(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 714 177**

(51) Int. CI.:

G06F 21/34 (2013.01)
G06F 21/41 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.05.2009 PCT/EP2009/055666**

(87) Fecha y número de publicación internacional: **21.01.2010 WO10006822**

(96) Fecha de presentación y número de la solicitud europea: **11.05.2009 E 09779438 (2)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2018 EP 2304642**

(54) Título: **Procedimiento para leer atributos desde un código de identidad-ID**

(30) Prioridad:

15.07.2008 DE 102008040416

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.05.2019

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
Oranienstrasse 91
Berlin , DE

(72) Inventor/es:

DIETRICH, FRANK y
PAESCHKE, MANFRED

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCION

Procedimiento para leer atributos desde un código de identidad-ID

La invención se refiere a un procedimiento para la lectura de al menos un atributo desde un código de identidad-ID, a un producto de programa de ordenador, a un código de identidad-ID así como a un sistema de ordenador.

Se conocen a partir del 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 posibilitar a usuarios de Internet comunicar su identidad digital frente a servicios en línea. En este caso es un inconveniente, entre otros, que el usuario puede manipular su identidad digital.

En OPENID se trata, en cambio, de un sistema basado en servidor. Un llamado servidor de identidad almacena una base de datos con identidades digitales de los usuarios registrados. Aquí es un inconveniente, entre otros, una protección deficiente de los datos, puesto que las identidades digitales de los usuarios son almacenadas de forma centralizada y se puede registrar el comportamiento de los usuarios.

El documento "*An Implementer's Guide to the Identity Selector Interoperability Profile V1.0"; Abril de 2007, Microsoft Corporation und Ping Identity Corporatión*, publica un procedimiento para la autentificación de un usuario por medio de una Smartcard. El usuario es requerido en el curso de este procedimiento a introducir su Smartcard en un Selector de Identidad y a autentificarse con su PIN. A continuación, el Selector de Identidad utiliza un Certificado X.509 de la Smartcard, para autentificarse en otro servicio.

Se conoce a partir del documento US 2007/0294431 A1 otro procedimiento para la administración de las identidades digitales, que requiera igualmente un registro del usuario.

Se conoce a partir del documento US 2001/0045451 A1 un procedimiento basado en código de identidad para la autentificación de un usuario.

Se conoce a partir de la solicitud de patente DE102008000067.1 "Verfahren zum Lesen von Attributen aus einem ID-Token" no publicada en el momento de la solicitud de la misma solicitante un procedimiento, que posibilita a un sistema de ordenador del proveedor de ID leer uno o varios atributos desde el código de identidad-ID de un usuario para transmitirlos a un sistema de ordenador de servicio.

En cambio, la invención tiene el problema de crear un procedimiento mejorado para leer al menos un atributo, así como un producto de programa de ordenador correspondiente, un código de identidad-ID y un sistema de ordenador.

Los problemas en los que se basa la invención se solucionan, respectivamente, con las características de las reivindicaciones independientes de la patente. Formas de realización de la invención se indican en las reivindicaciones dependientes.

De acuerdo con formas de realización de la invención, se crea un procedimiento para leer al menos un atributo almacenado en un código de identidad-ID, en el que el código de identidad-ID está asociado a un usuario. El procedimiento contiene las siguientes etapas: emisión de una solicitud desde un cuarto sistema de ordenador del usuario a un segundo sistema de ordenador de servicio, especificación de uno o varios atributos a través del segundo sistema de ordenador de servicio, emisión de la especificación del atributo desde el segundo sistema de ordenador de servicio a un tercer sistema de ordenador, transmisión de la especificación del atributo desde e tercer sistema de ordenador a un primer sistema de ordenador, autentificación del usuario frente al código de identidad-ID, autentificación de un primer sistema de ordenador frente al código de identidad-ID, después de la autentificación con éxito del usuario y del primer sistema de ordenador frente al código de identidad-ID, acceso de lectura del primer sistema de ordenador al menos a un atributo almacenado en el código de identidad-ID, firma del al menos un atributo leído desde el código de identidad-ID a través del primer sistema de ordenador, transmisión del atributo firmado desde el primer sistema de ordenador al segundo sistema de ordenador de servicio, en el que la autentificación del primer sistema de ordenador (136') frente al código de identidad-ID se realiza en virtud de una autentificación del atributo (166, 168'), que recibe el primer sistema de ordenador desde un tercer sistema de ordenador (136), en el que la especificación del atributo especifica el al menos un atributo, en el que el acceso de lectura del primer sistema de ordenador se realiza para leer el uno o varios atributos, especificados en la especificación del atributo, desde el código de identidad-ID.

De esta manera se puede crear un "ancla de confianza".

La invención posibilita la lectura de uno o varios de los atributos almacenados en un código de identidad-ID a través del primer sistema de ordenador, en el que la conexión entre el código de identidad-ID y el primer sistema de ordenador se puede establecer a través de una red, en particular el Internet. En el al menos un atributo de puede

tratar de un dato con respecto a la identidad del usuario asociado al código de identidad-ID, en particular con respecto a su llamada identidad digital. Por ejemplo, a través del primer sistema de ordenador se leer los atributos nombre, apellidos, dirección, para transmitir estos atributos a un segundo sistema de ordenador, por ejemplo de un servicio en línea.

Pero también se puede leer, por ejemplo, sólo un único atributo, que no sirve para la determinación de la identidad del usuario, sino, por ejemplo, para la verificación de la autorización del usuario puesta la utilización de un servicio en línea determinado, como por ejemplo la edad del usuario, cuando éste quiere utilizar un servicio en línea, que está reservado para un grupo determinado de edad, u otro atributo, que documenta la pertenencia del usuario a un grupo determinado, que está autorizado para la utilización del servicio en línea.

En el código de identidad-ID se puede tratar de un aparato electrónico portátil, como por ejemplo una llamada memoria USB, o un documento, en particular un documento de valor o documento de seguridad.

Por un "Documento" se extienden de acuerdo con la invención documentos basados de papel y/o basados en plástico, como por ejemplo documentos de identidad, en particular pasaportes, documentos de identidad personal, Visa así como carnés de conducir, matriculaciones de vehículos, cartas de vehículos, tarjetas de identidad de empresa, tarjetas sanitarias y otros documentos de identidad, así como tarjetas de chip, medios de pago, en particular billetes de banco, tarjetas de banco y tarjetas de crédito u otras cartas de credenciales, en las que está integrada una memoria de datos para el registro de al menos un atributo.

Formas de realización de la invención son también especialmente ventajosa, puesto que el al menos un atributo se lee desde un documento especialmente de con fianza, por ejemplo un documento oficial. Además, es especialmente ventajoso que no es necesario un registro central de los atributos. La invención posibilita también una medida especialmente alta de confianza con respecto a la comunicación de los atributos que pertenecen a una identidad digital, unido con una protección óptima de los datos con una manipulación extraordinariamente cómoda.

Con respecto al código de identidad-ID, se definen primeras y segundas cantidades de sistemas de ordenador del proveedor de ID, que pueden estar constituidos, en principio, iguales, pero disponen de derechos diferentes: la primera cantidad de los sistemas de ordenador del proveedor de ID se define como de confianza para el segundo sistema de ordenador, pero no tiene derechos de lectura para la lectura del al menos un atributo desde el código de identidad-ID. En el segundo sistema de ordenador se trata, por ejemplo, de un sistema de ordenador de servicio, que sirve para la preparación de un servicio para los usuarios.

La segunda cantidad de sistemas de ordenador del proveedor de ID se define como de confianza con respecto al código de identidad-ID y/o al cuarto sistema de ordenador, es decir, el sistema de ordenador del usuario, tiene también derechos de lectura sobre el al menos un atributo del código de identidad-ID. A través de las primeras y segundas cantidades de sistemas de ordenador del proveedor de ID se definen aquí los llamados dominios de activación. Por ejemplo, el sistema de ordenador de servicio y el tercer sistema de ordenador pertenecen al mismo dominio de activación, en cambio el cuarto sistema de ordenador, es decir, el sistema de ordenador del usuario, y el primer sistema de ordenador pertenecen al otro dominio de activación diferente de aquél.

Al menos una cantidad parcial de la segunda cantidad de sistemas de ordenador del proveedor de ID se define, sin embargo, como de confianza para al menos una cantidad parcial de la primera cantidad de sistemas de ordenador del proveedor de ID, siendo las cantidades parciales, respectivamente, diferentes de la cantidad vacía.

Por lo tanto, cuando se recibe una especificación del atributo desde el sistema de ordenador de servicio a través del sistema de ordenador del usuario, entonces el sistema de ordenador del usuario transmite la especificación del atributo a un sistema de ordenador del proveedor de ID de la cantidad parcial de la primera cantidad. Este sistema de ordenador del proveedor de ID de la cantidad parcial de la primera cantidad transmite la especificación del atributo a un sistema de ordenador del proveedor de ID de la cantidad parcial de la segunda cantidad, que está clasificada como de confianza por el sistema de ordenador del proveedor de ID de la cantidad parcial de la primera cantidad.

El sistema de ordenador del proveedor de ID de la cantidad parcial de la segunda cantidad lee entonces después de la autentificación previa el al menos un atributo desde el código de identidad personal-ID. Por este sistema de ordenador del proveedor de ID de la cantidad parcial de la segunda cantidad se envía el al menos un atributo al sistema de ordenador del proveedor de ID de la cantidad parcial de la primera cantidad, desde donde se transmite el al menos un atributo al sistema de ordenador de servicio, Opcionalmente, el al menos un atributo es transmitido desde el sistema de ordenador del proveedor de ID de la cantidad parcial de la primera cantidad en primer lugar al sistema de ordenador del usuario, desde donde se transmite el al menos un atributo al sistema de ordenador de servicio.

Con preferencia, el al menos un atributo es enviado desde el sistema de ordenador del proveedor de ID de la cantidad parcial de la segunda cantidad en forma de un mensaje firmado al sistema de ordenador del proveedor de ID de la cantidad parcial de la primera cantidad. El sistema de ordenador del proveedor de ID de la cantidad parcial

de la primera cantidad puede verificar la firma. Cuando la firma es válida y se reconoce por un sistema de ordenador del proveedor de ID que pertenece a la cantidad parcial de la segunda cantidad, entonces el sistema de ordenador del proveedor de ID de la cantidad parcial de la primera cantidad firma, por su parte, el al menos un atributo y transmite un mensaje correspondiente al sistema de ordenador de servicio. El sistema de ordenador de servicio puede verificar entonces la validez de la firma y confiar en la autenticidad del al menos un atributo, puesto que la firma ha sido generada por el sistema de ordenador del proveedor de ID, clasificado como de confianza, de la cantidad parcial de la primera cantidad.

Formas de realización de la invención son especialmente ventajosas por que posibilitan un tráfico electrónico de derechos libre de interrupción de medios y asegurado en los derechos más allá de los límites de dominios de activación.

Formas de realización de la invención son, además, especialmente ventajosas, puesto que no es necesario un registro del usuario para la utilización del servicio proporcionado por el sistema de ordenador de servicio. En virtud del carácter "sin estado" de la capacidad de activación de ID aportada a través de los sistemas de ordenador del proveedor de ID, es decir, de la lectura del al menos un atributo, no es necesario que el usuario se haya autentificado previamente en uno de los sistemas de ordenador del proveedor de ID. En este caso, además, es especialmente ventajoso que en los sistemas de ordenador del proveedor de ID no deben almacenarse datos relacionados con el usuario.

De acuerdo con una forma de realización de la invención, el primer sistema de ordenador tiene al menos un certificado, que se utiliza para la autentificación del primer sistema de ordenador frente al código de identificación personal-ID. El certificado contiene un dato de aquellos atributos, para los que el primer sistema de ordenador tiene una autorización de lectura. El código de identidad personal-ID verifica con la ayuda de este certificado si el primer sistema de ordenador tiene la autorización de lectura necesaria para el acceso de lectura al atributo, antes de que se pueda realizar tal acceso de lectura a través del primer sistema de ordenador.

De acuerdo con una forma de realización de la invención, el primer sistema de ordenador envía el al menos un atributo leído desde el código de identificación personal-ID al tercer sistema de ordenador, que transmite el atributo leído al segundo sistema de ordenador. En el segundo sistema de ordenador se puede tratar, por ejemplo, de un servidor para la prestación de un servicio en línea o de otro servicio, como, por ejemplo, de una prestación de servicio bancario o para el encargo de un producto. Por ejemplo, un usuario puede abrir una cuenta en línea, a cuyo fin se transmiten atributos, que contienen la identidad del usuario, desde el primer sistema de ordenador al segundo sistema de ordenador de un banco.

De acuerdo con una forma de realización de la invención, la transmisión de los atributos leídos desde el código de identificación personal-ID se realiza desde el primer sistema de ordenador en primer lugar a un cuarto sistema de ordenador del usuario, es decir, el sistema de ordenador del usuario. Por ejemplo, el cuarto sistema de ordenador tiene un navegador de Internet habitual, con el que el usuario puede abrir una página Web del segundo sistema de ordenador. El usuario puede introducir en la página Web una solicitud o encargo de un servicio o un producto.

