(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 431**

(51) Int. CI.:

G06F 21/62 (2013.01)
G06Q 10/10 (2012.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.05.2004 E 13000661 (2)**

(97) Fecha y número de publicación de la concesión europea: **04.01.2017 EP 2618285**

(54) Título: **Sistema seguro de red informática para la gestión de datos personales**

(30) Prioridad:

23.05.2003 CH 9292003

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2017

(73) Titular/es:

DIE SCHWEIZERISCHE POST AG (100.0%)
Wankdorfallee 4
3030 Bern, CH

(72) Inventor/es:

GOBET. JEAN

(74) Agente/Representante:

COBO DE LA TORRE, María Victoria

DESCRIPCIÓN

Sistema seguro de red informática para la gestión de datos personales

(0001) La invención presente hace referencia a un sistema seguro de red informática para la gestión de datos, especialmente, datos personales. La invención hace referencia en particular a un sistema seguro de red informática para la gestión de expedientes médicos en un sistema de salud de una región o un país.

(0002) Existen numerosos proyectos para crear, desarrollar y mantener las redes de salud informatizadas con la finalidad, entre otros, de mejorar los servicios a los pacientes y de reducir los costes de los sistemas de salud. La conversión a la forma electrónica de datos de los pacientes en los sistemas actuales de salud tiene el objetivo general de mejorar uno o varios de los siguientes procesos: el flujo administrativo, especialmente, el referente al reembolso de los servicios médicos; la distribución y el completado de los expedientes médicos para los médicos tratantes, hospitales y emergencias; y la prescripción de medicamentos, especialmente, para la adecuación del diagnóstico y las interacciones para limitar los errores de prescripción, tanto como su distribución al farmacéutico o a la aseguradora para el reembolso.

(0003) En los sistemas en vigor o en forma de proyectos piloto en diferentes países o regiones, se propone el almacenamiento de ciertos datos del paciente en tarjetas inteligentes o el almacenamiento de datos del paciente en un servidor centralizado, o una combinación de los dos, los datos variando desde simples datos administrativos (por ejemplo, sobre la cobertura del seguro y los beneficios de la seguridad social, así como sobre la identificación de la persona) a la información médica del paciente. Los sistemas de salud basados en las tarjetas inteligentes o en la centralización de datos informáticos de un paciente están resumidos a continuación:

Tarjeta SESAM-Vitale, Francia

(0004) Los habitantes de Francia están provistos de una carta inteligente que contiene información sobre sus beneficios de seguridad social, usados para la comunicación entre pacientes, médicos y aseguradoras.

Red de salud social, Francia

(0005) La red de salud social francesa hace posible la comunicación mejorada entre los pacientes y las aseguradoras y ofrece una mensajería segura entre los profesionales de la salud. Esta red admite la tarjeta inteligente.

Proyecto alemán

(0006) La red alemana propone un expediente médico informatizado y herramientas para una comunicación segura y para dar apoyo en el día a día a los médicos. Cada paciente está provisto de una tarjeta de salud.

Picnic, Dinamarca

(0007) Una red segura en la que los servicios tales como la mensajería de seguridad se pueden incorporar está siendo desarrollada como una facilidad de recurso abierto y que tiene el objetivo de hacer más uniformes las industrias y las empresas de telecomunicaciones europeas.

Rimouski, Quebec

(0008) Una tarjeta de salud experimental fue distribuida a los habitantes de la región de Rimouski. La misma contiene toda la información médica del paciente (vacunas, alergias, medicamentos).

Laval, Quebec

(0009) La misma tarjeta de salud experimental que aquélla de Rimouski fue distribuida a los habitantes de Laval, pero la arquitectura de la red de datos fue modificada, con un expediente del paciente centralizado.

Hygeianet, Creta

(0010) La red de salud de Creta propone una comunicación mejorada del expediente médico informatizado entre profesionales y la gestión remota de recursos médicos.

Proyecto esloveno

(0011) Cada habitante de Eslovenia está provisto de una tarjeta de salud que contiene información sobre sus beneficios de seguridad social, medicamentos prescritos e información de emergencia (vacunas, alergias, etc.)

Proyecto danés

(0012) El objetivo de este proyecto es el de investigar y estudiar los diferentes proyectos que existen en el país, o incluso, en otros países nórdicos, y obtener las directrices federadas.

Banco Carrefour

(0013) Este proyecto belga propone un portal gubernamental sobre todos los servicios sociales, incluidos los servicios de salud, una identificación única y nacional de los habitantes de Bélgica y una transferencia segura de sus datos entre los servicios para evitar tener que volver a introducir los datos.

(0014) Una de las principales desventajas de los sistemas basados en el uso de la tarjeta inteligente para almacenar datos, especialmente, datos en el expediente médico de un paciente, es que los datos pueden perderse. Por otro lado, en un caso de emergencia, el acceso al expediente dependerá de la presencia de la tarjeta inteligente. Otra desventaja de almacenar los datos de un expediente médico en una tarjeta inteligente es que, incluso con el consentimiento del paciente, los profesionales de la salud (proveedor de cuidados, farmacéuticos, médicos, enfermeras, hospitales y otros proveedores de servicios médicos) no tienen acceso a los datos en todo momento.

(0015) Estas desventajas se eliminan por el almacenamiento de los datos relativos al paciente en un servidor de una red informática accesible por varios proveedores de servicios. Una desventaja principal de semejante sistema tiene que ver con el nivel de seguridad y con la confidencialidad de los datos sensibles. La protección de los datos personales, tales como los documentos de un expediente médico de un paciente, es importante no sólo en relación con las terceras partes no autorizadas, sino también en relación con usuarios autorizados que podrían abusar de sus derechos de acceso a estos datos, o que podrían ser negligentes, y mediante semejante negligencia podrían permitir a terceras partes obtener los datos.

(0016) Aunque las redes seguras y el intercambio de la información codificada hacen posible mitigar los riesgos de que se piratee una red de salud informatizada y el acceso ilícito a los datos personales almacenados en un servidor o circulando en la red entre los usuarios, siguen siendo un problema el abuso o la negligencia en relación con estos datos por un usuario autorizado.

(0017) En vista a las desventajas mencionadas arriba, uno de los objetivos de la invención es proporcionar un sistema seguro de red informática para la gestión de los datos que hace posible asegurar un alto nivel de protección de los datos. En particular, la invención pretende proporcionar un sistema seguro de red informática para la gestión de datos médicos en un sistema de salud regional, nacional o internacional.

(0018) Otro objeto de la invención es proporcionar una red informática segura para la gestión de datos médicos personales que hace posible, por un lado, mejorar la calidad de la información accesible a los usuarios autorizados, y por el otro lado, reducir los costes administrativos unidos al procesamiento de datos, al mismo tiempo que ofrecer un nivel alto de protección de los datos ante las terceras partes no autorizadas o contra el abuso o negligencia por parte de personas autorizadas.

(0019) Es ventajoso proporcionar un sistema seguro de red informática para la gestión de datos médicos personales en un sistema de salud que posibilita el acceso rápido a la información en un expediente médico.

(0020) Es ventajoso proporcionar un sistema seguro de red informática para la gestión de datos médicos personales en el que el acceso a los datos que constituyen un expediente médico puedan ser definidos de un modo variable en relación con los documentos accesibles y en el tiempo por cada usuario autorizado.

(0021) Es ventajoso proporcionar un sistema seguro de red informática para la gestión de datos médicos personales que sea flexible, como para asegurar su longevidad y la posibilidad de integración en otras redes informáticas existentes o futuras.

(0022) Los objetos de la invención se ejecutan por un sistema seguro de red informática según la reivindicación 1ª para gestionar datos confidenciales y por un método según la reivindicación 8ª para gestionar datos en un sistema seguro de red informática.

(0023) El documento WO 02/05061 A1 describe las características de la introducción de las reivindicaciones 1ª y 18ª.

