicación 8, 9 o 10, en el que el testigo de ID es un aparato electrónico, en particular un lápiz USB, o un documento, en particular un documento de valor o de seguridad.

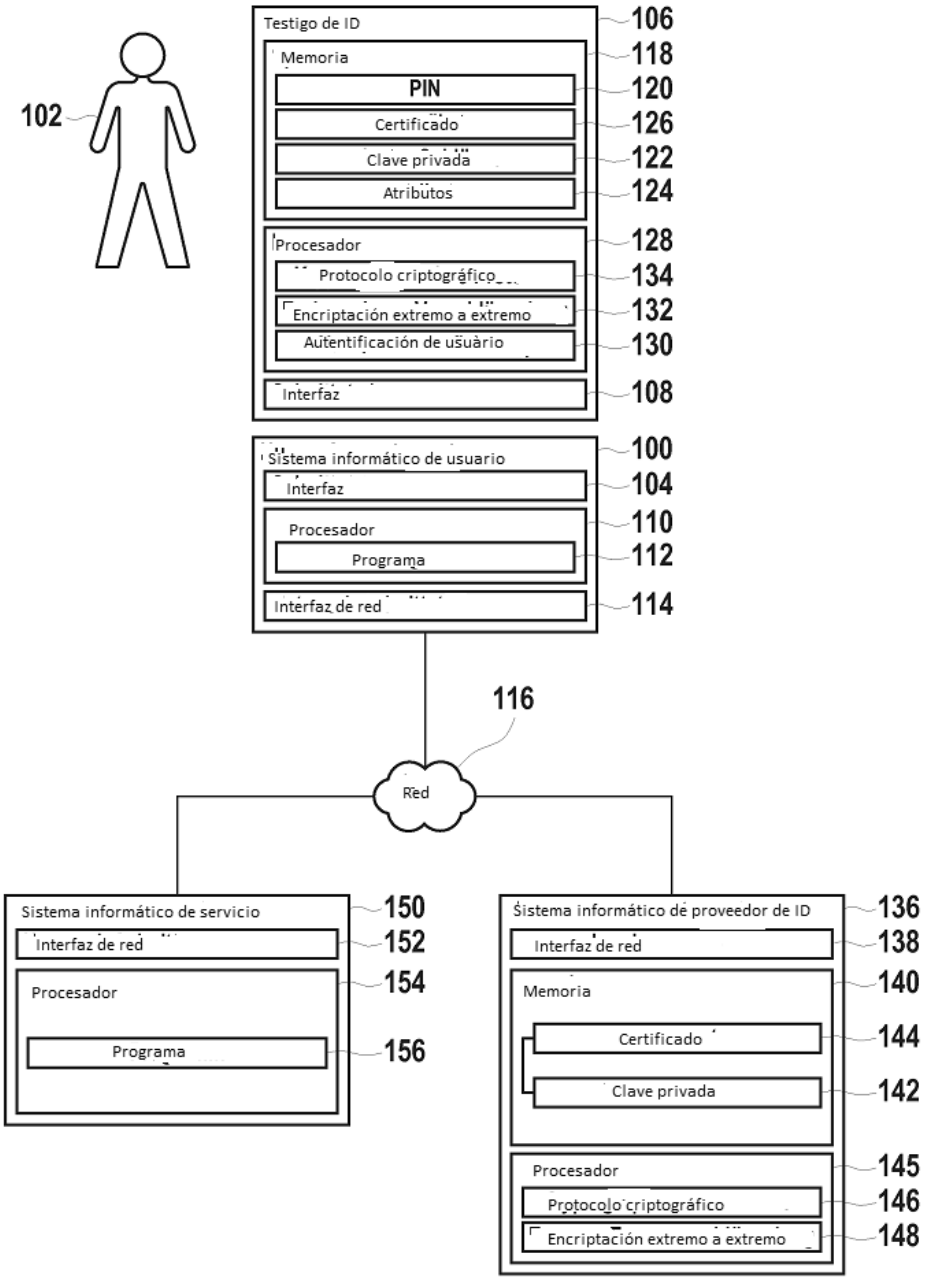

102
Testigo de ID
106
Memoria
118
PIN
120
Certificado
126
Clave privada
122
Atributos
124
Procesador
128
Protocolo criptográfico
134
Encriptación extremo a extremo
132
Autentificación de usuario
130
Interfaz
108
Sistema informático de usuario
100
Interfaz
104
Procesador
110
Programa
112
Interfaz de red
114
116
Red
Sistema informático de servicio
150
Interfaz de red
152
Procesador
154
Programa
156
Sistema informático de proveedor de ID
136
Interfaz de red
138
Memoria
140
Certificado
144
Clave privada
142
Procesador
145
Protocolo criptográfico
146
Encriptación extremo a extremo
148