El segundo sistema de ordenador especifica a continuación aquellos atributos, por ejemplo del usuario o de su código de identidad personal-ID, que necesita para la prestación del servicio o para la aceptación del encargo. La especificación del atributo correspondiente, que contiene la especificación de estos atributos, se envía a continuación desde el segundo sistema de ordenador hasta el primer sistema de ordenador. Esto se puede realizar con o sin interconexión del cuarto sistema de ordenador. En el último caso, el usuario puede especificar el primer sistema de ordenador deseado frente al segundo sistema de ordenador, por ejemplo a través de la entrada de la URL del primer sistema de ordenador en una página Web del segundo sistema de ordenador desde el cuarto sistema de ordenador.

De acuerdo con una forma de realización de la invención, la solicitud de servicio del usuario al segundo sistema de ordenador contiene al dato de un identificador, de manera que el identificador identifica el primer sistema de ordenador. Por ejemplo, en el identificador se trata de un enlace, por ejemplo una URL del primer sistema de ordenador.

De acuerdo con una forma de realización de la invención, la especificación del atributo no se envía directamente desde el segundo sistema de ordenador al primer sistema de ordenador, sino que se envía primero desde el segundo sistema de ordenador al cuarto sistema de ordenador. El cuarto sistema de ordenador tiene varios conjuntos de datos de configuración predefinidos, 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 de ordenador de la segunda cantidad de sistemas de ordenador del proveedor de ID, en el que la especificación de tributo se transmite desde el segundo sistema de ordenador en primer lugar al cuatro sistema de ordenador, de modo que por medio del cuarto sistema de ordenador 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 del atributo, y en el que el cuarto ordenador transmite la especificación del atributo al primer sistema

de ordenador, y se establece la comunicación con el código de identificación personal-ID especificado a través de la indicación de la fuente de datos en el conjunto de datos de configuración seleccionado.

De acuerdo con una forma de realización de la invención, los atributos leídos desde el código de identidad personal-ID son firmados por el primer sistema de ordenador y entonces son enviados al tercer sistema de ordenador. Desde el tercer sistema de ordenador se transmiten los atributos entonces al cuarto sistema de ordenador. El usuario del cuarto sistema de ordenador puede leer, por lo tanto, los atributos, pero sin poder modificarlos. Sólo después de la liberación a través de usuario, se transmiten los atributos desde el cuarto sistema de ordenador al segundo sistema de ordenador.

De acuerdo con una forma de realización de la invención, el usuario puede completar los atributos antes de su transmisión a través de otros datos.

De acuerdo con una forma de realización de la invención, el primer sistema de ordenador tiene varios certificados con diferentes derechos de lectura. En virtud de la recepción de la especificación del atributo, el primer sistema de ordenador selecciona uno o varios de estos certificados, para leer los atributos correspondientes desde el código de identificación personal-ID o varios códigos de identificación personal-ID.

De acuerdo con una forma de realización de la invención, el cuarto sistema de ordenador tiene al menos un conjunto de datos de configuración, que especifica una fuente de datos externa para la consulta de otro atributo desde el cuarto sistema de ordenador a través de la red.

De acuerdo con una forma de realización de la invención, la consulta del otro atributo se realiza después de que ha sido leído el al menos un atributo del código de identidad personal-ID, y después de que el cuarto sistema de ordenador ha recibido el al menos un atributo desde el primer sistema de ordenador, en el que la consulta contiene el al menos un atributo.

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

En otro aspecto, la invención se refiere a un código de identificación personal con una zona de memoria asegurada para el almacenamiento de al menos un atributo y de al menos un identificador de un primer sistema de ordenador, con medios para la autentificación de un usuario asociado al código de identidad personal-ID frente al código de identidad personal-ID, medios para autentificación de un primer sistema de ordenador frente al código de identidad personal-ID, medios para el establecimiento de una comunicación protegida con el primer sistema de ordenador, a través del cual el primer sistema de ordenador puede leer el al menos un atributo, en el que una condición previa necesaria para la lectura del al menos un atributo desde el código de identidad personal-ID a través del primer sistema de ordenador es la autentificación con éxito del usuario y del primer sistema de ordenador frente al código de identidad personal-ID.

Según formas de realización de la invención, a través del o de los identificadores se define la segunda cantidad de sistemas de ordenador del proveedor de ID.

Adicionalmente a la autentificación del primer sistema de ordenador frente al código de identidad personal-ID, como se conoce en sí, por ejemplo, como el llamado Control de Acceso Extendido para documentos de viaje legibles con máquina (machine-readable travel documents - MRTD) y se especifica por las Autoridades Aeronáuticas Internacionales ICAO, el usuario debe autentificarse, por lo tanto, frente al código de identidad personal-ID. Por ejemplo, a través de una autentificación con éxito del usuario frente al código de identidad personal-ID, éste se libera, de manera que se pueden ejecutar las otras etapas, a saber, la autentificación del primer sistema de ordenador frente al código de identidad personal-ID y/o el establecimiento de una comunicación protegida para la lectura de los atributos.

De acuerdo con una forma de realización de la invención, el código de identidad personal-ID tiene medios para la codificación de fin-a-fin. Esto posibilita establecer la comunicación entre el código de identidad personal-ID y el primer sistema de ordenador a través de un tercer sistema de ordenador del usuario, puesto que el usuario, en virtud de la codificación de fin-a-fin, no puede realizar modificaciones de los datos transmitidos a través de la comunicación.

De acuerdo con una forma de realización de la invención, el código de identidad personal-ID contiene medios para la codificación de fin-a-fin de la comunicación para la transmisión protegida de al menos uno de los atributos hacia el primer sistema de ordenador, en el que en el código de identidad personal-ID se trata con preferencia de un aparato electrónico, en particular una memoria USB, o un documento, en particular un documento de valor o un documento de seguridad.

En otro aspecto, la invención se refiere a un primer sistema de ordenador con medios para la recepción de una

especificación de atributos a través de una red desde un sistema de ordenador (136) no autorizado, en el que la especificación del atributo especifica al menos un atributo, medios para la autentificación frente a un código de identidad personal-ID, medios para la lectura de al menos un atributo desde el código de identidad personal-ID a través de una comunicación asegurada, en el que la lectura del al menos un atributo presupone que un usuario asociado al código de identidad personal-ID se haya autentificado frente al código de identidad personal-ID, y medios para la transmisión del al menos un atributo al sistema de ordenador no autorizado.

De acuerdo con una forma de realización de la invención, en el sistema de ordenador no autorizado se trata de un sistema de ordenador del proveedor de ID de la primera cantidad, en particular del tercer sistema de ordenador.

De acuerdo con una forma de realización de la invención, el primer sistema de ordenador puede contener medios para la generación de una demanda al usuario. Después de que el primer sistema de ordenador ha recibido la especificación del atributo, por ejemplo, desde el segundo sistema de ordenador a través del tercer sistema de ordenador, envía a continuación la demanda al cuarto sistema de ordenador del usuario, de manera que el usuario es requerido para que se autentifique frente al código de identidad personal-ID. Después de que se ha realizado con éxito la autentificación del usuario frente al código de identidad personal-ID, el primer sistema de ordenador recibe una confirmación desde el cuarto sistema de ordenador. A continuación, el primer sistema de ordenador se autentifica frente al código de identidad personal-ID y se establece una comunicación segura entre el código de identidad personal-ID y el primer sistema de ordenador con una codificación de fin-a-fin.

De acuerdo con una forma de realización de la invención, el primer sistema de ordenador tiene varios certificados que especifican, respectivamente, diferentes derechos de lectura. Después de la recepción de la especificación de atributos, el primer sistema de ordenador selecciona al menos uno de estos certificados con los derechos de lectura suficientes para la lectura de los atributos especificados.

Formas de realización del primer sistema de ordenados de acuerdo con la invención son especialmente ventajosas, puesto que forman en combinación con la necesidad de la autentificación del usuario frente al código de identidad personal-ID un ancla de confianza para la identidad digital no falsificada del usuario. En este caso es especialmente ventajoso que esto no requiere ningún registro previo del usuario frente al sistema de ordenador, así como tampoco ningún almacenamiento central de los atributos que forman las identidades digitales.

De acuerdo con una forma de realización de la invención, el primer sistema de ordenador recibe junto con la especificación del atributo un identificador del segundo sistema de ordenador. Con la ayuda del identificador, el sistema de ordenador identifica el segundo sistema de ordenador, que quiere utilizar los servicios de identificación, para cobrar por esta prestación de servicio frente al segundo sistema de ordenador. De manera alternativa o adicional, el primer sistema de ordenador recibe junto con la especificación del atributo un identificador del tercer sistema de ordenador. Con la ayuda del identificador, el sistema de ordenador identifica el tercer sistema de ordenador, que quiere utilizar los servicios de identificación, para cobrar por esta prestación de servicio frente al tercer sistema de ordenador. El tercer sistema de ordenador puede cargar estas cuotas al segundo sistema de ordenador, es decir, al prestador del servicio.

De acuerdo con una forma de realización de la invención, en el sistema de ordenador se trata de un Centro de Confianza certificado por las autoridades, en particular, un Centro de Confianza conforme a la Ley de Firmas

Por lo demás, se explican en detalle formas de realización de la invención con referencia a los dibujos. En este caso:

La figura 1 muestra un diagrama de bloques de una primera forma de realización de sistemas de ordenador de acuerdo con la invención y de un código de identidad personal-ID de acuerdo con la invención.

La figura 2 muestra un diagrama de flujo de una forma de realización de un procedimiento de acuerdo con la invención.

La figura 3 muestra un diagrama de bloques de otras formas de realización de sistemas de ordenador de acuerdo con la invención.

La figura 4 muestra un diagrama-UML de otra forma de realización de un procedimiento de acuerdo con la invención.

Los elementos de las siguientes formas de realización, que se corresponden entre sí, se identifican con los mismos signos de referencia.

La figura 1 muestra un sistema de ordenador del usuario 100 de un usuario 102. En el sistema de ordenador del usuario 100 se puede tratar de un ordenador personal, un ordenador portátil como, por ejemplo un Laptop o Palmtop, un Asistente Digital Personal, un aparato de telecomunicaciones, en particular un Smart Phone o similar. El sistema de ordenador del usuario 100 tiene una interfaz 104 para la comunicación con un código de identidad personal-ID 106, que presenta una interfaz 108 correspondiente.

El sistema de ordenador del usuario 100 tiene al menos un procesador 110 para la ejecución de instrucciones de

programa 112 así como una interfaz de la red 114 para la comunicación a través de una red 116. En la red se puede tratar de una red de ordenador, como por ejemplo el Internet.

El código de identidad personal-ID 106 tiene una memoria electrónica 118 con zonas de memoria 120, 122 y 124 protegidas. La zona de memoria 120 protegida sirve para el almacenamiento de un valor de referencia, que se necesita para la autentificación del usuario 102 frente al código de identidad personal-ID 106. En este valor de referencia se trata, por ejemplo, de una identificación, en particular un llamado Número de Identificación Personal (PIN), o de datos de referencia para una característica biométrica del usuario 102, que se puede utilizar para la autentificación del usuario frente al código de identidad personal-ID 106.

La zona protegida 122 sirve para el almacenamiento de una clave privada y la zona protegida de la memoria 124 sirve para el almacenamiento de atributos, por ejemplo del usuario 102, como por ejemplo su nombre, domicilio, fecha de nacimiento, sexo y/o de atributos, que se refieren al propio código de identidad personal-ID, como por ejemplo la institución, que crea o ha emitido el código de identidad personal-ID, la duración de la validez del código de identidad personal-ID, un identificador del código de identidad personal-ID, como por ejemplo un número de paso o un número de tarjeta de crédito.

La memoria electrónica 118 puede presentar, además, una zona de memoria 126 para el almacenamiento de un certificado. El certificado contiene una clave pública, que está asociada a la clave privada almacenada en la zona protegida de la memoria 122. El certificado puede haber sido creado de acuerdo con una Norma de Infraestructura de Clave Pública (PKI), por ejemplo según la Norma X.509.

El certificado no tiene que estar almacenado forzosamente en la memoria electrónica 118 del código de identidad personal-ID 106. De manera alternativa o adicional, el certificado puede estar almacenado también en un servidor de índices público.

El código de identidad personal-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 autentificación del usuario, es decir, para la autentificación del usuario 102 frente al código de identidad personal-ID.

El código de identidad personal-ID puede presentar una zona de memoria (no mostrada en la figura 1), que sirve para el almacenamiento de al menos un identificador para la identificación de un sistema de ordenador del proveedor de ID de la segunda cantidad. Al menos una cantidad parcial de la segunda cantidad de los sistemas de ordenador del proveedor está definida como de confianza con respecto al sistema de ordenador de servicio 150, pero está autorizada para la lectura con respecto al código de identidad personal-ID 106 al menos con relación a uno de los atributos.

En una forma de realización con PIN, el usuario 102 introduce su PIN para su autentificación en el código de identidad personal-ID 106, por ejemplo a través del sistema de ordenador del usuario 100. Por medio de la ejecución de las instrucciones de programa 130 se accede entonces a la zona protegida de la memoria 120, para comparar el PIN introducido con el valor de referencia del PIN almacenado allí. Para el caso de que el PIN introducido coincida con el valor de referencia del PIN, el usuario 102 vale como autentificado.