(0024) En la presente invención, un sistema seguro de red informática para la gestión de datos protegidos comprende, al menos, una infraestructura de portal conectada mediante una red de comunicación troncal cerrada a una multitud de sistemas de servidor de registro de datos, cada sistema de servidor de registro de datos comprendiendo, al menos, una base de datos en la que se almacenan datos protegidos que constituyen documentos médicos de pacientes, y un mediador técnico de servicio de registro para gestionar el acceso a los documentos almacenados en la base de datos, y los diferentes documentos que forman un expediente médico relativo a una persona posiblemente son distribuidos a través de una multitud de sistemas de servidor de registro de datos situados en distintos lugares, la infraestructura de portal comprendiendo, al menos, un mediador de acceso de expediente en forma de un sistema de servidor con aplicaciones que controlan y gestionan el acceso de los usuarios a los documentos almacenados en los sistemas de servidor de registro de datos.

(0025) Las reivindicaciones dependientes describen otros aspectos ventajosos de la invención.

(0026) Ventajosamente, el uso de una multitud de servidores de registro de datos distribuidos para almacenar datos desde un expediente médico accesible mediante una red segura cerrada (red troncal) hace posible asegurar un nivel alto de protección de los datos porque, incluso en el caso de una entrada ilícita (forzada) dentro del sistema seguro de red, la recuperación de los datos que constituyen un expediente médico exige un ataque en una multitud de servidores protegidos, y por ello, es extremadamente dificultoso. Al menos, dos niveles de derechos de accesos, por ejemplo, la autorización a acceder a la red troncal y a los datos personales de un paciente mediante una tarjeta inteligente y al acceso a diferentes datos de un expediente médico específico, hacen posible reducir enormemente el riesgo de abuso de los datos y definir el acceso a los varios elementos del expediente como una función del cargo y la identidad del usuario autorizado. El registro del acceso a los datos y a otras operaciones en los servidores hace posible identificar a los usuarios, y por ello, prevenir el abuso por los usuarios. El acceso a los datos protegidos, sin embargo, es posible en una emergencia por ciertos profesionales de la salud, tales como hospitales y médicos tratantes, estando provista la seguridad, por un lado, por el registro del acceso, y por el otro lado, por la necesidad de usar medios fuertes de autorización y autentificación, mediante la tarjeta inteligente.

(0027) Otras finalidades y aspectos ventajosos de la invención resultan de las reivindicaciones, de la descripción siguiente y de los dibujos adjuntos, en los cuales:

La figura 1 es una representación de la arquitectura física de un sistema de red informática, de acuerdo con la invención para la gestión de los datos;

La figura 1a es una representación de una parte de la arquitectura física de acuerdo con una variante;

La figura 2 es una representación de la arquitectura lógica de un sistema de red informática de acuerdo con la invención para la gestión de datos;

La figura 3 es una representación de la arquitectura lógica de un sistema de red informática de acuerdo con la invención para la gestión de datos basado en una plataforma J2EE (Java 2 Enterprise Edition);

La figura 4 es una representación simplificada de la arquitectura física de dos portales de un sistema de red informático de acuerdo con la invención;

La figura 5 es una representación de la estructura lógica de una parte del sistema de red informática de acuerdo con la invención relativa al acceso a los servicios de valor añadido;

La figura 6 es una representación gráfica de la arquitectura lógica de una parte del sistema de red informática de acuerdo con la invención relativa al servicio de valor añadido, en el ejemplo se muestra un servicio de ayuda de prescripción de medicamentos;

La figura 7 es una representación de la arquitectura lógica de una parte del sistema de red informática de acuerdo con la invención relativa a un servicio de valor añadido, en el ejemplo se muestra una base de datos de logística;

La figura 8 es un diagrama mostrando las acciones principales de la apertura de una sesión en el sistema de red informática; La figura 9 es un diagrama ilustrando las secuencias de acciones en una creación (publicación) de un documento relativo a un paciente para ser almacenado en el sistema de red informática de acuerdo con la invención; La figura 10 es un diagrama mostrando las secuencias de acciones buscando documentos en un sistema de red informática de acuerdo con la invención;

La figura 11 es un diagrama mostrando la secuencia de acciones para consultar un documento almacenado en el sistema de red informática; La figura 12 es un diagrama mostrando la secuencia de acciones para modificar los derechos de acceso al sistema de red informática o a un expediente almacenado en el sistema; La figura 13 es un diagrama mostrando la secuencia de acciones para el uso de un servicio de valor añadido, en este ejemplo, para el uso de herramientas de ayuda de prescripción de medicamentos.

(0028) Haciendo referencia a las Fig. 1 y 2, un sistema de red informática para la gestión de datos médicos personales (confidenciales) (1) (en adelante: sistema de salud informatizado) comprende, al menos, una infraestructura de portal (2a, 2b), una multitud de sistemas de servidor de registro de datos (3a, 3b, 3c) y una red de comunicación troncal cerrada (4) que conecta las infraestructuras de portal a los sistemas de servidor de registro de datos. Los sistemas de servidor de registro de datos y las infraestructuras de portal están situados en distintos lugares. La descentralización de los datos, tanto físicamente (datos distribuidos entre diferentes bases de datos) y geográficamente (bases de datos situados en distintos lugares), ofrece un alto nivel de protección de los datos.

(0029) El sistema de salud informatizado puede comprender además uno o varios sistemas de servidor de puntos de interconexión (5) conectados, por un lado, a la red de comunicación troncal, y por otro lado, a las redes informáticas externas, por ejemplo, redes informáticas de otros sistemas de salud informatizados regionales o nacionales. Los usuarios (6) acceden a la infraestructura del portal (2a, 2b) del sistema de salud informatizado mediante internet (7)

usando una conexión segura, por ejemplo, una conexión codificada tipo VPN (inglés: Virtual Private Network": red privada virtual). Los usuarios pueden ser profesionales de la salud (médicos, enfermeras, farmacéuticos) o pacientes.

(0030) Cada usuario está provisto de una tarjeta inteligente (8) y de un código personal (contraseña) para su autentificación y autorización para acceder al sistema de salud informatizado. La estación desde la cual accede el usuario al sistema de salud informatizado, por ello, tiene que estar provisto de un lector de tarjeta inteligente (9). Este lector puede tener varias formas, pero preferiblemente es compatible con el ordenador personal/ la tarjeta inteligente (PC/SC) estándar o el RSA estándar para asegurar el interfuncionamiento con todos los componentes del sistema de autentificación (tarjeta inteligente, lector de la tarjeta inteligente, interfaz y aplicación). El lector puede estar provisto de una doble ranura para permitir la inserción de dos tarjetas, por ejemplo, la tarjeta de un profesional de la salud y la tarjeta del paciente, cuando se está consultando el expediente médico del paciente. Esto hace posible tranquilizar al paciente en relación con la protección de sus datos personales, especialmente, en el momento de su primera consulta con el profesional de la salud.

(0031) La tarjeta inteligente (8) constituye un elemento importante en la autentificación del usuario, tanto si se trata del profesional de la salud como del paciente. Los datos almacenados en una memoria del microprocesador de la tarjeta incluye un identificador único del titular de la tarjeta, un certificado de autentificación, al menos, una clave privada electrónica, y datos administrativos, tales como, nombre, apellido, fecha de nacimiento, seguro o número de la seguridad social, etc. Sin embargo, La tarjeta no contiene ningún dato médico. Cuando la tarjeta está conectada al lector de la tarjeta inteligente, puede ser desbloqueada usando el código personal del usuario. El usuario está autentificado en el sistema de salud informatizado por la transmisión del certificado de autentificación. La clave privada almacenada en el microprocesador de la tarjeta inteligente posibilita la codificación y la firma de los datos intercambiados entre el usuario y el sistema de salud informatizado. Por razones de seguridad, una multitud de claves privadas pueden ser almacenadas en la tarjeta inteligente, es decir, una clave privada para cada una de las operaciones de autentificación, firma, datos y codificación.

(0032) La infraestructura del portal comprende un área VPN externa (8) conectada a la red de internet (7) a través de un acceso de router (19a) y un cortafuegos (10a), un área de servicio (11) conectada al área externa (8) a través de un cortafuegos (10b), un área de prueba (13) conectada al área externa (8) a través de un cortafuegos (10b), un área VPN interna (22) conectada al área de servicio (11) a través de un cortafuegos (10b), un área de alta seguridad (15) y un área de gestión (16) conectada al área de servicio (11) a través de un cortafuegos (10c).