Fig. 1

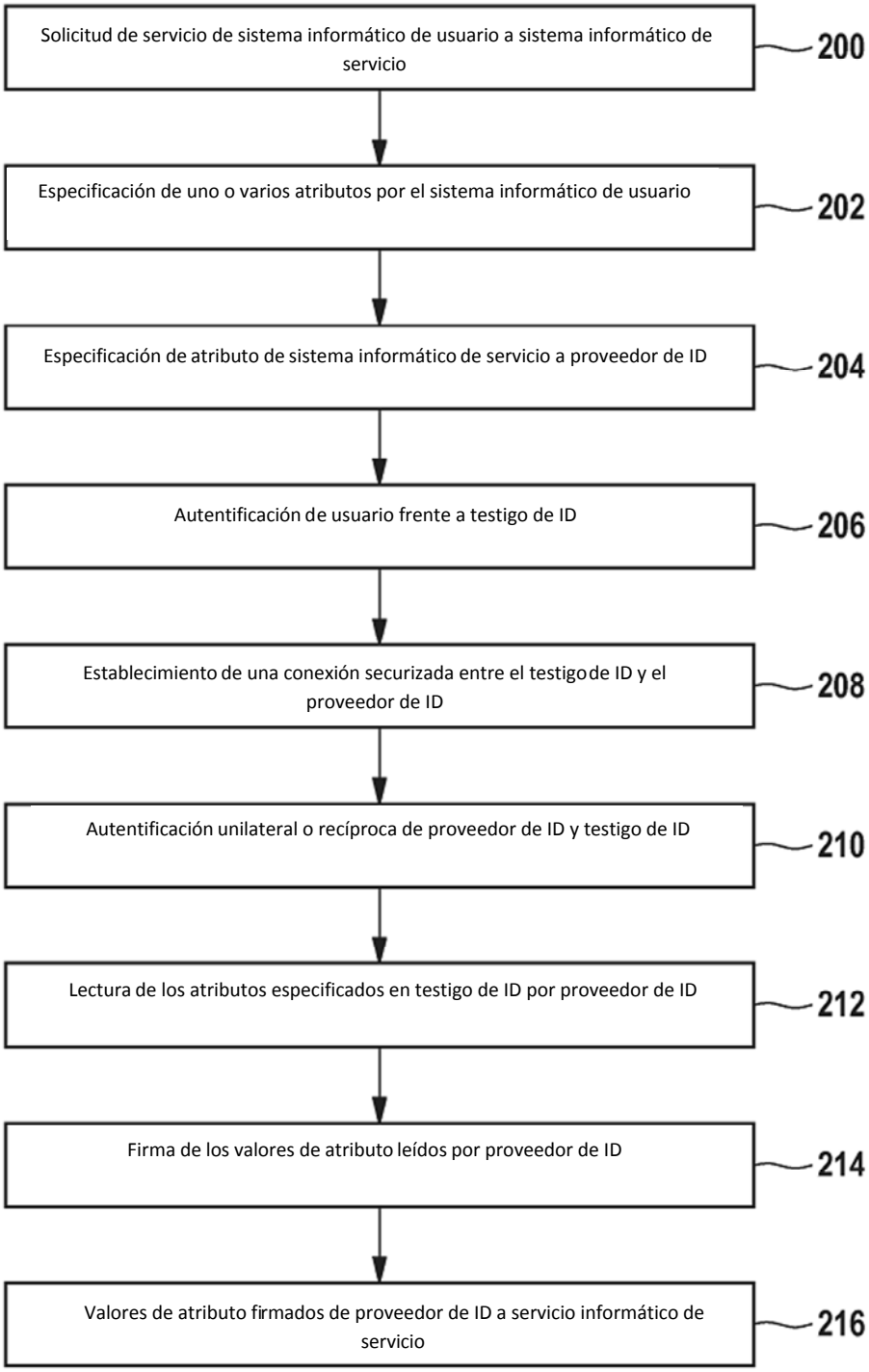

Solicitud de servicio de sistema informático de usuario a sistema informático de servicio
200
Especificación de uno o varios atributos por el sistema informático de usuario
202
Especificación de atributo de sistema informático de servicio a proveedor de ID
204
Autentificación de usuario frente a testigo de ID
206
Establecimiento de una conexión securizada entre el testigo de ID y el proveedor de ID
208
Autentificación unilateral o recíproca de proveedor de ID y testigo de ID
210
Lectura de los atributos especificados en testigo de ID por proveedor de ID
212
Firma de los valores de atributo leídos por proveedor de ID
214
Valores de atributo firmados de proveedor de ID a servicio informático de servicio
216