De manera alternativa, se registra una característica biométrica del usuario 102, Por ejemplo, el código de identidad personal-ID 106 tiene a tal fin un sensor de huella dactilar o un sensor de huella dactilar está conectado en el sistema de ordenador del usuario 100. Los datos biométricos registrados del usuario 102 son comparados con los datos biométricos de referencia almacenados en la zona protegida de la memoria 120, ejecutando las instrucciones del programa 130 según esta forma de realización. En el caso de coincidencia suficiente de los datos biométricos registrados del usuario 102 con los datos biométricos de referencia, el usuario 102 vale como autentificado.

Las instrucciones del programa 134 sirven para la ejecución de las etapas, relacionadas con el código de identidad personal-ID 106, de un protocolo criptográfico para la autentificación de un sistema de ordenador del proveedor de ID 136 frente al código de identidad personal-ID 106. En el protocolo criptográfico se puede tratar de un Protocolo de Desafío-Respuesta sobre la base de una clave simétrica o de una pareja de claves asimétricas.

Por ejemplo, a través del protocolo criptográfico se implementa un procedimiento de Control de Acceso Extendido, como está especificado para documentos de viaje legibles con máquina (machine-readable travel documents - MRTD) por las Autoridades Aeronáuticas Internacionales (ICAO). A través de la ejecución con éxito del protocolo criptográfico se autentifica el sistema de ordenador del proveedor de ID 136 frente al código de identidad personal-ID y prueba de esta manera su autorización para la lectura de los atributos almacenados en la zona protegida de la memoria 124. La autentificación puede ser en este caso mutua, es decir, que también el código de identidad personal-ID 106 debe autentificarse entonces frente al sistema de ordenador del proveedor 136 de acuerdo con el mismo u otro protocolo criptográfico.

Las instrucciones de programa 132 sirven para la codificación de fin-a-fin de datos transmitidos entre el código de identidad personal-ID 106 y el sistema de ordenador del proveedor 136, pero al menos de los atributos leídos por el

sistema de ordenador del proveedor 136 desde la zona protegida de la memoria 124. Para la codificación de fin-a-fin se puede utilizar una clave simétrica, que se acuerda, por ejemplo, con motivo de la ejecución del protocolo criptográfico entre el código de identidad personal-ID 106 y el sistema de ordenador del proveedor de ID 136.

De manera alternativa a la forma de realización representada en la figura 1, el sistema de ordenador del usuario 100 no se puede comunicar con su interfaz 104 directamente con la interfaz 108, sino a través de un aparato de lectura, conectado en la interfaz 104 para el código de identidad personal-ID 106. A través de este aparato de lectura, como por ejemplo un llamado terminal de tarjetas de chip de clase 2, se puede realizar también la entrada del PIN.

El sistema de ordenador del proveedor 136 tiene una interfaz de la red 138 para la comunicación a través de la red 116. El sistema de ordenador del proveedor de ID 136 tiene, además, una memoria 140, en la que está almacenada una clave privada 142 del sistema de ordenador del proveedor de ID 136 así como el certificado 144 correspondiente. También en este certificado de puede tratar, por ejemplo, de un certificado de acuerdo con una Norma-PKI, como, por ejemplo, X.509.

El sistema de ordenador del proveedor de ID 136 tiene, además, un procesador 145 para la ejecución de instrucciones de programa 146 y 148. A través de la ejecución de las instrucciones de programa 146 se ejecutan las etapas, relacionadas con el sistema de ordenador del proveedor de ID 136, del protocolo criptográfico. En general, por lo tanto, el protocolo criptográfico se implementa a través de la ejecución de instrucciones de programa 134 por medio del procesador 128 del código de identidad personal-ID 106 así como a través de la ejecución de las instrucciones de programa 146 por medio del procesador 145 del sistema de ordenador del proveedor de ID 136.

Las instrucciones de programa 148 sirven para la implementación de la codificación de fin-a-fin por parte del sistema de ordenador del proveedor de ID 136, por ejemplo sobre la base de la clave simétrica, que ha sido acordada con motivo de la ejecución del protocolo criptográfico entre el código de identidad personal-ID 106 y el sistema de ordenador del proveedor de ID 136. En principio, se puede utilizar cualquier procedimiento conocido anteriormente en sí para convenir la clave simétrica para la codificación de fin-a-fin, como por ejemplo un intercambio de claves de Diffie-Hellman.

El sistema de ordenador del proveedor de ID 136 se encuentra con preferencia en un entorno especialmente protegido, en particular en un llamado Centro de Confianza, de manera que el sistema de ordenador del proveedor de ID 136 forma en combinación con la necesidad de la autentificación del usuario 102 frente al código de identidad personal-ID 106 el ancla de confianza para la autenticidad de los atributos leídos desde el código de identidad personal-ID 106.

El sistema de ordenador de servicio 150 puede estar configurado para la recepción de una petición o de un encargo para una prestación de servicio o un producto, en particular una prestación de servicio en línea. Por ejemplo, el usuario 102 puede abrir en línea a través de la red 116 una cuenta en un banco o utilizar otra prestación financiera o de servicio bancario. El sistema de ordenador de servicio 150 puede estar configurado también como centro comercial en línea, de manera que el usuario 102 puede adquirir, por ejemplo en línea un teléfono móvil o similar. Además, el sistema de ordenador de servicio 150 puede estar configurado también para el suministro de contenidos digitales, por ejemplo para la descarga de datos de música y/o de vídeo.

El sistema de ordenador de servicio 150 tiene a tal fin una interfaz de red 152 para la comunicación con la red 116. Además, el sistema de ordenador de servicio 150 tiene al menos un procesador 154 para la ejecución de instrucciones de programa 156. A través de la ejecución de las instrucciones de programa 156 se generan, por ejemplo, páginas-HTML dinámicas, a través de las cuales el usuario 102 puede introducir su encargo o su petición.

De acuerdo con el tipo de producto encargado o pedido o de la prestación de servicio, el sistema de ordenador de servicio 150 debe verificar uno o varios atributos del usuario 102 y/o de su código de identidad personal-ID 106 con la ayuda de uno o varios criterios predeterminados. Solamente cuando se supera esta verificación, se recibe y/o se ejecuta el pedido o el encargo del usuario 102.

Por ejemplo, para la apertura de una cuenta bancaria o la compra de un teléfono móvil con el contrato correspondiente es necesario que el usuario 102 publique su identidad frente al sistema de ordenador de servicio 150 y que se verifique esta identidad. En el estado de la técnica, el usuario 102 debe presentar a tal fin, por ejemplo, su carné de identidad. Este proceso se sustituye por la lectura de la identidad digital del usuario 102 desde su código de identidad personal-ID 106.

Pero de acuerdo con el caso de aplicación, el usuario 102 no debe publicar su identidad frente al servicio de ordenador de servicio 150, sino que es suficiente una comunicación, por ejemplo de uno de los atributos. Por ejemplo, el usuario 102 puede aportar a través de uno de sus atributos una prueba de que pertenece a un grupo determinado de personas, que está autorizado para datos preparados para la descarga en el sistema de ordenador de servicio 150. 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 proporcionado por el sistema de ordenador de servicio 150 se procede de la siguiente manera:

1. Autentificación del usuario 102 frente al código de identidad personal-ID 106.

El usuario 102 se autentifica frente al código de identidad personal-ID 106. En el caso de una implementación con PIN, el usuario 102 introduce a tal fin su PIN, por ejemplo a través del sistema de ordenador del usuario 100 o a través de un terminal de tarjetas de chip conectado en él. A través de la ejecución de las instrucciones de programa 130, el código de identidad personal-ID 106 verifica entonces la corrección del PIN introducido. Cuando el PIN introducido coincide con valor de referencia del PIN almacenado en la zona protegida de la memoria 120, el usuario 102 vale como autentificado. De manera similar se procede cuando se utiliza una característica biométrica del usuario 102 para su autentificación, como se ha descrito anteriormente.

2. Autentificación del sistema de ordenador del proveedor de ID 136 frente al código de identidad personal-ID 106.

A tal fin, se establece una comunicación entre el código de identidad personal-ID 106 y el sistema de ordenador del proveedor de ID 136 a través del sistema de ordenador del usuario 100 y la red 116. Por ejemplo, el sistema de ordenador del proveedor de ID 136 transmite su certificado 144 a través de esta comunicación al código de identidad personal-ID 106. A través de las instrucciones de programa 134 se genera entonces un llamado desafío, es decir, por ejemplo un número aleatorio. Este número aleatorio se codifica con la clave pública contenida en el certificado 144 del sistema de ordenador del proveedor de ID 136. El cifrado resultante se envía desde el código de identidad personal-ID 106 a través de la comunicación hasta el sistema de ordenador del proveedor de ID 136. El sistema de ordenador del proveedor de ID 136 descodifica el cifrado con la ayuda de su clave privada 142 y recibe de esta manera el número aleatorio. El número aleatorio es devuelto por el sistema de ordenador del proveedor de ID 136 a través de la comunicación al código de identidad personal-ID 106. A través de la ejecución de las instrucciones de programa 134 se verifica allí si el número aleatorio recibido desde el sistema de ordenador del proveedor 136 coincide con el número aleatorio generado originalmente, es decir, el desafío. Si éste es el caso, entonces el sistema de ordenador del proveedor de ID 136 vale como autentificado frente al código de identidad personal-ID 106. El número aleatorio se puede utilizar como clave simétrica para la codificación de fin-a-fin.

3. Después de que el usuario 102 se ha autentificado con éxito frente al código de identidad personal-ID 106, y después de que el sistema de ordenador del proveedor de ID 136 se ha autentificado con éxito frente al código de identidad personal-ID 106, el sistema de ordenador del proveedor de ID 136 recibe una autorización de lectura para la lectura de uno, varios o todos los atributos memorizados en la zona protegida de la memoria 124, En virtud de un comando de lectura correspondiente, que el sistema de ordenador del proveedor de ID 136 emite a través de la comunicación al código de identidad personal-ID 106, se leen los atributos solicitados desde la zona protegida de la memoria 124 y se codifican a través de la ejecución de las instrucciones de programa 132. Los atributos codificados son transmitidos a través de la comunicación al sistema de ordenador del proveedor de ID 136 y allí son descodificados a través de la ejecución de las instrucciones de programa 148. De esta manera, el sistema de ordenador del proveedor de ID 136 recibe conocimiento de los atributos leídos desde el código de identidad personal-ID 106.

Estos atributos son firmados por el sistema de ordenador del proveedor de ID con la ayuda de su certificado 144 y son transmitidos a través del sistema de ordenador del usuario 100 o directamente al sistema de ordenador de servicio 150. De esta manera se ponen en conocimiento del sistema de ordenador de servicio 150 los atributos leídos desde el código de identidad personal-ID 106, de manera que el sistema de ordenador de servicio 150 puede verificar estos atributos con la ayuda de uno o varios de los criterios predeterminados, para prestar a continuación, dado el caso, el servicio solicitado por el usuario 102.

A través de la necesidad de la autentificación del usuario 102 frente al código de identidad personal-ID 106 y de la autentificación del sistema de ordenador del proveedor de ID 136 frente al código de identidad personal-ID 106 se crea el ancla de confianza necesaria, de manera que el sistema de ordenador de servicio 150 puede estar seguro de que los atributos del usuario 102 que le han sido comunicados por el sistema de ordenador del proveedor de ID 136 son pertinentes y no están falsificados.

De acuerdo con la forma de realización, la secuencia de la autentificación puede ser diferente, Por ejemplo, puede estar previsto que deba autentificarse en primer lugar el usuario 102 frente al código de identidad personal-ID 106 y a continuación el sistema de ordenador del proveedor de ID 136. Pero, en principio, también es posible que deba autentificarse en primer lugar el sistema de ordenador del proveedor de ID 136 frente al código de identidad personal-ID 106 y sólo a continuación el usuario 102.

En el primer caso, el código de identidad personal-ID 106 está configurado, por ejemplo, para que sólo se libere a través de la entrada de un PIN correcto o de una característica biométrica correcta a través del usuario 102. Sólo esta liberación posibilita el inicio de las instrucciones del programa 132 y 134 y con ello la autentificación del sistema de ordenador del proveedor 136.

En el segundo caso, es posible un inicio de las instrucciones del programa 132 y 134 también ya cuando el usuario 102 no se ha autentificado todavía frente al código de identidad personal-ID 106. En este caso, por ejemplo, las instrucciones del programa 134 están configuradas de tal forma que el sistema de ordenador del proveedor 136 sólo puede ejecutar un acceso de lectura a la zona protegida de la memoria 124 para la lectura de uno o varios de los atributos después de que ha sido firmada por las instrucciones del programa 130 la autentificación con éxito también del usuario 102.

Es especialmente ventajosa la utilización del código de identidad personal-ID 106, por ejemplo, para comercio electrónico y gobierno electrónico y, en concreto, libre de interrupción de medios y asegurado en los derechos en virtud del ancla de confianza formada a través de la necesidad de la autentificación del usuario 102 y del sistema de orden ador del proveedor 136 frente al código de identidad personal-ID 106. Además, es especialmente ventajoso que no sea necesario un almacenamiento central de los atributos de diferentes usuarios 102, de manera que con ello se solucionan los problemas de protección de datos que existen en el estado de la técnica. Por lo que se refiere a la comodidad de la aplicación del procedimiento, es especialmente ventajoso que no sea necesario un registro previo del usuario 102 para la utilización del sistema de ordenador del proveedor de ID 136.