(0033) La infraestructura del portal puede comprender además un área pública (12) conectada a internet (7) a través de un router de acceso (19a) y un cortafuegos (10a). El área de servicio (11) está conectado a través de un cortafuegos (10b) y un router de acceso interno (19b) a la red de comunicación troncal (4) conectando la infraestructura del portal (2a, 2b) a los sistemas de servidor de registro de datos (3) y a los sistemas de servidor de punto de interconexión (5).

(0034) El área pública (9) es independiente de la parte interna del sistema seguro de red usado para gestionar los expedientes de los pacientes. Contiene un servidor de web (20) y un servidor de nombre de dominio público (DNS) (21).

(0035) Las pruebas de integración de los diversos componentes de la red son efectuados en el área de prueba (13) antes de integrar esos componentes en la red. También aquí se lanzan actualizaciones a la red.

(0036) En el área VPN externa (8) se establecen todas las conexiones de red de estaciones de usuarios. Aquí finaliza el túnel de seguridad entre la estación del usuario y la infraestructura del portal. Este túnel posibilita el acceso seguro y codificado entre la estación del usuario y el sistema de salud informatizado. También es aquí donde se realizan los primeros controles de acceso al sistema y donde se realiza la primera detección de intrusión.

(0037) Todos los accesos a los componentes externos de la red troncal (4) están efectuados desde el área VPN interna (22), tales como acceso a los sistemas de servidor de registro de datos (3) y a los sistemas de servidor de punto de interconexión (5) para la conexión de inter-redes. Aquí se establecen nuevos túneles de comunicación segura entre los mediadores de acceso (25) y los componentes externos de la red troncal (4).

(0038) Todos los servicios denominados "públicos" están situados en el área de servicio (11). Éste área es accesible por las estaciones de usuarios (6) para permitirles acceder a los distintos servicios ofrecidos por el sistema de salud informatizado.

(0039) Los servicios unidos a la seguridad de la red están situados en el área de alta seguridad (15). Esta área es solamente accesible por los servidores que albergan las aplicaciones del sistema de salud informatizado y por el personal de la administración.

(0040) Todos los servicios que están relacionados con la gestión de la infraestructura del sistema de salud informatizado están situados en el área de gestión (16). Esta área es accesible solamente por el personal de administración responsable de las operaciones de gestión de la infraestructura.

(0041) Los routers (19a, 19b) se usan para conectar la red a otras redes en las que están situados varios participantes. Estos routers están situados en la periferia de la red troncal (4), la infraestructura del portal (2a, 2b), los sistemas de servidor del punto de interconexión (5) y los sistemas del servidor de registro de datos (3). Sus parámetros son ajustados para ofrecer un primer nivel de protección a los elementos de la red segura que los mismos conectan. Los routers instalados dentro del sistema de salud informatizado apoyan el filtrado de paquetes, el registro de eventos y las funciones de detección de intrusión en las redes.

(0042) Los cortafuegos son máquinas que hacen posible la protección de toda la red o parte de ella mediante el análisis del contenido de los paquetes, o incluso de las sesiones. Estas máquinas están situadas dentro de la red, justo detrás del router (19a) y son un punto obligatorio de paso para la entrada dentro de la parte de la red que protegen.

(0043) Los cortafuegos (10a, 10b, 10c) instalados en el sistema de salud informatizado apoyan las funciones de filtrado de paquetes, de la inspección de paquetes, del registro de eventos, del antivirus y de defensa activa.

(0044) Hay tres tipos de contrafuegos que son utilizados:

- Los cortafuegos periféricos (10a): estas máquinas se usan en todos los portales. Están situados entre el router periférico (19a) y el concentrador VPN (23) y hacen posible la protección de la red del sistema de salud ante ataques externos. En el momento de un acceso “normal” a la red del sistema de salud, estas máquinas no son capaces de inspeccionar el contenido de paquetes, porque están codificados en un túnel de seguridad (ver abajo). Los parámetros de estos cortafuegos están ajustados para efectuar un control en el nivel de los paquetes (direcciones y origen de puertos y destino). Los cortafuegos periféricos son accedidos por todas las estaciones de usuarios (6) del sistema seguro de red, así como para todos los accesos “públicos” a los servidores (20, 21) del área pública (12).

- Los cortafuegos internos (10b): estas máquinas se usan en todas las partes del sistema seguro de red conectado a la red troncal (4). Están situados en las partes del sistema que comunican con la red troncal (4) y hacen posible inspeccionar paquetes fuera de los túneles seguros para proteger la parte pública del sistema accesible durante las sesiones por los proveedores de cuidados o por los pacientes. Los cortafuegos internos de los sistemas de servidor de interconexión son accedidos por mediadores técnicos de acceso (25) y mediadores del servicio (24). No precisan de otras funciones complementarias, aparte de las mencionadas más arriba. Los cortafuegos internos de las infraestructuras del portal (2a, 2b) se acceden por todas las estaciones de usuarios. Habida cuenta que el servicio, las áreas de alta seguridad y las áreas de gestión usan direcciones privadas de Protocolo de Internet (IP), estos cortafuegos realizan la traducción de direcciones de redes de IP (NAT, en inglés: Network Address Translation), además de las funciones listadas más arriba.

- Los cortafuegos administrativos (10c): estas máquinas se usan en todas las infraestructuras de portal (2a, 2b). Están situados detrás del área de servicio (11) y hacen posible proteger las áreas de alta seguridad y las áreas de gestión (15, 16). Los cortafuegos administrativos (10c) son accedidos por mediadores de acceso (25), los concentradores VPN (23) y el personal responsable de la operación de la infraestructura del sistema de salud informatizado y la gestión de la estructura de la clave pública (PKI, en inglés: Public Key Infrastructure). Todas las funciones a que se hace referencia más arriba se activan en estas máquinas, los parámetros son controlados frecuentemente para asegurar un muy alto nivel de seguridad en las áreas que protegen.

(0045) Para asegurar que las sesiones sean seguras, los túneles seguros (VPN) son establecidos en todas las conexiones de la red que no son seguras. Estos túneles VPN se establecen en los siguientes casos:

- Acceso al sistema de salud informatizado por un usuario (6);

- Acceso al sistema de servidor de registro de datos (3) desde la red troncal (4);

- Acceso al sistema de servidor del punto de interconexión desde la red troncal (4).

(0046) Dos tipos de VPN están presentes en el sistema de salud informatizado:

- Usuario VPN: este VPN usa la tecnología de capa de conexión segura (SSL, en inglés: “Secure Socket Layer”) y están establecidos entre una estación de usuario (6) y la infraestructura del portal (2a, 2b) en el acceso al sistema de salud informatizado. El protocolo SSL se usa para establecer una sesión con uno de los concentradores SSL (23) de la infraestructura del portal. La autentificación por el concentrador SSL VPN (23) usa el certificado de autentificación recuperado por la tarjeta inteligente (8) del usuario.

- Interconexión de red VPN (26): Estos VPN usan la tecnología IPSec o SSL y están establecidos entre los servidores VPN internos de las infraestructuras del portal (2a, 2b) y el servidor VPN (26) del sistema de servidor de registro de datos (3) o el sistema de servidor de interconexión de red (5). Estos túneles seguros

entre dos sitios son permanentes y no precisan autentificación por parte de los usuarios o los mediadores de acceso, porque la comunicación se efectúa entre elementos fiables a través de la red troncal (4).

(0047) Habida cuenta que solamente la red troncal (4) que transporta los datos se considera “insegura”, sólo este canal será codificado. El establecimiento de estos VPN está autentificado por un certificado de autentificación proporcionado para cada sistema de servidor de registro de datos y para cada infraestructura del portal.