Fig. 2

Fig. 3

Fig. 3a	Fig. 3b	Fig. 3c

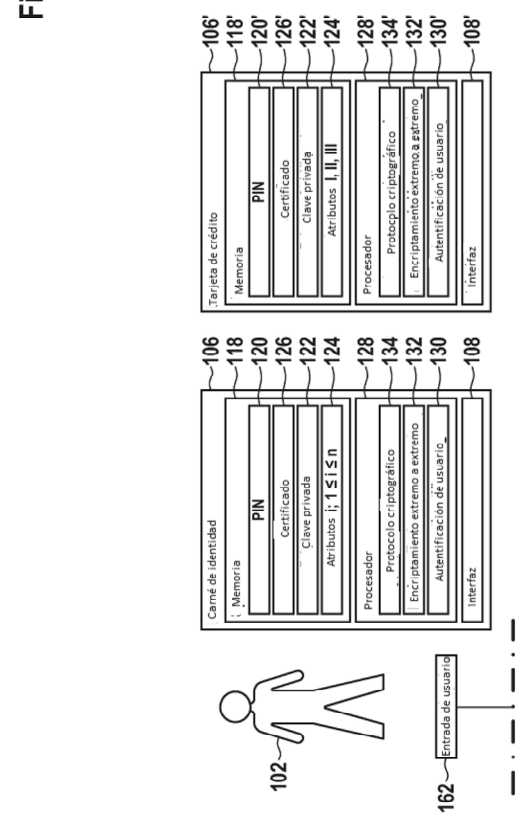
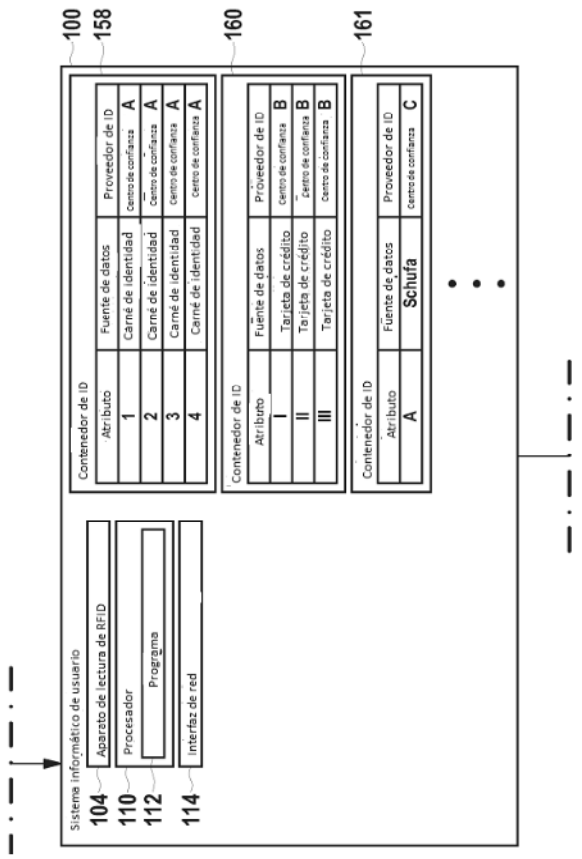


Fig. 3

Fig. 3a | Fig. 3b | Fig. 3c



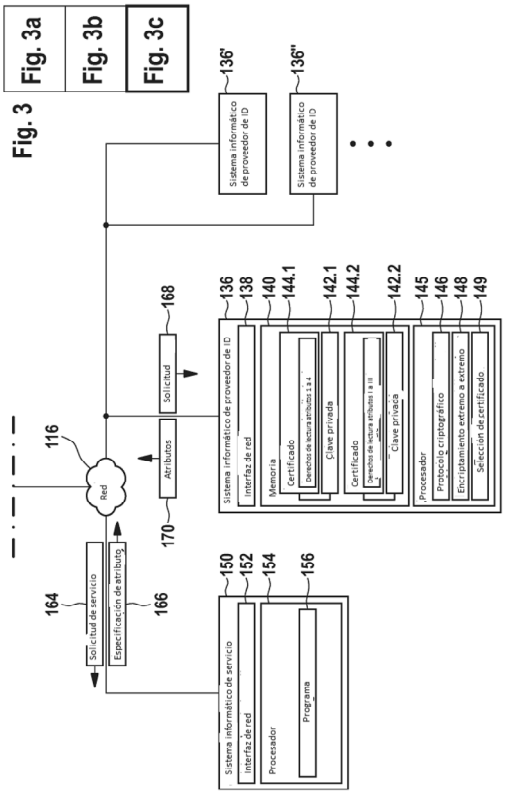


Fig. 3
Fig. 3a
Fig. 3b
Fig. 3c
136'
Sistema informático de proveedor de ID
136''
Sistema informático de proveedor de ID
168
Solicitud
Atributos
116
Red
170
164
Solicitud de servicio
Especificación de atributos
166
136
138
140
144.1
142.1
144.2
142.2
145
146
148
149
Sistema informático de proveedor de ID
Interfaz de red
Memoria
Certificado
Datos de lectura atributos 1 a i
Clave privada
Certificado
Datos de lectura atributos 1 a iii
Clave privada
Procesador
Protocolo criptográfico
Encriptamiento extremo a extremo
Selección de certificado
150
152
154
156
Sistema informático de servicio
Interfaz de red
Procesador
Programa