En la forma de realización considerada aquí, no está almacenado ningún identificador para el sistema de ordenador del proveedor de ID 136 en la memoria del código de identidad personal-ID. De manera correspondiente, el sistema de ordenador del proveedor de ID 136 tampoco dispone de derechos de lectura para la lectura de los atributos desde el código de identidad personal-ID. Sin embargo, en la memoria del código de identidad personal-ID está almacenado un identificador para un sistema de ordenador del proveedor de ID 136' (véase la figura 3), que está constituido, en principio, igual que el sistema de ordenador del proveedor de ID 136 y dispone de derechos de lectura para la lectura de los atributos desde el código de identidad personal-ID.

La figura 2 muestra una forma de realización de un procedimiento de acuerdo con la invención. En la etapa 200 se envía una solicitud de servicio desde el sistema de ordenador del usuario hasta el sistema de ordenador de servicio. Por ejemplo, el usuario inicia a tal fin un navegador de Internet del sistema de ordenador del usuario e introduce una URL para la llamada de una página Web del servicio de ordenador del usuario. En la página Web llamada el usuario introduce entonces su solicitud de servicio, por ejemplo el pedido o concesión de encargo para un servicio o un producto.

En la etapa 202 el sistema de ordenador del usuario 150 especifica a continuación uno o varios atributos, que necesita para verificar la autorización del usuario para la solicitud del servicio. En particular, el sistema de ordenador del usuario puede especificar aquellos atributos que determinan la identidad digital del usuario 102. Esta especificación de los atributos a través del sistema de ordenador del usuario 150 puede estar prevista fijamente o se puede determinar de acuerdo con la solicitud del servicio en el caso individual a través del sistema de ordenador de servicio 150 con la ayuda de reglas predeterminadas.

En la etapa 204 se transmite la especificación del atributo, es decir, la especificación realizada en la etapa 202 de uno o varios de los atributos, desde el sistema de ordenador de servicio al sistema de ordenador del proveedor de ID y, en concreto, o bien directamente o a través del sistema de ordenador del usuario.

Para dar al sistema de ordenador del proveedor de ID la posibilidad de leer atributos desde su código de identidad personal-ID, el usuario se autentifica en la etapa 206 frente al código de identidad personal-ID.

En la etapa 208 se establece una comunicación entre el código de identidad personal-ID y el sistema de ordenador del proveedor de ID. En este caso, se trata con preferencia de una comunicación asegurada, por ejemplo de un llamado procedimiento de Mensaje Seguro.

En la etapa 210 se realiza al menos una autentificación del sistema de ordenador de proveedor de ID frente al código de identidad personal-ID a través de la comunicación establecida en la etapa 208. Adicionalmente, puede estar prevista también la autentificación del código de identidad personal-ID frente al sistema de ordenador del proveedor de ID.

Después de que tanto el usuario como también el sistema de ordenador del proveedor de ID han sido autentificados con éxito frente al código de identidad personal-ID, el sistema de ordenador del proveedor de ID recibe, en efecto, desde el código de identidad personal-ID la autorización de acceso para la lectura de los atributos. En la etapa 212, el sistema de ordenador del proveedor de ID envía uno o varios comandos de lectura para la lectura de los atributos necesarios de acuerdo con la especificación de atributos desde el código de identidad personal-ID. Los atributos son transmitidos entonces por medio de codificación de fin-a-fin a través de la comunicación asegurada al sistema de ordenador del proveedor de ID y son descodificados allí.

Los valores de los atributos leídos son firmados en la etapa 214 por el sistema de ordenador del proveedor de ID. En la etapa 216, el sistema de ordenador del proveedor de ID envía los valores de los atributos firmados a través de la red. Los valores de los atributos firmados llegan al sistema de ordenador de servicio o bien directamente o a través del sistema de ordenador del usuario, En el último caso, el usuario puede tener la posibilidad de tomar conocimiento

de los valores de los atributos firmados y/o de completarlos con otros datos. Puede estar previsto que los valores de los atributos firmados sean transmitidos, dado el caso, con los datos completados sólo después de la liberación a través del usuario desde el sistema de ordenador del usuario al sistema de ordenador de servicio. De esta manera, se establece la transparencia máxima posible para el usuario con respecto a los atributos enviados desde el sistema de ordenador del proveedor de ID hasta el sistema de ordenador de servicio.

Cuando el sistema de ordenador del proveedor de ID pertenece a una cantidad de corte de la primera y de la segunda cantidades, no es necesaria ninguna otra acción, puesto que tal sistema de ordenador del proveedor de ID pertenece a ambos dominios de actuación. Cuando éste no es el caso, se envía la especificación del atributo en la etapa 204 a un sistema de ordenador del proveedor de ID de la primera cantidad y desde allí se transmite a un sistema de ordenador del proveedor de ID de la segunda cantidad. A través del sistema de ordenador del proveedor de ID de la segunda cantidad se ejecutan entonces las etapas 208 a 216. La emisión de los valores de los atributos firmados desde el sistema de ordenador del proveedor de ID de la segunda cantidad al sistema de ordenador de servicio se puede realizar a través del sistema de ordenador del proveedor de ID de la primera cantidad.

La figura 3 muestra otras formas de realización de un código de identidad personal-ID de acuerdo con la invención y otros sistemas de ordenador de acuerdo con la invención. En la forma de realización de la figura 3, el código de identidad personal-ID 106 está configurado como documentos, como por ejemplo como documento a base de papel y/o a base de plástico con un circuito electrónico integrado, a través del cual se forman la interfaz 108, la memoria 118 y el procesador 128. En el circuito electrónico integrado se puede tratar, por ejemplo de una llama da etiqueta de radio, que se puede designar como etiqueta-RFID o marcador-RFID. Pero la interfaz 108 puede estar configurada también como interfaz de contacto como la llamada Interfaz de Modo Dual.

En particular, en el documento 106 se puede tratar de un documento de valor o documento de seguridad, como por ejemplo de un documento de viaje legible con máquina (MRTD), como por ejemplo un pase de viaje electrónico o de un carné personal electrónico, o de un medio de pago, como por ejemplo una tarjeta de crédito.

En la zona protegida de la memoria 124, en la forma de realización considerada aquí, están almacenados los atributos i, siendo $1 \leq i \leq n$. Por lo demás, se parte, sin limitación de la generalidad, que en el código de identidad personal-ID 106 mostrado de forma ejemplar en la figura 3 se trata de un carné de identidad personal electrónico. Por ejemplo, en el atributo i = 1 se trata del nombre, en el atributo i = 2 se trata de los apellidos, en el atributo i = 3 de trata de la dirección y en el atributo i = 4 se trata de la fecha de nacimiento, etc.

La interfaz 104 del sistema de ordenador del usuario 100 puede estar configurada en la forma de realización considerada aquí como aparato de lectura RFID o puede estar conectada como componente separado en éste.

El usuario 102 dispone de uno u otros varios códigos de identidad personal-ID, que pueden estar constituidos, en principio, iguales, como por ejemplo un código de identidad personal-ID 106', en el que se trata de una tarjeta de crédito.

En el sistema de ordenador del usuario 100 pueden estar almacenados varios conjuntos de datos de configuración 158, 160 … Cada uno de los conjuntos de datos de configuración indica para una cantidad determinada de atributos una fuente de datos y un sistema de ordenador del proveedor, que tiene derechos de lectura para la lectura de la fuente de datos especificada. En este sistema de ordenador del proveedor de ID se trata, por lo tanto, de sistemas de ordenador del proveedor de ID de la segunda cantidad.

En la forma de realización considerada aquí, el sistema de ordenador del usuario 100 activar a través de la red 116 diferentes sistemas de ordenador del proveedor de ID 136, 136', 136''..., que pueden pertenecer a diferentes llamados Centros de Confianza. Por ejemplo, el sistema de ordenador del proveedor de ID 136 pertenece al Centro de Confianza A y el sistema de ordenador del proveedor de ID 136' estructurado, en principio, igual pertenece a otro Centro de Confianza B y el sistema de ordenador del proveedor de ID 136'' pertenece a otro Centro de Confianza C. Los sistemas de ordenador del proveedor de ID 136, 136', 136'' pueden estar constituidos, en principio, iguales, tal como se explica en detalle con relación al sistema de ordenador del proveedor de ID 136. Los sistemas de ordenador del proveedor de ID 136, 136', 136'' se pueden distinguir, sin embargo, con respecto a los derechos de lectura sobre los atributos almacenados en los códigos de identidad personal-ID 106, 106', tal como es el caso en la forma de realización considerada aquí.

En el conjunto de datos de configuración 158, que se designa también como contenedor de ID, se define la cantidad de los atributos i = 1 a i = 4. A estos atributos se asocia en cada caso la fuente de datos "carné de identidad", es decir, el código de identidad personal-ID 106 así como el Centro de Confianza A, es decir, el sistema de ordenador del proveedor de ID 136. Éste puede estar especificado, por ejemplo, en forma de su URL en el conjunto de datos de configuración 158.

En el conjunto de datos de configuración 116, en cambio, se define una cantidad de atributos I, II y III. Como fuente de datos para estos atributos se indica en cada caso una tarjeta de crédito, es decir, el código de identidad personal-ID 106'. El código de identidad personal-ID 106' tiene una zona protegida de la memoria 124', en la que están

almacenados los atributos I, II, III, … En el atributo I se puede tratar, por ejemplo, del nombre del titular de la tarjeta de crédito, en el atributo II se puede tratar del número de la tarjeta de de crédito y en el atributo III se puede tratar de la duración de la validez de la tarjeta de crédito, etc.

Como sistema de ordenador del proveedor de ID se indica en el conjunto de datos de la configuración 160 el sistema de ordenador del proveedor de ID 136' del Centro de Confianza B.

De manera alternativa a la forma de realización mostrada en la figura 3, en el mismo conjunto de datos para diferentes atributos pueden estar indicadas también diferentes fuentes de datos y/o diferentes sistemas de ordenador del proveedor de ID.

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

Por ejemplo, en la memoria 140 del sistema de ordenador del proveedor de ID 136, que se muestra de forma ejemplar 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 asociadas en cada caso. En el certificado 144.1 están definidos derechos de lectura del sistema de ordenador del proveedor de ID 136 sobre los atributos i = 1 a i = 4, en cambio en el certificado 144.2 están definidos derechos de lectura sobre los atributos I a III.

Por lo demás, se supone, sin limitación de la generalidad, que el sistema de ordenador del proveedor de ID 136 pertenece a la primera cantidad, es decir, a la cantidad de sistemas de ordenador del proveedor de ID, que son considerados como de confianza por el sistema de ordenador de servicio 150, pero los sistemas de ordenador del proveedor de ID 136', 136''… no pertenecen a la primera cantidad, sino a la segunda cantidad. El sistema de ordenador del proveedor de ID 136 pertenece, por lo tanto, a la cantidad parcial de la primera y de la segunda cantidades.

La primera cantidad puede estar fijada, por ejemplo, en una memoria de configuración del sistema de ordenador de servicio 150 con la ayuda de identificadores de los sistemas de ordenador del proveedor de ID de la primera cantidad. Estos identificadores pueden estar programados también fijamente en el programa 156. Otra posibilidad es que los identificadores de la primera cantidad de los sistemas de ordenador del proveedor de ID están almacenados en un servidor de índices, desde el que el sistema de ordenador de servicio llama los identificadores.

De una manera correspondiente se comporta para la definición de la segunda cantidad. La segunda cantidad puede estar definida también directamente sobre el plano del código de identidad personal-ID, almacenando allí los identificadores de los sistemas de ordenador del proveedor de ID de la segunda cantidad.

Para la utilización de un servicio ofrecido por el sistema de ordenador de servicio 150, el usuario 102 activa en primer lugar una entrada de usuario 162 en el sistema de ordenador del usuario 100, para introducir, por ejemplo, en una página Web del sistema de ordenador de servicio 150 su solicitud para un servicio deseado. Esta solicitud de servicio 164 se transmite desde el sistema de ordenador del usuario 100 a través de la red 116 hasta el sistema de ordenador de servicio 150.

El sistema de ordenador de servicio 150 responde a ello con una especificación de atributo 166, es decir, con una especificación de aquellos atributos, que el sistema de ordenador de servicio 150 necesita para el procesamiento de la solicitud de servicio 164 desde el usuario 102. La especificación de atributo 166 se puede realizar en forma de los nombres del atributo, como por ejemplo "Nombre", "Apellidos", "Dirección", "Número de tarjeta de crédito". La especificación del atributo 166 puede contener una indicación de uno o varios identificadores de sistemas de ordenador del proveedor de ID de la primera cantidad.

Por lo demás, si limitación de la generalidad, se parte de que el identificador del sistema de ordenador del proveedor 138 se transmite con la especificación de atributo 166. De manera alternativa, el identificador puede ser consultado por el sistema de ordenador del usuario 100 desde un servidor de índices.