(0048) A pesar de que se instalan numerosos mecanismos de protección dentro de la infraestructura del sistema de red seguro, se instala un sistema de detección de intrusión (IDS, en inglés: Intrusion Detection System) en la infraestructura del portal, con la finalidad de lograr una respuesta rápida en el caso de intrusión. Otra función importante del IDS es posibilitar la reconstrucción y seguir la pista a los eventos mediante el análisis de los registros y de otros datos recopilados.

(0049) Estos IDS proporcionan detección, registro, alerta, reacción y servicios de síntesis en relación con cualquier intento de ataque o intrusión dentro del sistema de red seguro. Estos pueden interrelacionarse con otros IDS y usar un lenguaje haciendo posible la definición de normas personalizadas. El IDS incluye funciones del tipo “red” (NIDS) y “hardware” (HIDS).

(0050) La arquitectura del sistema de detección de intrusión está distribuido y es redundante y comprende los siguientes elementos:

- Un sistema de servidor de gestión de seguridad (28) que contiene un software que recupera todos los datos enviados por las pruebas IDS (27) y centraliza esos datos para analizarlos, y si es apropiado, reacciona para alertar a los operadores y/o para bloquear estos intentos de intrusión. Este software está presente en el área de gestión (16) de cada infraestructura de portal (2a, 2b) para ofrecer un nivel adecuado de redundancia. Todos los sistemas de servidor de gestión de seguridad se comunican entre sí con la finalidad de intercambiar información que sea pertinente y necesaria para el funcionamiento correcto de todo.

- Las pruebas IDS (27), que son “rastreadores” especializados que analizan todos los paquetes, protocolos y sesiones que transitan a través del equipo que controlan. Las pruebas están presentes en todos los equipos críticos del sistema de red seguro, en particular, en el router externo (19) de la infraestructura del portal y en los cortafuegos internos y externos. Las pruebas (27) se comunican con el sistema de servidor de gestión de seguridad (28) más cercano y responden con toda la información necesaria a este sistema de servidor para cumplir con su misión apropiadamente.

(0051) El área de servicio (11) del interfaz del portal (2a, 2b) incluye un sistema de servidor que actúa como un mediador técnico de acceso (en adelante: “mediador de acceso”) hacia los datos protegidos, especialmente, a los expedientes médicos, incluyendo el mediador de acceso, por ejemplo, un servidor de acceso (25). El mediador de acceso materializa el punto de entrada en el sistema de salud informatizado de aplicaciones relacionadas con los datos médicos confidenciales distribuidos a través de la red y usados por los profesionales de la salud y por los pacientes. El mediador de acceso (25) oculta la estructura interna de la red y hace posible conservar el control de la seguridad y de los interfaces mostrados a los usuarios (6). Debe hacerse referencia a que el sistema de salud informatizado, de acuerdo con la invención, puede incluir una multitud de servidores de acceso (25), siendo compartido cada uno por diferentes grupos de usuarios, por ejemplo. Para simplificar la operación de los servidores de acceso y para incrementar su eficiencia y velocidad es preferible, sin embargo, que se agrupen en las infraestructuras del portal (2a, 2b). Los servidores de acceso almacenan en la memoria, fundamentalmente, solo datos técnicos y no datos médicos, aunque pueden incluir cachés técnicos para almacenar temporalmente ciertos resultados de búsqueda, tales como direcciones de servidores y datos que constituyen el expediente médico de un paciente, con la finalidad de ser capaz de acceder con más rapidez, cuando una sesión está abierta en la red por un usuario.

(0052) Sin embargo, una vez que la sesión está cerrada, los datos almacenados en este caché se borran/pierden.

(0053) Las funciones principales del mediador técnico de acceso (25) son (véanse las interacciones en la Fig. 2):

- Autentificación por usuarios, incluyendo la verificación de posibles revocaciones (véase también la Fig. 8);

- Autorización: el mediador de acceso efectúa un primer nivel de filtrado de peticiones, de acuerdo con la función relacionada con la identidad de la persona que presenta la petición;

- Gestión de sesiones con usuarios, en particular, recuperación del perfil de acceso del paciente desde un mediador técnico de servicio de registro (29) en uno de los sistemas de servidor de registro de datos (3); Creación y verificación de la validez de los documentos (formato, codificación, atributos, etc.) y transmisión al sistema de servidor de los datos de registro por el profesional de salud afectado (véase también Fig. 9);

- Búsqueda de datos de un expediente médico (véase también la Fig. 10) a petición de una aplicación de consulta, en la que el mediador de acceso de expediente interroga a todos los mediadores del servicio de registro, presentando el documento solicitados a ellos y luego recopila las respuestas de las ausencias a

una respuesta, consolida el resultado y lo devuelve a la aplicación que inició la petición; el resultado de una búsqueda consiste en una lista de referencias de los documentos que pueden ser consultados; los documentos a los que el acceso no está autorizado, no están listados;

- Consulta de datos de un expediente médico (véase también la Fig. 11): basado en una referencia precisa suministrada por una aplicación de consulta, el mediador de acceso del expediente (25) interroga al mediador de servicio de registro (29) afectado y recupera el contenido del documento de referencia; el acceso al documento está registrado por el mediador de acceso;

- Muestra de los derechos de acceso: a petición de la aplicación de gestión de perfil, el mediador de acceso obtiene el perfil de los derechos de acceso del paciente desde un sistema de servidor de registro de datos (a través del sistema de búsqueda descrito arriba) y entonces devuelve el último a la aplicación que inició la petición;

- Modificación de los derechos de acceso (véase también la Fig. 12): a petición de la aplicación de gestión de perfil, el mediador de acceso del expediente (25) actualiza el perfil de acceso almacenado por el mediador del servicio de registro (29) del médico de confianza del paciente afectado;

- Registro del acceso: un registro de cada petición está retenido localmente por el mediador de acceso del expediente;

- Búsqueda de registros de acceso por un paciente determinado por interrogación del registro de aplicación;

- Administración: respuesta a las órdenes definidas por la interfaz común de administración de la aplicación.

(0054) Con esta finalidad, el mediador del acceso colabora con un número de componentes del sistema seguro de red informática, siendo las colaboraciones principales como se expone a continuación:

- El mediador de acceso se usa por el componente de gestión de expediente del paciente, el componente de consulta de expediente virtual (50) y el componente de gestión de perfil de acceso (51);

- El mediador de acceso usa los servicios de seguridad (53) para la autentificación y la autorización basada en rollos, gracias a los certificados contenidos en las tarjetas inteligentes del paciente y del profesional de la salud;

- El mediador de acceso usa el servicio (54) para validar los documentos publicados;

- El mediador de acceso accede a todos los mediadores de servicio de registro (29) para la publicación, búsqueda, consulta y gestión de los perfiles de acceso;

- El mediador usa el servicio de registro de aplicación local (55);

- El mediador de acceso accede a todos los registros de aplicación para reconstituir las ocasiones de acceso al expediente del paciente;

- El mediador de acceso accede al registro (directorio) de los profesionales de la salud (56) para obtener la información necesaria, tal como el identificador del registro del profesional de la salud o su función;

- El mediador de acceso accede a la información de configuración del sistema de salud informatizado (57), tal como la dirección de los registrantes.

(0055) El área de servicio (11) incluye además un sistema de servidor que actúa como el mediador de acceso técnico especializado (24) (en adelante: “mediador de acceso especializado”) que materializa el portal para las aplicaciones de los usuarios a servicios electrónicos de valor añadido (en adelante: “servicios de valor añadido” o SVA), tales como la ayuda para prescribir medicamentos, que forma parte del sistema de salud informatizado. El sistema electrónico de ayuda de prescripción de medicamentos (31) puede comprender una base de datos que almacena en forma electrónica un compendio de medicamentos y un software para determinar la adecuación de un diagnostico como una función de la interacción entre medicamentos, alergias y otras condiciones que surgen del expediente médico del paciente. El mediador de acceso especializado (31) puede incluir un servidor que fundamentalmente almacena solo datos técnicos y que tiene las siguientes funciones:

- Recibir peticiones que vienen directamente del software del usuario a través de un túnel seguro de comunicación;

- Autentificar al usuario y autorizar la petición de acuerdo con los derechos relacionados con su identidad o su función;

- Transmitir peticiones al servicio de valor añadido (31a, 31b) al cual está unido y devolver respuestas para el usuario; desarrolla una función clásica de “proxy” para el protocolo de servicio de valor añadido;

- A petición del servicio de valor añadido, interactúa con el resto del sistema de salud informatizado, especialmente, los mediadores de servicio de registro (29) para obtener información (por ejemplo, en el caso de la ayuda de prescripción de medicamentos);

- Localmente registrar las acciones efectuadas.