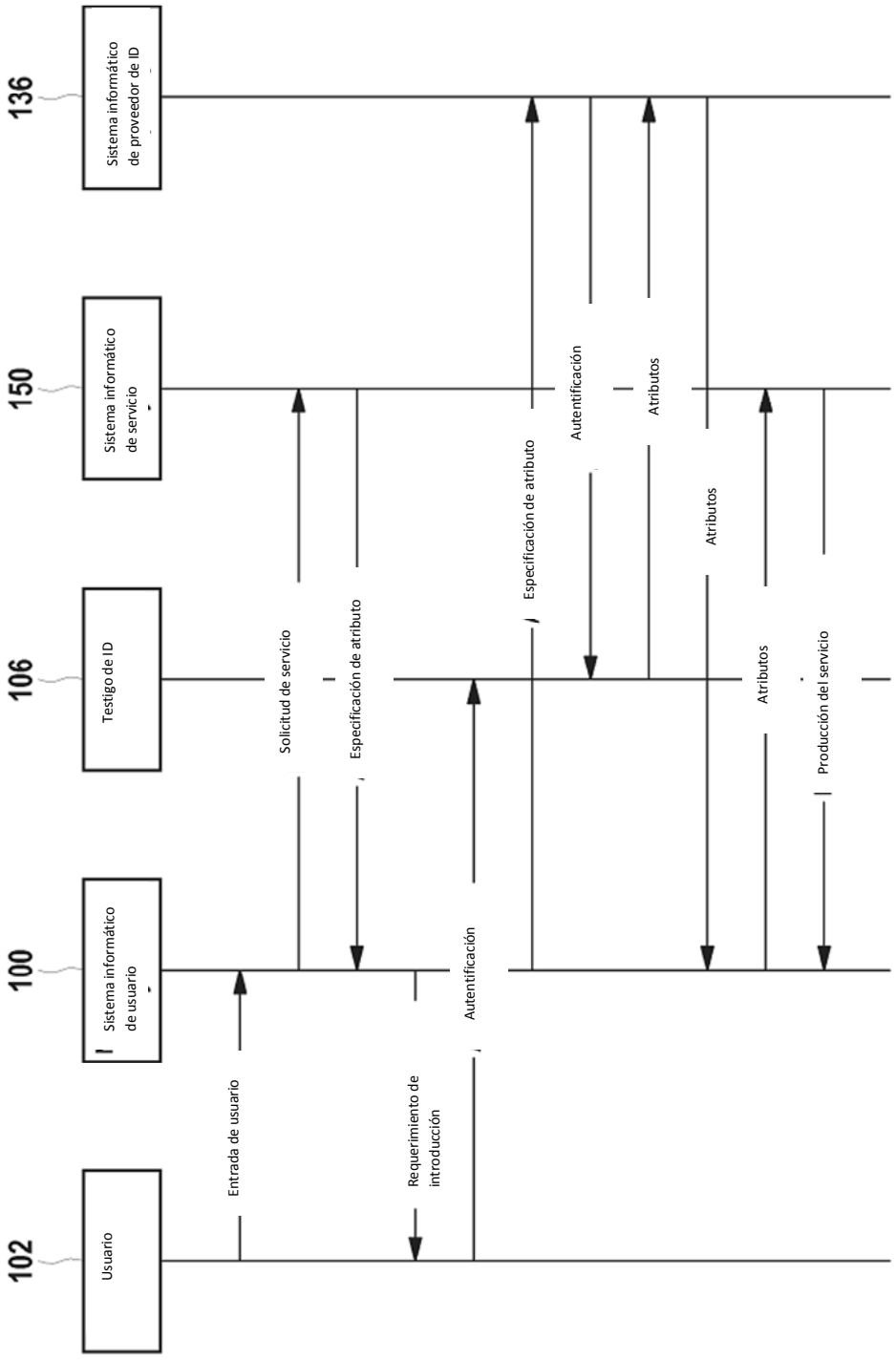

136
Sistema informático de proveedor de ID
150
Sistema informático de servicio
106
Testigo de ID
100
Sistema informático de usuario
102
Usuario
Entrada de usuario
Requerimiento de introducción
Autentificación
Solicitud de servicio
Especificación de atributo
Especificación de atributo
Autentificación
Atributos
Atributos
Atributos
Producción del servicio

Fig. 4