La recepción de la especificación del atributo 166 es señalizada por el usuario 102 a través del sistema de ordenador del usuario 100. El usuario 102 puede seleccionar a continuación uno o, en caso necesario, varios de los conjuntos de datos de configuración 158, 160, …, que definen en cada caso cantidades de atributos, que contienen los atributos de acuerdo con la especificación de atributos 166 al menos como cantidad parcial.

Si la especificación del atributo 166 exige, por ejemplo, solamente la comunicación del nombre, de los apellidos y de la dirección del usuario 102, entonces el usuario 102 puede seleccionar el conjunto de datos de configuración 158. En cambio, si se especifica adicionalmente en la especificación del atributo 166 el número de la tarjeta de crédito, entonces el usuario 102 puede seleccionar adicionalmente el conjunto de datos de configuración 160. Este proceso se puede realizar también de una manera totalmente automática a través del sistema de ordenador del usuario 100, por ejemplo a través de la ejecución de las instrucciones del programa 112.

Por lo demás, se parte en primer lugar de que sólo se selecciona uno de los conjuntos de datos de configuración, como por ejemplo el conjunto de datos de configuración 158, en virtud de la especificación del atributo 166.

El sistema de ordenador del usuario 100 envía a continuación una solicitud 168 al o a los sistemas de ordenador del proveedor de ID indicados en conjunto de datos de configuración seleccionados, en el ejemplo considerado al sistema de ordenador del proveedor de ID 136 del Centro de Confianza A. Esta solicitud 168 contiene una indicación del sistema de ordenador del proveedor de ID 136 de los atributos que deben leerse desde la fuente de datos indicada en el conjunto de datos de configuración 158 de acuerdo con la especificación del atributo 166.

El sistema de ordenador del proveedor de ID 136 selecciona a continuación uno o varios de sus certificados, que presentan los derechos de lectura necesarios para la lectura de estos atributos. Cuando, por ejemplo, deben leerse los atributos i = 1 a 3 desde el cané de identidad personal, entonces el sistema de ordenador del proveedor de ID 136 selecciona su certificado 144.1, que define los derechos de lectura necesarios para ello. Esta selección del certificado se realiza a través de la ejecución de las instrucciones del programa 149.

A continuación se inicia la ejecución del protocolo criptográfico. Por ejemplo, el sistema de ordenador del proveedor de ID 136 envía a tal fin una respuesta al sistema de ordenador del usuario 100. El sistema de ordenador del usuario 100 solicita a continuación al usuario 102 su autentificación frente a la fuente de datos especificada, es decir, aquí frente al cené de identidad personal.

El usuario 102 lleva a continuación su carné de identidad personal, es decir, el código de identificación personal-ID 106, a la zona del aparato de lectura de RFID 104 e introduce, por ejemplo, su PIN para su autentificación. A través de la autentificación con éxito del usuario 102 frente al código de identificación personal-ID 106, éste se libera para la realización del protocolo criptográfico, es decir, para la ejecución de las instrucciones del programa 134. Por lo demás, el sistema de ordenador del proveedor de ID 136 se autentifica frente al código de identificación personal-ID 106 con la ayuda del certificado 144.1 seleccionado, por ejemplo con la ayuda del procedimiento de desafío-respuesta. Esta autentificación puede ser mutual. Después de la autentificación con éxito del sistema de ordenador del proveedor de ID 136 frente al código de identificación personal-ID 106, el sistema de ordenador del proveedor de ID dirige una solicitud de lectura para la lectura de los atributos necesarios al sistema de ordenador del usuario 100, que éste transmite a través del aparato de lectura-RFID 104 al código de identificación personal-ID 106. El código de identificación personal-ID 106 verifica con la ayuda del certificado 144.1, si el sistema de ordenador del proveedor 136 tiene los derechos de lectura necesarios para ello. Este es aquí el caso, puesto que el sistema de ordenador del proveedor de ID 136 pertenece a la segunda cantidad, de manera que se leen los atributos deseados desde la zona protegida de la memoria 124 y se transmiten por medio de la codificación de fin-a-fin al sistema de ordenador del proveedor de ID a través del sistema de ordenador del usuario 100.

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

De manera alternativa, el sistema de ordenador del proveedor de ID 136 envía la respuesta 170 al sistema de ordenador del usuario 100. El usuario 102 recibe a continuación la posibilidad de leer los atributos contenidos en la respuesta 170 y de decidir si quiere transmitir o no realmente estos atributos al sistema de ordenador de servicio 150. Sólo después de la introducción de un comando de liberación del usuario 102 en el sistema de ordenador del usuario 100 será transmitida la respuesta 170 al sistema de ordenador de servicio 150. En esta forma de realización es posible, además, que el usuario 102 complete la respuesta 170 con otros datos. La firma de la respuesta 170 es verificada por el sistema de ordenador de servicio 150. Puesto que procede desde el sistema de ordenador del proveedor de ID 136, que pertenece a la primera cantidad, se clasifica la respuesta 170 desde el sistema de ordenador de servicio 150 como de confianza.

En cambio, cuando la especificación del atributo 166 especifica uno o varios atributos, que pueden ser leídos desde una fuente de datos, a la que puede acceder el sistema de ordenador del proveedor de ID, que pertenece a la segunda cantidad, pero no a la primera cantidad, se procede de la siguiente manera:

El sistema de ordenador del usuario 100 transmite la especificación del atributo 166 en forma de la solicitud 168 a un sistema de ordenador del proveedor de ID de la primera cantidad, es decir, en el ejemplo de realización considerado aquí, al sistema de ordenador del proveedor de ID 136. La solicitud 168 contiene, además, de la especificación del atributo 166 una indicación del sistema de ordenador del proveedor de ID de la segunda cantidad, que puede acceder a los atributos especificados. El sistema de ordenador del proveedor de ID de la primera cantidad, que recibe la solicitud 168, transmite esta solicitud entonces al sistema de ordenador del proveedor de ID indicado en la solicitud 168 de la segunda cantidad como solicitud 168'.

Este sistema de ordenador del proveedor de ID de la segunda cantidad se autentifica entonces frente a la fuente de datos y lee el al menos un atributo de acuerdo con la especificación del atributo desde la fuente de datos, como se ha explicado anteriormente con relación al sistema de ordenador del proveedor de ID 136.

El sistema de ordenador del proveedor de ID de la segunda cantidad genera a continuación la respuesta 170', que contiene los atributos. El sistema de ordenador del proveedor de ID de la segunda cantidad firma la respuesta 170' y envía la respuesta 170' al sistema de ordenador del proveedor de ID de la primera cantidad.

El sistema de ordenador del proveedor de ID de la primera cantidad considera el sistema de ordenador del proveedor de ID de la segunda cantidad como digno de confianza. Después de la verificación de la firma de la respuesta 170' recibida desde el sistema de ordenador del proveedor de ID de la segunda cantidad, el sistema de ordenador del proveedor de ID de la primera cantidad firma la respuesta 170', por su parte, y envía la respuesta 170' o bien al sistema de ordenador del usuario 100 para la transmisión al sistema de ordenador del usuario 150 o directamente al sistema de ordenador del usuario 150. El sistema de ordenador de servicio 150 verifica entonces la firma del sistema de ordenador del proveedor de ID de la primera cantidad. Puesto que el sistema de ordenador de servicio 150 clasifica el sistema de ordenador del proveedor de ID de la primera cantidad como digno de confianza, considera los atributos comunicados con la respuesta 170' como válidos, si la firma del sistema de ordenador del proveedor de ID de la primera cantidad es válida.

Por ejemplo, la especificación del atributo 166 contiene una especificación de los atributos I, II y III, Después de que el sistema de ordenador del usuario 100 ha recibido esta especificación del atributo a través de la red 116, establece con la ayuda del conjunto de datos de configuración 160 que estos atributos están almacenados en la fuente de dato "tarjeta de crédito", es decir, en el código de identificación personal-ID 106. A tal fin, el "Centro de Confianza B" del proveedor de ID, es decir, el sistema de ordenador del proveedor de ID 136' de la segunda cantidad está autorizado para la lectura. Pero el sistema de ordenador del proveedor de ID 136' no pertenece a la primera cantidad, que es clasificada como digna de confianza por el sistema de ordenador de servicio 150. Esto puede ser establecido por el sistema de ordenador del usuario 100, por ejemplo, a través de una consulta del servidor público de índices. De la misma manera, el sistema de ordenador del usuario 100 puede establecer a través de la consulta de un servicio de índices, cual o cuales sistemas de ordenador del proveedor de ID pertenecen a la primera cantidad, es decir, a la cantidad de sistemas de ordenador del proveedor de ID, que considera el sistema de ordenador de servicio 150 como digno de confianza. En el caso del ejemplo considerado aquí, éste es el sistema de ordenador del proveedor de ID 136.

El sistema de ordenador del usuario 100 transmite a continuación la identificación del atributo 166 en forma de la solicitud 168 al sistema de ordenador del proveedor de ID 136 de la primera cantidad, en el que la solicitud 168 contiene un identificador, que identifica el sistema de ordenador del proveedor de ID 136'. El sistema de ordenador del proveedor de ID 136 transmite la solicitud 168 al sistema de ordenador del proveedor de ID 136' especificado en la solicitud 168, donde se procesa la solicitud 168'.

El sistema de ordenador del proveedor de ID 136' lee, por lo tanto, los atributos I, II, III desde el código de identidad personal-ID 106', por ejemplo de manera correspondiente a las etapas 204 a 206 de la forma de realización según la figura 2. El sistema de ordenador del proveedor de ID 136' no envía la respuesta 170' firmada por él, que contiene los atributos I, II, III leídos, directamente al sistema de ordenador de servicio 150 o al sistema de ordenador del usuario 100, sino al sistema de ordenador del proveedor de ID 136, desde el que ha recibido la solicitud 168'.

El sistema de ordenador del proveedor de ID 136 verifica a continuación la validez de la firma del sistema de ordenador del proveedor de ID 136'. En el caso de que la firma sea válida, el sistema de ordenador del proveedor de ID 136 considera los valores de los atributos I, II y III comunicados con la respuesta 170' como válidos y firma la respuesta 170', por su parte, para enviarla al sistema de ordenador del usuario 100 para la transmisión al sistema de ordenador de servicio 150 o para enviar la respuesta 170' directamente al sistema de ordenador de servicio 150.

La especificación del atributo 166 se puede enviar desde el sistema de ordenador de servicio 150, por ejemplo, como un llamado Código de identidad digital. Este Código de identidad digital se complementa en caso necesario desde el sistema de ordenador del usuario 100 a través de la indicación de un sistema de ordenador del proveedor de ID de la segunda cantidad, es decir, del sistema de ordenador del proveedor de ID 136' y se transmite como solicitud 168 a, sistema de ordenador del proveedor de ID 136. Si existe una relación de confianza del sistema de ordenador del proveedor de ID 136 con respecto al sistema de ordenador de servicio 150, se puede indicar por el sistema de ordenador de servicio 150 en el Código de identidad digital. En este caso, no es necesaria una consulta de un servidor público de índices a través del sistema de ordenador del usuario 100.

Cuando están implicados varios sistemas de ordenador del proveedor de ID 136, 136',…, entonces se pueden agrupar las respuestas individuales de los sistemas de ordenador del proveedor de ID a través del sistema de orden ador de usuario 100 en una única respuesta, que contiene todos los atributos de acuerdo con la especificación de atributos 166, que se envía entonces desde el sistema de ordenador del usuario 100 al sistema de ordenador de servicio 150.

De acuerdo con una forma de realización de la invención, el usuario 102 puede publicar con motivo de la solicitud de servicio 164 uno o varios de sus atributos frente al sistema de ordenador de servicio 150, por ejemplo transmitiendo estos atributos del usuario como parte de la solicitud del servicio 164 a través de la red 116 hasta el sistema de

ordenador de servicio. En particular, el usuario 102 puede introducir estos atributos en la página Web del sistema de ordenador de servicio 150. La corrección de estos atributos es confirmada entonces a través de la respuesta 170, es decir, que el sistema de ordenador de servicio 150 puede comparar los atributos recibidos desde el usuario 102 con los atributos leídos por el sistema de ordenador del proveedor de ID 136 desde el código de identidad personal-ID 106 y puede verificar la coincidencia.

De acuerdo con otra forma de realización de la invención, se puede indicar también al menos otro atributo en la especificación del atributo 166, que no está almacenado en uno de los códigos de identidad personal-ID del usuario 102, sino que se puede consultar desde una fuente de datos externa. En este caso, se puede tratar, por ejemplo, de un atributo relacionado con la solvencia del usuario 102. El sistema de ordenador del usuario 100 puede contener a tal fin otro conjunto de datos de configuración 161, que contiene para el atributo A – por ejemplo la solvencia – la indicación de una fuente de datos y de un sistema de ordenador del proveedor de ID. En la fuente de datos se puede tratar de una fuente de información, como por ejemplo, Schufa, Dun & Bradstreet o similar. Como sistema de ordenador del proveedor de ID se indica, por ejemplo, un Centro de Confianza C, como en la forma de realización de la figura 3. La fuente de datos se puede encontrar aquí en el Centro de Confianza C.