(0056) Para las finalidades mencionadas previamente, el mediador de acceso especializado interactúa con los usuarios y otros componentes del sistema seguro informático en las colaboraciones principales siguientes (véanse Figuras 2 y 5):

- El mediador de acceso especializado se usa por los clientes del servicio de valor añadido (6a);

- El mediador de acceso especializado llama y es llamado por el servicio de valor añadido (31a, 31b) al cual está conectado;

- El mediador de acceso especializado (24) (24a, 24b) accede a los mediadores del servicio de registro (29) para buscar y consultar documentos médicos;

- El mediador de acceso especializado usa los servicios electrónicos de seguridad (53) proporcionados en el área de alta seguridad (15) para la autentificación y autorizaciones basadas en las funciones de los usuarios;

- El mediador de acceso especializado usa el servicio electrónico de registro de acceso de la aplicación local (58);

- El mediador de acceso especializado accede al directorio electrónico (56) de los profesionales de salud y a las funciones provistas en el área de alta seguridad (tales como el identificador del sistema de servidor del registro de datos (3a) del profesional de salud afectado);

- El mediador del acceso especializado accede a la información de configuración de la infraestructura del sistema seguro de red informático (tales como las direcciones de los sistemas de servidor del registro), siendo almacenada esta información en un sistema de servidor de gestión de la infraestructura (33) en el área de gestión (16).

(0057) Los servicios de valor añadido, tales como bases de datos de medicamentos y apoyo logístico, pueden ser implementados de un modo centralizado, porque no almacenan información relativa a los pacientes. Esta centralización es solamente “lógica”, sin embargo, no excluye una descentralización “física” por razones de desarrollo y accesibilidad.

(0058) En el nivel de la arquitectura, estos servicios de valor añadido pueden verse, por ello, como cajas negras del sistema de salud informatizado. Están disponibles a los usuarios a través de un mediador de acceso especializado que provee la unión entre el SVA y el resto de la red.

(0059) La Fig. 6 muestra una arquitectura lógica posible para el servicio electrónico de ayuda de prescripción. Este servicio es invocado desde un mediador de servicio de valor añadido (24b), a su vez invocado por un mediador de acceso especializado (24a) (no mostrado en la Fig. 6).

(0060) Este SVA tiene sus propios datos, especialmente, una base de datos de medicamentos (“compendio”) (58) e interacciones potenciales entre medicamentos.

(0061) Más bien, el motor de detección de interacción tiene acceso (59) a las prescripciones actuales del paciente.

(0062) En referencia a las Fig. 1 y 2, el área de servicio (11) puede incluir además un servidor de mensajería seguro (34) usado primeramente para enviar mensajes electrónicos entre los usuarios (6b) del sistema de salud informatizado o para la transmisión y almacenamiento de los datos protegidos, tales como datos médicos de un paciente, en un sistema de servidor de registro de datos (3a). Para proteger los datos transmitidos, los mensajes electrónicos se firman con la clave privada de la tarjeta inteligente del profesional de la salud y enviados a una dirección que corresponde a otro participante, por ejemplo, 123456789@e-toile.ch donde 123456789 es el identificador del participante. El servidor de e-mail acepta solo e-mails que vienen del VPN y la firma que corresponde a un profesional de la salud conocido por el sistema de red seguro. El profesional de la salud puede, por ello, añadir un mensaje mediante un documento adjunto al paciente en la base de documentos del sistema del servidor de registro de datos del profesional de la salud que lo envía.

(0063) El área de alta seguridad (15) incluye un sistema de servidor (32) que incluye un directorio electrónico de profesionales de la salud (57) (en adelante: directorio PDS) usado para autorizar a los usuarios el acceso como una

función de sus cargos, un sistema de gestión de certificado electrónico (35) (en adelante: gestor PKI), que almacena y gestiona los certificados y listados electrónicos de certificados revocados que han sido enviados, y una autoridad electrónica de certificación (36) (en adelante: autoridad de certificación) que actúa como una autoridad para la certificación de la organización del sistema de salud informatizado. Cuando la producción de las tarjetas inteligentes es subcontratada a una organización externa, el sistema de gestión de certificado electrónico (35) y la autoridad de certificación electrónica (36) puede estar fuera del sistema seguro de red informática en un sistema seguro externo bajo el control de la organización responsable para la producción de las tarjetas inteligentes.

(0064) El área de alta seguridad (15) puede incluir además un servidor de nombre de dominio interno (en adelante: DNS interno) (37) para gestionar los nombres de las centrales internas. Cada uno de los componentes del área de alta seguridad puede tomar la forma de un sistema de servidor. La función principal del sistema de servidor del directorio PDS (32) es hacer un inventario de los profesionales de la salud afiliados al sistema de salud informatizado y agrupar la información necesaria sobre este asunto. El sistema de servidor del directorio PDS (32) fundamentalmente almacena datos administrativos, tales como nombre, apellido, dirección, especialidad, etc. del profesional de la salud, certificados digitales de cada profesional de la salud, información sobre los cargos y/o las autorizaciones de los profesionales de la salud, y las direcciones u otra información sobre el sistema de servidor de registro de datos (3a) asociado al usuario. Las funciones principales del directorio de los profesionales de la salud son las siguientes:

- Creación de una nueva entrada en el directorio;
- Modificación de los atributos de una entrada existente;
- Desactivación de una entrada;
- Búsqueda y consulta de entradas en el directorio;
- Importación y exportación por lotes;
- Establecimiento de listas e informes a través de un interfaz de administración humano-mecánico (HMI); Administración: respuesta a las ordenes definidas por el interfaz común de administración de la aplicación.

(0065) El directorio (57) de los profesionales de salud se usa por el servicio de mensajería seguro (34) para obtener la clave publica del destinatario de un mensaje codificado. Los mediadores de acceso (25) también usan el directorio para autorizar peticiones de acuerdo con el cargo del profesional de la salud.

(0066) El gestor PKI (35) puede ser un producto de mercado estándar para la producción, distribución, revocación y verificación de los certificados electrónicos.

(0067) El sistema de servidor de la autoridad del certificado (36) tiene el cargo de autentificar al usuario de la red y de autorizar ciertas peticiones como una función de su cargo.

(0068) El sistema de servidor de la autoridad de certificación fundamentalmente almacena datos en los certificados de la autoridad de certificación que expidió el certificado de las tarjetas inteligentes de los usuarios, así como la revocación o las listas de acceso.

(0069) Las funciones principales de la autoridad de certificación (36) son como se expone a continuación:

- Comprobación de la autenticidad del certificado presentado;
- Verificación de las listas de revocación; Verificación de las autorizaciones relativas al cargo de un usuario;
- Si es necesario: establecimiento del contexto de seguridad de la sesión;
- Administración: respuesta a las ordenes definidas por el interfaz común de la administración de la aplicación.

(0070) La autoridad de certificación es usada, sobre todo, por los mediadores de acceso (25) o por los mediadores de acceso especializados (24). Debe hacerse referencia a que los datos de las listas de revocación también pueden ser almacenadas en otro-s servidores y en este caso, la autoridad de certificación (36) accederá a esos servidores para verificar la lista de revocaciones.

(0071) La zona de gestión (16) incluye un sistema de servidor para la gestión de la infraestructura (33) del sistema de salud informatizado que hace uso de la infraestructura de la red informática posible proporcionando los siguientes servicios electrónicos:

- Vigilancia de eventos críticos (rotura, sobrecarga, superación de capacidad, etc.);

- Histórico centralizado de los eventos históricos del uso del trafico de la red;
- Centralización de las configuraciones de red;
- Centralización de las imágenes de servidor (del tipo “Ghost”);
- Generación de alarmas en el caso de eventos críticos; Posibilidades de distribuir actualizaciones;
- Gestión de alarmas por el equipo y notificación de las alarmas más severas al sistema de problemas de billetaje (TTS, en inglés: Trouble Ticketing System) del servicio de asistencia;
- Gestión del inventario de equipos y versiones de software instalados.

(0072) El área de gestión (16) incluye además un sistema de gestión electrónica aplicativa (38) para administrar y gestionar las aplicaciones del sistema de salud informatizado, especialmente, la administración de las aplicaciones y la gestión de la configuración de varios componentes y aplicaciones del sistema, así como la teledistribución a las estaciones de los clientes (véase también en el titular servidor de instalación).

(0073) Como se describió más arriba, el área de gestión (16) puede incluir igualmente un sistema de servidor de gestión de seguridad (28) para reconstituir o seguir la pista a los eventos analizando los registros y de otros datos recopilados por las pruebas de detección de intrusión (27) instalados en los puntos críticos del sistema de salud informatizado.

(0074) El área de gestión puede incluir también un sistema (39) para producir compact disks u otros medios de comunicación para proveer el expediente a los pacientes que lo requieran, por ejemplo, cuando viajan al extranjero.

(0075) El sistema de gestión de la infraestructura (33) incluye un registro de configuración (57) que mantiene la información común relativa a la configuración lógica y física del sistema de salud informatizado. Los datos almacenados en este registro incluyen además las direcciones de los mediadores, los servicios de valor añadido y los servicios comunes, tales como los registros. El registro que es accesible por todos los componentes internos del sistema de salud informatizado, tiene las siguientes funciones:

- Búsqueda de un elemento de configuración y acceso a su(s) valor(es);
- Importación y exportación por lotes;
- En los casos en que sea posible; descubrimiento automático de ciertos elementos (por ejemplo, mediadores) incluidos en la configuración;
- Mediante HMI o interfaz de administración: creación de una nueva entrada de configuración, modificación o eliminación de una entrada existente, producción de listas.

(0076) Debe hacerse referencia a que las configuraciones privadas especificas de cada componente de aplicación del sistema de salud informatizado no son en principio mantenidas en el registro de configuración, sino por un mecanismo local ad hoc.

(0077) El sistema de servidor de gestión aplicativa (38) que posibilita el uso y el control de los componentes de la aplicación del sistema de salud informatizado puede tener las siguientes funciones:

- Interrogación y muestra del estado de los componentes (automáticamente y en respuesta a una petición del operador);
- Comienzo y detención de los componentes; Modificación de los parámetros de operación de los componentes (si ellos lo permiten);
- Detección de problemas e información a los operadores; Recopilación y muestra de estadísticas (por ejemplo, tiempos de respuesta, contadores);
- Planificación de acciones en componentes (por ejemplo, comienzo automático de las tareas de mantenimiento de los antecedentes);
- Acción automática como una función de ciertos eventos (por ejemplo, reinicio en el caso de un error).

(0078) El área de gestión (16) también puede incluir un servidor de instalación que pone a disposición de los profesionales de la salud software actualizado que permiten el acceso a los servicios del sistema de salud informatizado.

(0079) En la zona pública (9), el sistema del servidor del portal de información (servidor web) tiene el papel principal de proveer información al público y a los profesionales de la salud. Este sistema de servidor almacena datos HTML estáticos y datos estructurados, de acuerdo con lo que esta requerido, este servidor que comunica con el área de administración (16), especialmente, con el sistema de servidor de gestión de infraestructura (33) y la gestión y el sistema de servidor aplicativo (38) para obtener el estado del sistema. Las funciones principales del sistema de servidor del portal de información (20) son las siguientes:

- Distribución de la información estática básica (historia, misión, modos de uso, direcciones de contacto, etc.);
- Distribución de la información de servicio (estado del sistema, problemas, ventana de mantenimiento, anuncios, eventos, etc.)

(0080) El sistema de servidor del portal es accesible sin una conexión VPN.

(0081) El sistema de servidor de registro de datos (3) que está conectado a la red troncal (4) por un router interno (19b) y un túnel seguro VPN interno (26) a través de un cortafuegos interno (10b) incluye un sistema de servidor que actúa como mediador técnico del servicio de registro (29) (en adelante: mediador del servicio de registro) y un servidor de documentos (40). El mediador del servicio de registro (29) gestiona el acceso a los datos almacenados en el servidor de documentos (40) cuando se invoca por los mediadores de acceso (24, 25) para acceder a los varios componentes del sistema de servidor de registro (3). El mediador del servicio de registro también accede a los servicios de registro locales (59) para mantener un registro de todas las operaciones efectuadas por uno o mas componentes del sistema del servidor de registro de datos. Las principales funciones del mediador de registro de datos son las siguientes:

- Publicación: recibe un documento para ser publicado por cuenta del mediador de acceso del expediente (25) y lo confía al servidor de documentos (40) para el almacenamiento; crea y también almacena en el servidor (40) la referencia única de cada documento de un paciente;
- En cuanto a la publicación del primer documento de un paciente en el registro correspondiente: creación del expediente y del perfil de acceso del paciente;
- Búsqueda: al recibir una petición de búsqueda de documento de un mediador de acceso del expediente, el mediador de servicio del registro busca el servidor de documentos (40) para las referencias de los documentos correspondientes a los criterios de búsqueda, verifica y devuelve los resultados al mediador de acceso de expedientes;
- Verifica la aplicación correcta de los derechos de acceso;
- Consulta de documentos: al recibir una petición de consulta de documentos de un mediador de acceso de expedientes, el mediador de servicios de registro, si es necesario, verifica la referencia (por ejemplo, si esta formulada correctamente y si aún es válida), verifica los derechos de acceso aplicables y obtiene el documento del registro;
- Verificación de los derechos de acceso relativos a los perfiles de acceso y a las excepciones especificadas por el paciente;
- Actualización de los perfiles de acceso por defecto de los pacientes (no específicos de un documento);
- Actualización de excepciones (específicos de un documento) en los derechos de acceso;
- Registro de peticiones;
- Gestión de errores del registro de gestión: siempre que sea posible, el mediador de servicio del registro protege al resto de las redes de errores de registro (incluyendo el procesamiento de cualquier tiempo de espera); Administración: respuesta a las ordenes definidas por el interfaz común de administración aplicativa.

(0082) Debe hacerse referencia a que cada mediador de registro de datos sabe solamente los documentos que gestiona y los pacientes para los cuales mantiene un documento, y el expediente completo de un paciente puede ser distribuido, por ello, a través de una multitud de registros de datos, de este modo evitando el almacenamiento de un expediente médico completo en un único servidor o en el registro central. Esto aumenta enormemente la protección de unos datos médicos de un paciente, habida cuenta que es extremadamente difícil para una tercera persona, piratear una multitud de sistemas de seguridad para reconstituir el expediente completo.

(0083) Por razones de desarrollo, el mediador del registro de servicio está preferiblemente físicamente cerca del servidor de referencia (41) y del servidor de documentos (40). El cargo del servidor de referencias permite encontrar, sobre la base de los criterios de búsqueda, las referencias sobre los documentos registrados. Los datos almacenados en el servidor de referencias son fundamentalmente las referencias a los documentos almacenados en

el servidor de documentos (40), los atributos de esos documentos y los índices.

(0084) El servidor de referencia también puede incluir, o al menos accede, a un registro (básico) de los derechos de acceso (60) específicos de los documentos, estando situado este registro preferiblemente en, al menos, un sistema de servidor de registro de datos (30), especialmente, el sistema de servidor de registro del médico de confianza del paciente.

(0085) Las funciones principales del servidor de referencia (41) son las siguientes: Almacenamiento de las referencias a los documentos; Almacenamiento de los atributos necesarios para las búsquedas; Creación y gestión de índices necesarios para las búsquedas; Búsqueda de referencias usando los criterios basados en atributos (identidad del paciente, tipo de documento, datos, etc.) teniendo en cuenta las restricciones de acceso impuestas por el paciente.