Para consultar el atributo A, por lo tanto, el sistema de ordenador del usuario 100 dirige una solicitud correspondiente (no mostrada en la figura 3) al Centro de Confianza C, es decir, al sistema de ordenador del proveedor de ID 136''. Éste transmite a continuación el atributo A, que ha sido leído por el sistema de ordenador del usuario 100 junto con los otros atributos, que han sido leídos desde el o los códigos de identificación personal-ID del usuario 102, al sistema de ordenador de servicio 150.

Con preferencia, la consulta del atributo A se realiza después de que los atributos relacionados con la identidad digital del usuario 102 ya han sido consultados desde uno de los códigos de identidad personal-ID del usuario 102, y han sido enviados, por ejemplo, como respuesta firmada 170 desde el sistema de ordenador del usuario 100. La consulta del atributo A a través del sistema de ordenador del usuario 100 desde el sistema de ordenador del proveedor de ID 136'' contiene entonces la respuesta firmada 170, de manera que el sistema de ordenador del 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 de acuerdo con la invención. El procedimiento implica los dominios de activación 1 y 2, en el que el dominio de activación 1 contiene el sistema de ordenador de servicio 150 y los sistemas de ordenador del proveedor.-ID de la primera cantidad, a la que pertenece el sistema de ordenador del proveedor de ID 136, en el que el dominio de activación 2 contiene el código de identidad personal-ID 106 del usuario 102, el sistema de ordenador del usuario 100 y los sistemas de ordenador del proveedor de ID de la segunda cantidad, a la que pertenece el sistema de ordenador del proveedor de ID 136'. En la forma de realización considerada aquí, el sistema de ordenador del proveedor de ID 136' no pertenece a la primera cantidad.

Por medio de una entrada del usuario 102 en el sistema de ordenador del usuario 100, el usuario 102 especifica un servicio de un sistema de ordenador de servicio, que quiere utilizar. Esto se realiza, por ejemplo, a través de una llamada de una página de Internet del sistema de ordenador de servicio y de una selección de uno de los servicios ofrecidos allí. Esta solicitud de servicio del usuario 102 se transmite desde el sistema de ordenador del usuario 100 al sistema de ordenador de servicio 150.

El sistema de ordenador de servicio 150 responde a la solicitud de servicio con una especificación del atributo, es decir, por ejemplo con una lista de nombres de atributos. La especificación de atributos se puede enviar en forma del Código de identidad digital. Junto a la especificación del atributo, el Código de identidad digital puede contener una indicación de un sistema de ordenador del proveedor de ID de la primera cantidad. En el caso del ejemplo considerado aquí, éste es el sistema de ordenador del proveedor de ID 136. Después de la recepción de la especificación del atributo, el sistema de ordenador del usuario 100 solicita al usuario 102, por ejemplo a través de una solicitud de entrada, la autentificación frente al código de identificación personal-ID 106.

El usuario 102 se autentifica a continuación frente al código de identidad-ID 106, por ejemplo a través de la entrada de su PIN. Además, el sistema de ordenador del usuario 100 determina qué sistema de ordenador del proveedor de ID tiene una autorización de lectura para la lectura de los atributos especificados desde el código de identificación personal-ID 106. Esto se puede realizar con la ayuda de conjuntos de datos de configuración, a través de la consulta del código de identificación personal-ID 106 o a través de la consulta de un servidor de índices. En el caso del ejemplo considerado aquí, éste es el sistema de ordenador del proveedor de ID 136'.

Después de la autentificación con éxito, el Código de identidad digital se transmite desde el sistema de ordenador del usuario 100 al sistema de ordenador del proveedor de ID 136, en el que el Código de identidad digital ha sido completado con un identificador del sistema de ordenador del proveedor de ID 136'. El Código de identidad digital se transmite desde el sistema de ordenador del proveedor de ID 136 al sistema de ordenador del proveedor de ID 136'. Éste se autentifica a continuación frente al código de identificación personal-ID 106 y dirige una solicitud de lectura para la lectura de los atributos de acuerdo con la especificación del atributo al código de identificación personal-ID 106.

En el supuesto de la autentificación con éxito anterior del usuario 102 y del sistema de ordenador del proveedor de ID 136', el código de identificación personal-ID 106 contesta a la solicitud de lectura con los atributos deseados. El sistema de ordenador del proveedor de ID 136' firma los atributos y envía los atributos firmados al sistema de ordenador del proveedor de ID 136. El sistema de ordenador del proveedor de ID 136 firma los atributos también, por su parte, y transmite los atributos firmados al sistema de ordenador del usuario 100. Después de la liberación a través del usuario 102 se transmiten los atributos junto con la firma del sistema de ordenador del proveedor de ID 136 entonces al sistema de ordenador de servicio 150 que puede prestar entonces, dado el caso, el servicio deseado.

Esto tiene en particular la ventaja de que se puede realizar un tráfico electrónico de derechos más allá de dominios de activación de una manera eficiente y, sin embargo, segura.

Lista de signos de referencia

100 Sistema de ordenador del usuario

102 Usuario

104 Interfaz

106 Código de identidad personal-ID

108 Interfaz

110 Procesador

112 Instrucciones del programa

114 Interfaz de la red

116 Red

118 Memoria electrónica

120 Zona protegida de la memoria

122 Zona protegida de la memoria

124 Zona protegida de la memoria

126 Zona de la memoria

128 Procesador

130 Instrucciones del programa

132 Instrucciones del programa

134 Instrucciones del programa

136 Sistema de ordenador del proveedor de ID

138 Interfaz de la red

140 Memoria

142 Clave privada

144 Certificado

145 Procesador

146 Instrucciones del programa

148 Instrucciones del programa

149 Instrucciones del programa

150 Sistema de ordenador de servicio

152 Interfaz de la red

154 Procesador

156 Instrucciones del programa

158 Conjunto de datos de configuración

160 Conjunto de datos de configuración

161 Conjunto de datos de configuración

162 Entrada del usuario

164 Solicitud de servicio

166 Identificación del atributo

168 Solicitud

170 Respuesta

REIVINDICACIONES

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

- emisión de una solicitud (164) desde un cuarto sistema de ordenador del usuario (100) a un segundo sistema de ordenador de servicio (150),
- especificación de uno o varios atributos a través del segundo sistema de ordenador de servicio (150),
- emisión de la especificación del atributo (166) desde el segundo sistema de ordenador de servicio (150) a un tercer sistema de ordenador (136),
- transmisión de la especificación del atributo desde el tercer sistema de ordenador (136) a un primer sistema de ordenador (136'),
- autentificación del usuario frente al código de identidad-ID (106, 106'),
- autentificación del primer sistema de ordenador (136') frente al código de identidad-ID,
- después de la autentificación con éxito del usuario y del primer sistema de ordenador frente al código de identidad-ID, acceso de lectura del primer sistema de ordenador al menos a un atributo almacenado en el código de identidad-ID,
- firma del al menos un atributo leído desde el código de identidad-ID a través del primer sistema de ordenador,
- transmisión del atributo firmado desde el primer sistema de ordenador al segundo sistema de ordenador de servicio,

en el que la autentificación del primer sistema de ordenador (136') frente al código de identidad-ID se realiza en virtud de una especificación del atributo (166, 168'), que recibe el primer sistema de ordenador desde el tercer sistema de ordenador (136),

en el que la especificación del atributo especifica el al menos un atributo,

en el que el acceso de lectura del primer sistema de ordenador se realiza para leer uno o varios atributos, especificados en la especificación del atributo, desde el código de identidad-ID.

2.- Procedimiento de acuerdo con la reivindicación 1, en el que la autentificación del primer sistema de ordenador frente al código de identidad-ID se realiza con la ayuda de un certificado (144) del primer sistema de ordenador, en el que el certificado contiene la indicación de aquellos atributos almacenados en el código de identidad-ID, para los que el primer sistema de ordenador está autorizado a leer, en el que con preferencia el código de identidad-ID verifica la autorización de lectura del primer sistema de ordenador para al acceso de lectura al menos a uno de los atributos con la ayuda del certificado.

3.- Procedimiento de acuerdo con la reivindicación 1 ó 2, en el que la solicitud (164) contiene un identificador para la identificación del primer sistema de ordenador a través del segundo sistema de ordenador de servicio, y en el que la transmisión de la especificación del atributo desde el segundo sistema de ordenador de servicio hasta el primer sistema de ordenador se realiza sin la interconexión del cuarto sistema de ordenador del usuario.

4.- Procedimiento de acuerdo con la reivindicación 3, en el que el cuarto sistema de ordenador del usuario presenta varios conjuntos de datos de configuración (158, 160,…) predefinidos, 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 de ordenador a partir de una cantidad de primeros sistemas de ordenados (136, 136',…), en el que la especificación del atributo se transmite desde el primer sistema de ordenador de servicio en primer lugar al cuarto sistema de ordenador del usuario, de manera que por medio del cuarto sistema de ordenador del usuario 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 del atributo, y en el que el tercer sistema de ordenador transmite la especificación del atributo a través del tercer sistema de ordenador al primer sistema de ordenador, y en el que la conexión entre el primer sistema de ordenador y el código de personal de identidad-ID especificado a través de la indicación de la fuente de datos en el conjunto de datos de configuración seleccionado se establece a través del cuarto sistema de ordenador del usuario.

5.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que el al menos un atributo leído por el primer sistema de ordenador desde el código de identidad-ID es enviado al cuarto sistema de ordenador del usuario, desde donde se transmite después de la liberación a través del usuario al segundo sistema de ordenador de

servicio, en el que con preferencia el usuario puede completar los atributos antes de la transmisión al segundo sistema de ordenador de servicio a través de otros datos.

6.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que el primer sistema de ordenador presenta varios certificados (144.1; 144.2) con diferentes derechos de lectura, en el que el primer sistema de ordenador selecciona en virtud de la recepción de la especificación del atributo al menos uno de los certificados, que presenta derechos de lectura suficientes para la lectura de los atributos especificados en la especificación de los atributos.

7.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que el cuarto sistema de ordenador del usuario tiene al menos un conjunto de datos de configuración (161), que especifica una fuente de datos externa para la consulota de otro atributo (A) desde el tercer sistema de ordenador a través de la red (116), en el que la consulta del otro atributo se realiza con preferencia después de que el al menos un atributo ha sido leído desde el código de identidad-ID, y después de que el cuarto sistema de ordenador del usuario ha recibido el al menos un atributo firmado desde el primer sistema de ordenador, en el que la consulta contiene el al menos un atributo firmado.

8.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que la solicitud (164) sirve para la llamada de un servicio proporcionado por el segundo sistema de ordenador de servicio, en el que la condición previa para la prestación del servicio es la recepción de uno o varios de los atributos a través del segundo sistema de ordenador de servicio, en el que la especificación del atributo se transmite desde el cuarto sistema de ordenador del usuario (100) al tercer sistema de ordenador (136) en forma de una solicitud (168), que contiene una indicación del primer sistema de ordenador (136'), en el que el primer sistema de ordenador emite el al menos un atributo al tercer sistema de ordenador, en el que el tercer sistema de ordenador transmite el al menos un atributo al segundo sistema de ordenador de servicio, en el que el tercer sistema de ordenador firma el al menos un atributo antes de la transmisión.

9.- Producto de programa de ordenador con instrucciones ejecutables por un sistema de ordenador para la realización de un procedimiento de acuerdo con una de las reivindicaciones anteriores.

10.- Código de identidad-ID para la realización de un procedimiento de acuerdo con la reivindicación 1, con

- una zona protegida de la memoria (124) para el almacenamiento de al menos un atributo y de al menos un identificador de un primer sistema de ordenador (136'),
- medios (120, 130) para la autentificación de un usuario (102) asociado al código de identidad-ID frente al código de identidad-ID,
- medios (134) para la autentificación del primer sistema de ordenador (136') frente al código de identidad-ID,
- medios (132) para el establecimiento de una conexión protegida con el primer sistema de ordenador, a través del cual el primer sistema de ordenador puede leer el al menos un atributo,

en el que una condición previa necesaria para la lectura del al menos un atributo desde el código de identidad-ID a través del primer sistema de ordenador es la autentificación con éxito del usuario y del primer sistema de ordenador frente al código de identidad-ID,

en el que los medios para la autentificación del primer sistema de ordenador frente al código de identidad-ID están configurados de tal manera que la autentificación del primer sistema de ordenador se realiza con la ayuda de un certificado (144) del primer sistema de ordenador, en el que el certificado contiene una indicación de aquellos atributos almacenados en el código de identidad-ID, para los que el primer sistema de ordenador está autorizado para el acceso de lectura,

en el que el código de identidad-ID contiene, además, medios para la codificación de fin a fin de la comunicación para una transmisión protegida de al menos uno de los atributos al primer sistema de ordenador, y en el que en el código de identidad-ID se trata con preferencia de un aparato electrónico, en particular una memoria USB, o un documento, en particular un documento de valor o documento de seguridad.