(0086) Debe hacerse referencia a que el servidor de referencia (41) podría estar integrado dentro o formar parte del servidor del documento (40), o al menos, compartir las mismas estructuras de datos.

(0087) Cuando se buscan los documentos (véase también la Fig. 10), un mediador de acceso de expedientes interroga a todos los mediadores del servicio de registro y espera de cada uno de ellos una respuesta positiva o negativa. Esto conduce a la carga de la red, el mediador de acceso (que debe gestionar un gran número de participantes simultáneamente) y cada mediador de servicio que tiene que responder a cada petición, lo consiguen. Esto constituye el riesgo de que el desarrollo de las operaciones de petición estén por debajo de la aceptabilidad y que en el caso de un aumento eventual del numero de los registrantes del servicio (y por ello, el numero de los mediadores de servicio y servidores de referencia) se degrade el desarrollo en su conjunto de la red.

(0088) Con la finalidad de prevenir estos problemas potenciales, es posible instalar servidores de referencia intermediarios haciendo un índice de la existencia de documentos o, más ampliamente, un expediente relativo a un paciente en un registro particular, como se muestra en la Fig. 1a.

(0089) El registro de los derechos de acceso específicos a los documentos (61) tiene la función de gestionar la lista de excepciones de acceso, especialmente, aquellos que son requeridos por el paciente. Este registro puede ser integrado en el servidor de referencia usando las mismas estructuras de datos que el anterior, pero igualmente podría ser una entidad distinta del servidor de referencia. El registro (61) de los derechos de acceso específicos a los documentos (también denominado “registro de excepciones”) tiene las siguientes funciones principales:

- Almacenamiento de las excepciones autorizando el acceso por personas especificas a ciertos documentos;
- Búsqueda de estas excepciones usando criterios relativos al paciente, el profesional de la salud, el documento u otros datos asociados con el expediente médico.

(0090) Las interacciones del registro de los derechos específicos (61) de acceso a los documentos son principalmente los siguientes:

- Consulta por el mediador de servicio de registro (29) en el momento de buscar y consultar documentos;
- Actualización por el mediador del servicio de registro en el contexto de la gestión de los derechos por los pacientes;
- El mediador del servicio de registro registra una nueva excepción la primera vez que un profesional consulta un documento para garantizarles el acceso subsecuente, incluso en el caso de la modificación de las restricciones por el usuario;
- Colaboración con los otros componentes del registrante de las operaciones de mantenimiento (por ejemplo, preservación de la integridad referencial en el caso de la eliminación de documentos).

(0091) El sistema del servidor de documentos (40) tiene la función de almacenar de forma fiable y permanente los documentos del expediente médico de un paciente. Los datos almacenados en la base de datos de este servidor pueden estar codificados o no. Las funciones principales del sistema de servidor de documentos son las siguientes:

- Acepta y almacena los nuevos documentos;
- Al presentar su referencia, suministra los documentos requeridos para su consulta;
- Elimina los documentos obsoletos, de acuerdo con las normas impuestas por el administrador del sistema;
- Importa y exporta documentos (separadamente o en lotes);
- Si es aplicable: gestiona versiones de documentos.

(0092) El mediador del registro de datos (29) accede a la base de documentos del servidor de documentos (40) en el momento de la publicación, la búsqueda y la consulta de documentos, como se muestra en las Fig. 9, 10 y 11.

(0093) En la aplicación presente, el término “publicación” se usa en relación con la presentación de documentos para la operación de crear y almacenar documentos en un servidor de documentos, poniendo a disposición de los usuarios el sistema de salud informatizado. Para ser capaces de publicar el expediente del paciente, el sistema de salud informatizado incluye una aplicación de publicación del expediente del paciente (63) que genera y almacena nuevos documentos de acuerdo con el procedimiento mostrado en la Fig. 9. La aplicación de la publicación accede a los certificados y a las funciones de la tarjeta inteligente (8) a través del lector de la tarjeta inteligente (9) y delega todas las peticiones de la red al mediador de acceso del expediente (25) de la infraestructura del portal (2a, 2b).

- Las funciones principales de esta aplicación son las siguientes:
- Autentificar al profesional de la salud mediante su tarjeta inteligente;
- Transmitir documentos a ser publicados a través de la red (los documentos se preparan localmente tanto por aplicaciones dedicadas o por herramientas de automatización de la oficina convencional);
- Si es aplicable: manteniendo la lista de los documentos publicados y sus referencias en el sistema de red seguro.

(0094) Debe hacerse referencia a que la tarjeta inteligente del paciente no es necesaria para publicar los documentos, sino que lo es el identificador del paciente. La aplicación no posibilita la modificación de los documentos publicados, para prevenir un abuso, y en el caso de una modificación es necesario producir nuevas versiones de los documentos.

(0095) La aplicación puede ser implementada a través de un interfaz de usuario grafico clásico (GUI, en inglés: Graphical User Interface) o un servidor de presentación WEB accedido por un navegador. El sistema de salud informatizado también incluye una aplicación de consulta de expedientes (50) para permitir al profesional de la salud o al paciente consultar su expediente almacenado en los varios sistemas de servidor de registro de datos, de acuerdo con sus autorizaciones y sus perfiles de acceso.

(0096) Esta aplicación accede a los certificados y a las funciones de la tarjeta inteligente a través del lector de la tarjeta inteligente y delega todas las peticiones al mediador de acceso del expediente (25) en la estructura del portal (2a, 2b). Esta aplicación también permite comunicarse con aplicaciones externas para visualizar ciertos tipos de documentos (por ejemplo, Acrobat, Viewer Graphic). En cuanto a la aplicación de la publicación, esta aplicación de consulta puede ser implementada a través de un cliente GUI clásico o a través de un servidor de presentación WEB accedido por un navegador.

(0097) Las principales funciones de la aplicación de consulta del expediente son las siguientes:

- Autentificación del profesional de la salud y del paciente mediante sus tarjetas inteligentes;
- Búsqueda de referencias de documentos que constituyen el expediente virtual del paciente, en base a los criterios a ser definidos (tipo de documento, datos de publicación, origen, etc.)
- Consulta: búsqueda y muestra de documentos seleccionados de las referencias devueltas por la búsqueda;
- Impresión de un documento mostrado, incluyendo información de rastreo; Cuando sea aplicable: almacenamiento de las referencias de los documentos ya consultados;
- Acceso a la información en una emergencia sin la tarjeta del paciente (pero siempre con la tarjeta del profesional).

(0098) Otra aplicación separada o integrada dentro de la aplicación de publicación del expediente del paciente es una aplicación de validación de documento (54) que asegura que los documentos publicados satisfacen los requerimientos de la red segura.

(0099) Esta aplicación se usa por el mediador de acceso del expediente (25) en el momento de la publicación y tiene las siguientes principales funciones:

- Verificación de conformidad (formato, codificador, sintaxis, normas estructurales, tamaño);
- Cuando sea aplicable, realización de los atributos del documento;
- Administración: respuesta a las ordenes definidas por el interfaz común de administración de la aplicación.

(0100) Una aplicación importante del sistema de salud informatizado es la aplicación de gestión del perfil de acceso (51) que permite a un paciente gestionar sus perfiles de derechos de acceso y visualizar el registro de acceso a sus expedientes. Esta aplicación accede a los certificados y a las funciones de la tarjeta inteligente (8) a través del lector de tarjeta inteligente (9) y delega todas las peticiones al mediador de acceso del expediente (25). Esta aplicación puede ser implementada por un GUI clásico o por un servidor de presentación WEB a través de un navegador. Las funciones principales de la aplicación de gestión de perfil de acceso (51) son las siguientes:

- Autentificación del paciente mediante su tarjeta inteligente;
- Búsqueda y muestra del perfil de los derechos de acceso del paciente;
- Modificación del perfil de los derechos de acceso y actualización del mismo en la red;
- Búsqueda (en los registros) del acceso a los expedientes del paciente en un periodo determinado, seguido de la muestra de los resultados;
- Renovación del certificado de la tarjeta inteligente: una aplicación de cliente de la red segura tiene que tener la función de renovar el certificado inscrito en la tarjeta inteligente; la aplicación de la gestión del perfil de acceso puede, por ello, tener esta función.