11.- Sistema de ordenador (136') adecuado para la realización de un procedimiento de acuerdo con la reivindicación 1, con

- medios (138') para la recepción de una especificación de atributo (166) a través de una red (116) desde un sistema de ordenador (136) no autorizado, en el que la especificación del atributo especifica al menos un atributo,
- medios (142', 144', 146') para la autentificación frente a un código personal de identificación-ID (106),

- medios para la lectura del al menos un atributo desde el código personal de identificación-ID a través de una comunicación protegida,

- medios para la transmisión del al menos un atributo al sistema de ordenador autorizado,

en el que la lectura del al menos un atributo presupone que un usuario asociado al código personal de identificación-ID y el sistema de ordenador se han autentificado ante el código personal de identificación-ID, y

con medios para la generación de una solicitud al usuario para la autentificación frente al código personal de identificación-ID en virtud de la recepción de la especificación del atributo, en el que el sistema de ordenador contiene con preferencia, además, medios (144) para la firma del al menos un atributo, en el que se envía el atributo firmado.

12.-. Sistema de ordenador de acuerdo con la reivindicación 11, con varios de los certificados (144.1; 144.2), en el que los certificados definen diferentes derechos de lectura, en el que el sistema de ordenador está configurado para seleccionar en virtud de la recepción de la especificación del atributo al menos uno de los certificados, que presenta los derechos de lectura suficientes para la lectura de los atributos especificados en la especificación de los atributos.

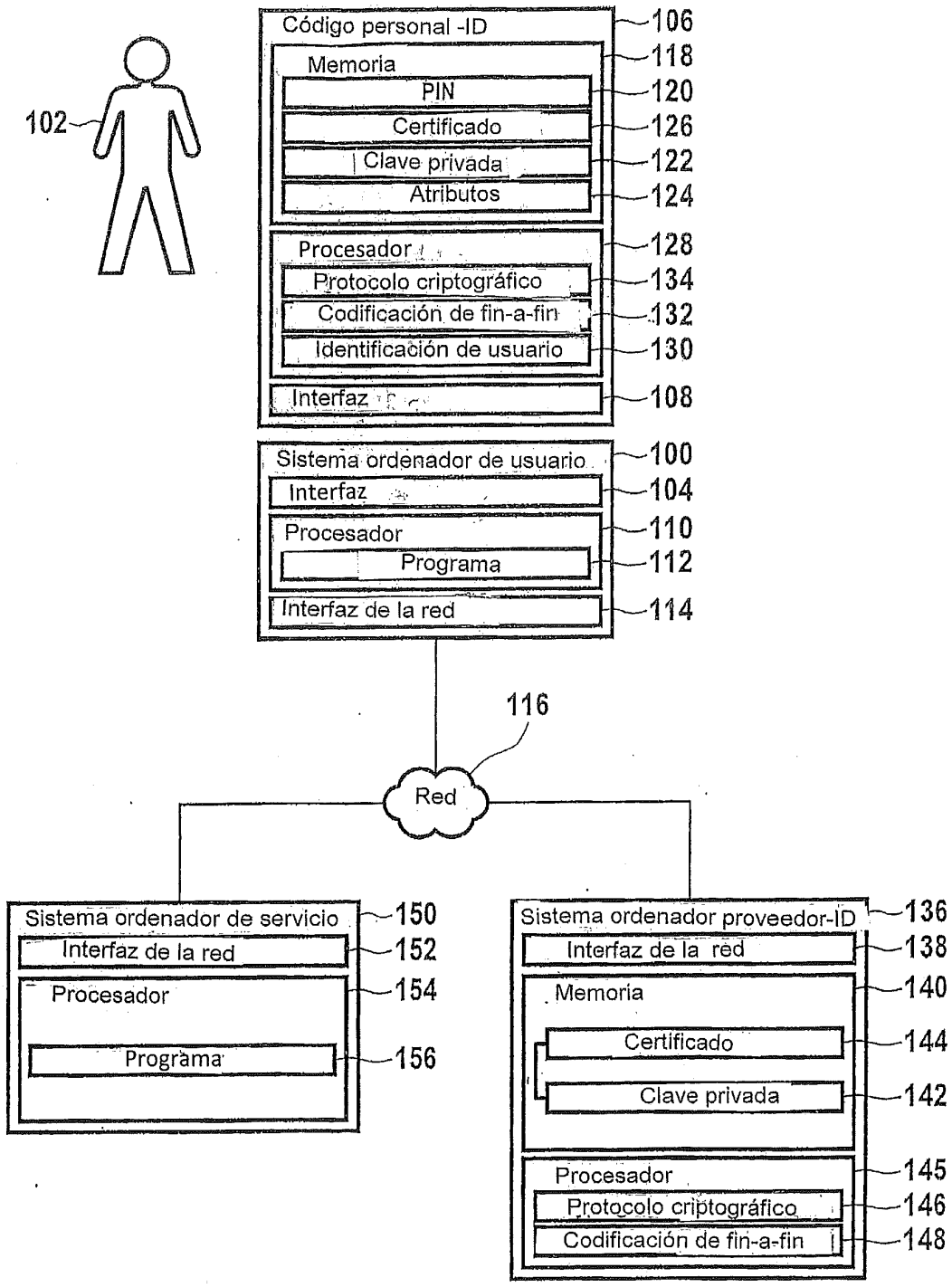

102
Código personal -ID
106
Memoria
118
PIN
120
Certificado
126
Clave privada
122
Atributos
124
Procesador
128
Protocolo criptográfico
134
Codificación de fin-a-fin
132
Identificación de usuario
130
Interfaz
108
Sistema ordenador de usuario
100
Interfaz
104
Procesador
110
Programa
112
Interfaz de la red
114
116
Red
Sistema ordenador de servicio
150
Interfaz de la red
152
Procesador
154
Programa
156
Sistema ordenador proveedor-ID
136
Interfaz de la red
138
Memoria
140
Certificado
144
Clave privada
142
Procesador
145
Protocolo criptográfico
146
Codificación de fin-a-fin
148

Fig. 1

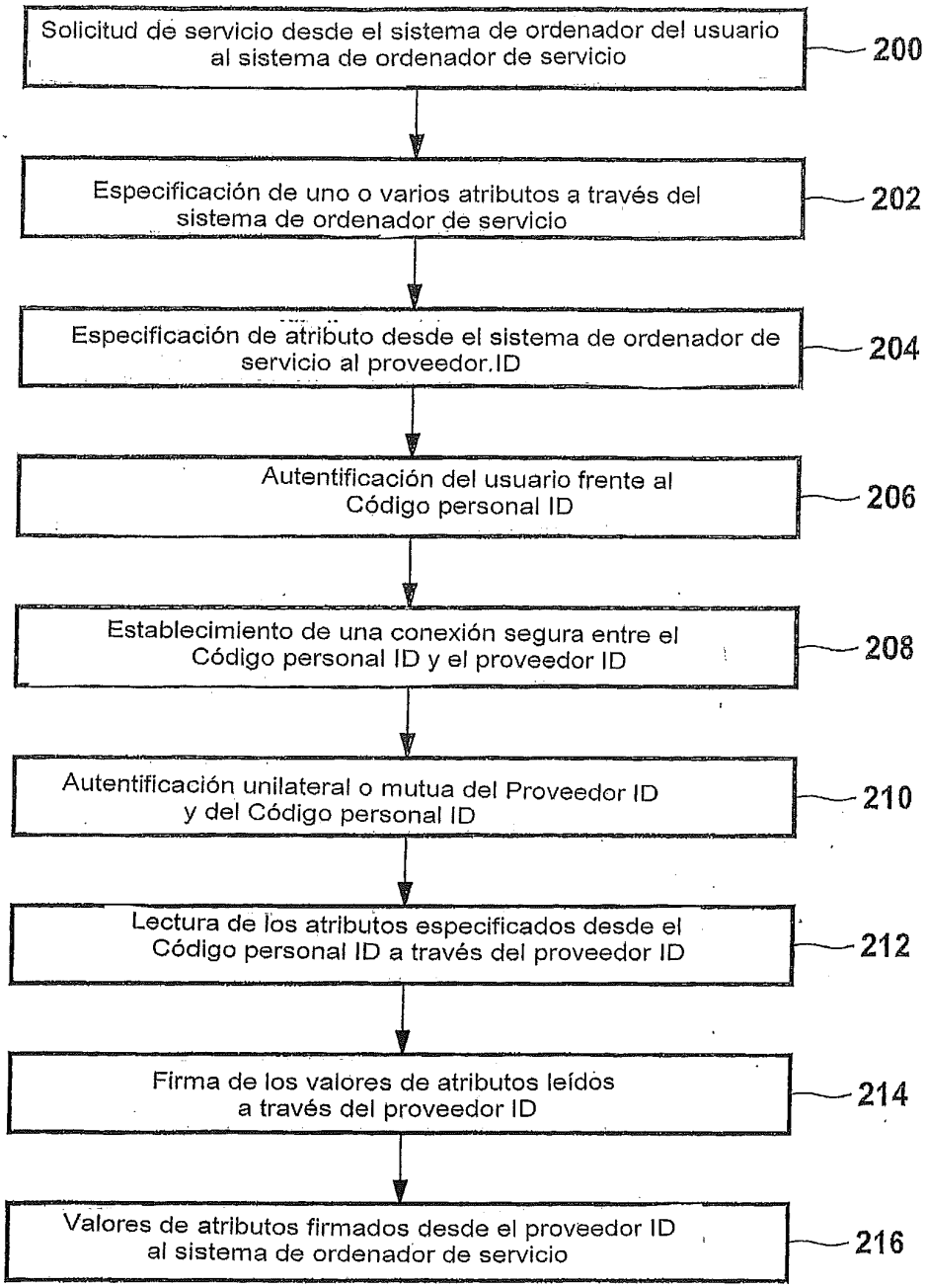

Solicitud de servicio desde el sistema de ordenador del usuario al sistema de ordenador de servicio
200
Especificación de uno o varios atributos a través del sistema de ordenador de servicio
202
Especificación de atributo desde el sistema de ordenador de servicio al proveedor.ID
204
Autentificación del usuario frente al Código personal ID
206
Establecimiento de una conexión segura entre el Código personal ID y el proveedor ID
208
Autentificación unilateral o mutua del Proveedor ID y del Código personal ID
210
Lectura de los atributos especificados desde el Código personal ID a través del proveedor ID
212
Firma de los valores de atributos leídos a través del proveedor ID
214
Valores de atributos firmados desde el proveedor ID al sistema de ordenador de servicio
216

Fig. 2

Fig. 3

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

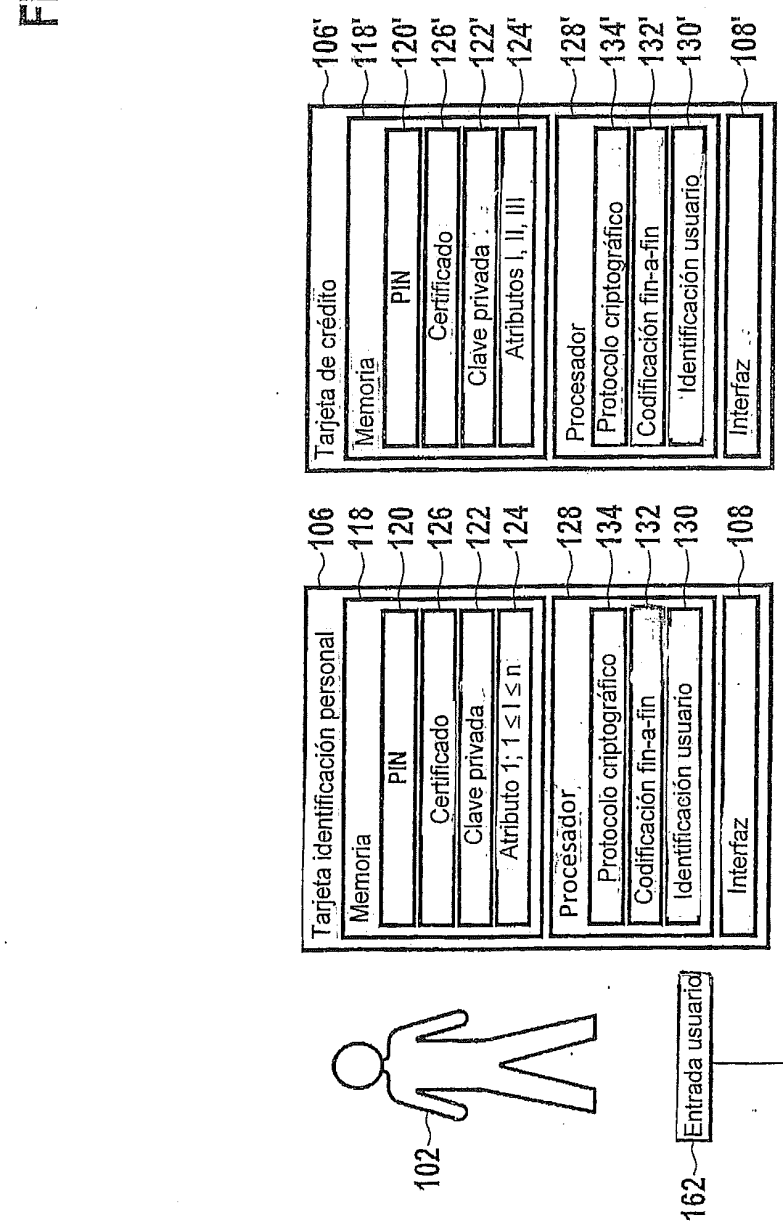


Fig. 3

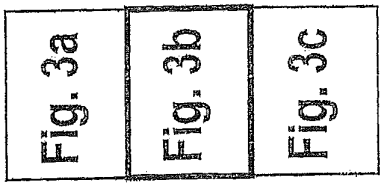
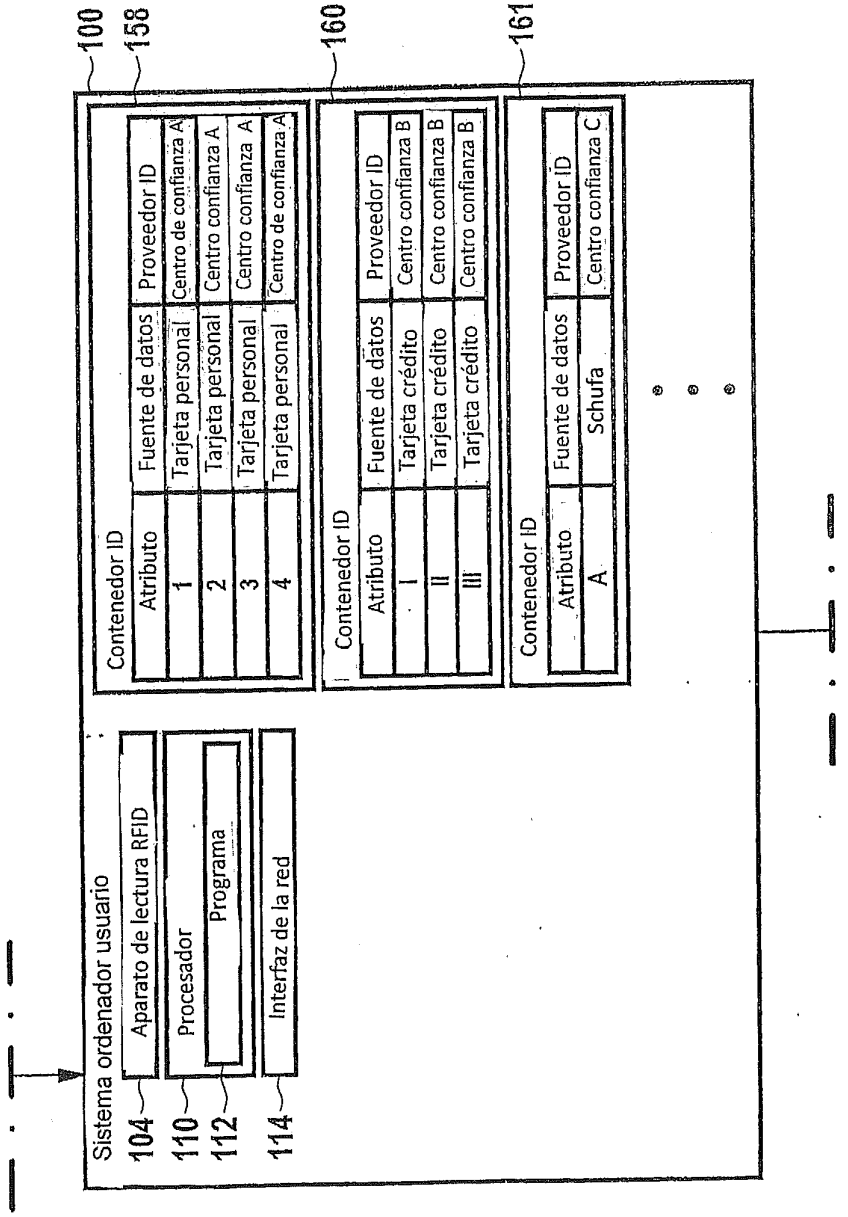


Fig. 3a
Fig. 3b
Fig. 3c


Sistema ordenador usuario
Aparato de lectura RFID
Procesador
Programa
Interfaz de la red
104
110
112
114
100
158
160
161
Contenedor ID
Atributo
Fuente de datos
Proveedor ID
1
Tarjeta personal
Centro de confianza A
2
Tarjeta personal
Centro confianza A
3
Tarjeta personal
Centro confianza A
4
Tarjeta personal
Centro de confianza A
Contenedor ID
Atributo
Fuente de datos
Proveedor ID
I
Tarjeta crédito
Centro confianza B
II
Tarjeta crédito
Centro confianza B
III
Tarjeta crédito
Centro confianza B
Contenedor ID
Atributo
Fuente de datos
Proveedor ID
A
Schufa
Centro confianza C

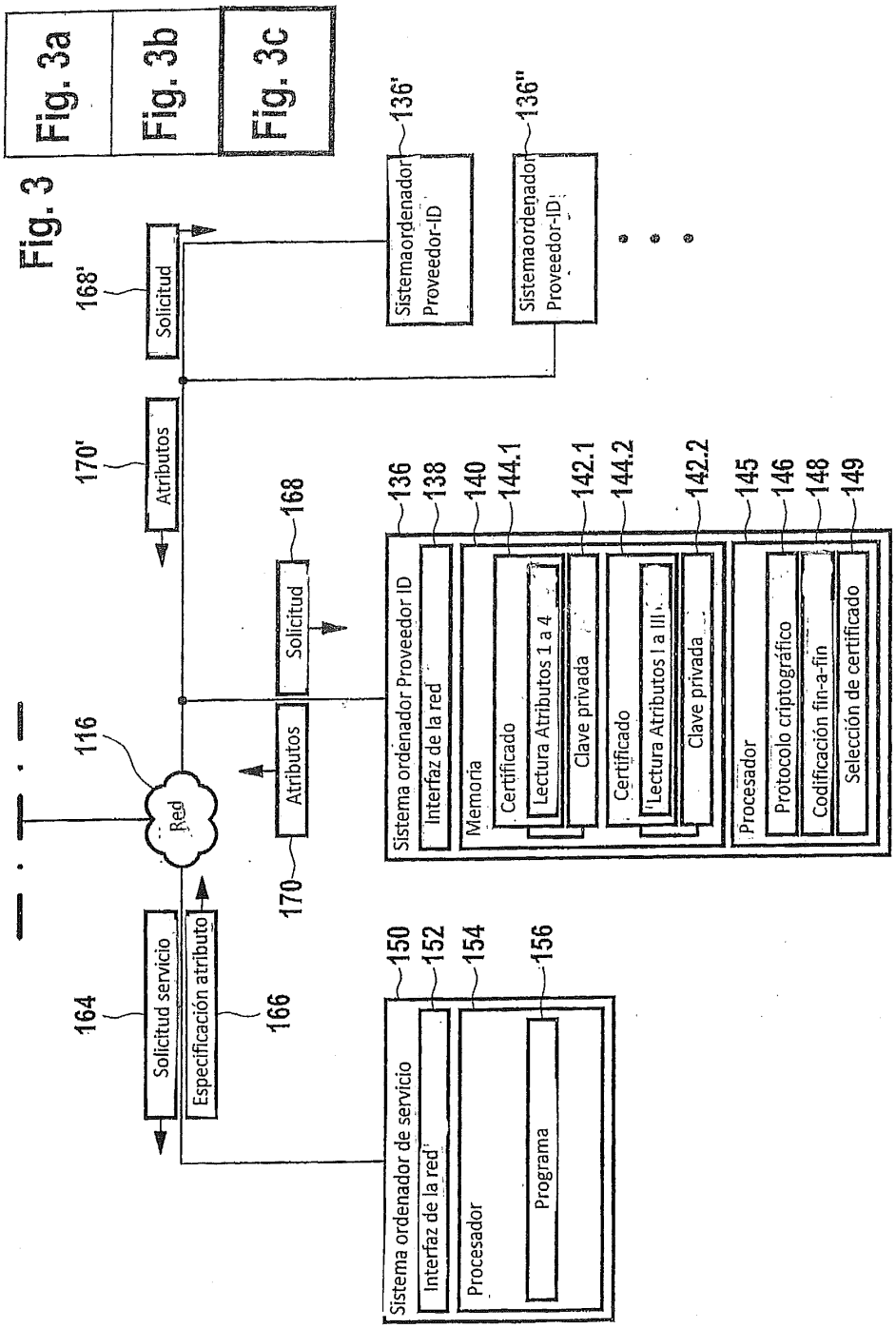


Fig. 3a
Fig. 3b
Fig. 3c
Fig. 3
168'
Solicitud
170'
Atributos
116
Red
164
Solicitud servicio
166
Especificación atributo
168
Solicitud
170
Atributos
136'
Sistemaordenador Proveedor-ID
136''
Sistemaordenador Proveedor-ID
136
138
140
144.1
142.1
144.2
142.2
145
146
148
149
Sistema ordenador Proveedor ID
Interfaz de la red
Memoria
Certificado
Lectura Atributos 1 a 4
Clave privada
Certificado
Lectura Atributos I a III
Clave privada
Procesador
Protocolo criptográfico
Codificación fin-a-fin
Selección de certificado
150
152
154
156
Sistema ordenador de servicio
Interfaz de la red
Procesador
Programa

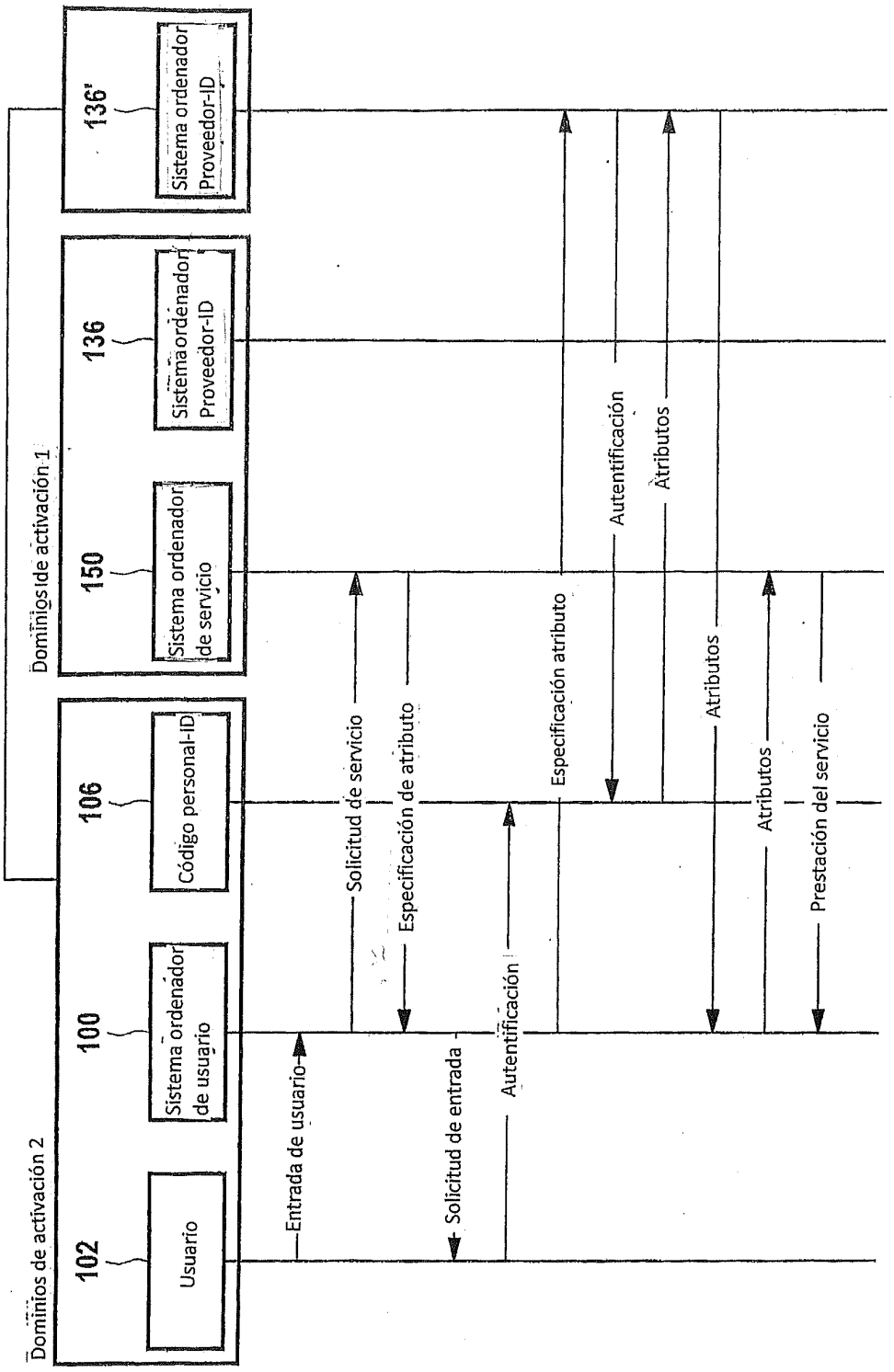

Dominios de activación 2
102
Usuario
100
Sistema ordenador de usuario
106
Código personal-ID
Dominios de activación 1
150
Sistema ordenador de servicio
136
Sistema ordenador Proveedor-ID
136'
Sistema ordenador Proveedor-ID
Entrada de usuario
Solicitud de entrada
Autentificación
Solicitud de servicio
Especificación de atributo
Especificación atributo
Autentificación
Atributos
Atributos
Atributos
Prestación del servicio

Fig. 4