(0101) El perfil de acceso de un paciente está almacenado en un registro de perfil de acceso (60) (también se le hace referencia como base de derechos de acceso) que preferiblemente está almacenado en un mediador de servicio de registro (29) de un modo centralizado, para hacer más difícil obtener acceso ilícito a las restricciones de acceso del documento.

(0102) En lugar de almacenar el registro de perfiles de acceso en el mediador de servicio de registro (29), igualmente se puede situar en el servidor de documentos (40), en el cual el documento afectado está almacenado. Este registro se usa por el mediador de servicio de registro a petición del mediador de acceso de expediente (25) en el momento del comienzo de una sesión o en el contexto de la gestión de los derechos de acceso del paciente. Las principales funciones del registro de perfil de acceso son las siguientes:

- Creación de un perfil de acceso en la primera visita del paciente;
- Modificación de las restricciones de acceso;
- Eliminación del perfil de acceso de un paciente determinado;
- Selección del perfil de acceso de un paciente determinado;
- Administración: respuesta a las ordenes definidas por el interfaz común de administración de la aplicación.

(0103) El acceso por un profesional de la salud a los documentos publicados en la red del sistema de salud informatizado está subordinado a la verificación con tres niveles de control. El primer nivel corresponde a la función del emisor de la petición. Este puede ser un médico, una enfermera o un farmacéutico, por ejemplo, y este nivel está relacionado con ciertas autorizaciones para el acceso a las funciones de la red. Por ejemplo, una enfermera puede consultar pero no publicar. El segundo nivel consiste en el perfil de acceso definido por el paciente. Por ejemplo, esto hace posible prohibir el acceso a todos los expedientes ginecológicos y documentos por los profesionales encargados, pero autorizarlo a los médicos de confianza. El tercer nivel se materializa por las excepciones específicas de los médicos y de los documentos o expedientes particulares. Por ejemplo, es posible autorizar el acceso al informe de la visita ginecológica al médico X en una fecha específica en la que el médico X es el médico encargado, pero no el médico de confianza.

(0104) Los niveles segundo y tercero son, por ello, procesados conjuntamente, para autorizar un acceso prohibido por el segundo nivel, pero autorizado bajo determinadas circunstancias para el tercer nivel.

(0105) Una solución consiste en mantener el perfil de acceso con los datos registrando al médico de confianza y proveyendo las listas de control de acceso (ACL, en inglés: Access Control List) para cada documento, incluyendo estos ACL solamente las excepciones de acceso, no los perfiles en sí.

(0106) Con la finalidad de solicitar los controles de acceso relativos a los perfiles, el mediador de acceso del expediente (25) tiene que suministrarlo a los mediadores del servicio de registro (29) en el momento de cada petición. Para una petición de búsqueda (véase Fig. 2 y 10), el mediador de acceso del expediente tiene que recuperar el perfil de acceso en el espacio de los derechos de acceso (60) desde el mediador del servicio del registro (29) del sistema de servidor de registro del documento del médico de confianza, antes de interrogar todas las bases de derechos de acceso (60', 60'') de los otros mediadores de registro (29', 29''). Con la finalidad de evitar esta sub-petición adicional en cada petición por el software del cliente, el mediador de acceso (25) puede mantener el perfil de acceso temporalmente en la información de la sesión.

(0107) La modificación del perfil de acceso por el paciente (véase también la Fig. 12) supone solo actualizar el perfil almacenado por el documento registrando al doctor de confianza sin modificar el ACL de todos los documentos.

(0108) Otra solución para implementar la estrategia de control de acceso podría ser para el ACL de cada documento la inclusión del perfil de acceso definido por el paciente, de manera que el cumplimiento con el ACL podría ser suficiente para solicitar los niveles de control segundo y tercero (2 y 3). Por su parte, el perfil de acceso siempre se almacena en el sistema de servidor de registro de datos del médico de confianza. En el momento de actualizar el perfil, entonces es necesario actualizar el perfil almacenado en el documento, registrando al médico de confianza y modificar todos los ACL de todos los documentos ya publicados.

(0109) Haciendo referencia a las Fig. 1, 2 y 8, una sesión está abierta por una aplicación de usuario después de que el túnel seguro VPN esté establecido entre la estación del profesional de la salud (6) y la infraestructura del portal (2a, 2b). Habida cuenta que al establecer el VPN se requiere la autentificación del servidor VPN (23) por el usuario y que todos los servidores en la estructura de portal pueden ser considerados como seguros, no es necesario que la aplicación del usuario autentifique de nuevo los servidores con los cuales se comunica (por ejemplo, un mediador de acceso).

(0110) Por otro lado, es necesario identificar y autentificar al usuario al servidor de autoridad de certificación (36) (también se le hace referencia como el “servidor de seguridad”) para por último saber la identidad de la persona que abre una sesión de aplicación y que efectúa acciones de acuerdo con su identidad y los derechos asociados.

(0111) Un profesional de la salud está sujeto al sistema de servidor de registro de datos especifico (3a, 3b, 3c) que puede elegir. En el momento de la publicación de un documento, el último está almacenado en este sistema de servidor de registro de datos tras pasar varios niveles de autorización y validación, como muestra la Fig. 9.

(0112) La Fig. 10 muestra el progreso de una petición de búsqueda de documentos que usa dos mecanismos muy importantes:

- La distribución de las peticiones de búsqueda por el mediador de acceso del expediente a todos los mediadores del servicio de registro;

- La verificación de los derechos de acceso basados en los perfiles de restricción y listas de excepción en el nivel de cada mediador de servicio de registro (y por ello, de un modo totalmente descentralizado).

(0113) Se hace referencia a que el perfil de acceso es transmitido por el mediador de acceso a los varios mediadores de servicio en el momento de la búsqueda. Este perfil de acceso se recupera, primeramente, por la búsqueda exhaustiva de los mediadores de servicio para descubrir cuál de ellos tiene el perfil de acceso del paciente (el mediador del servicio de registro (MS) del médico de confianza del paciente solamente responderá positivamente). Una vez que el perfil ha sido recuperado, el mediador de acceso puede mantenerlo como datos de sesión para acelerar las peticiones subsiguientes (otras búsquedas o consultas).

(0114) Haciendo referencia a la Fig. 11, la consulta de un documento consiste en obtener todo el documento basado en su referencia. Para conseguir este objetivo, el mediador de acceso (25) se comunica directamente con el mediador del servicio de registro (29) afectado. A pesar de que los derechos de acceso son verificados en el momento del paso de la búsqueda, tienen que ser verificados de nuevo en el momento de la consulta para protegerse de la situación en que una referencia se pase a otra persona que no tenga los derechos requeridos.

(0115) Por otra parte, un profesional que haya accedido a un documento una vez tiene que ser capaz de acceder de nuevo, incluso si el paciente cambia los derechos de acceso en ese intervalo de tiempo. Esto se logra mediante la inscripción de la identidad del profesional en la lista de las excepciones relativas al documento en el momento de la primera consulta.

(0116) Como se describe anteriormente, el paciente puede modificar los perfiles de acceso de información, dividiéndose los derechos en dos tipos distintos: restricciones basadas en perfiles de documentos y excepciones autorizando el acceso a documentos específicos o a expedientes por personas particulares.

(0117) Para actualizar el perfil de acceso (véase la Fig. 12), el mediador de acceso del expediente (25) contacta con el mediador del servicio de registro (29) del médico de confianza del paciente y les provee con nuevos perfiles a ser guardados. Para actualizar las excepciones de acceso, el mediador del acceso del expediente transmite a cada mediador del servicio de registro (29’) las excepciones que están afectadas. Las excepciones están almacenadas en la base de derechos de acceso (60’) del sistema del servidor de registro de los expedientes correspondientes. Los pasos que modifican los derechos de acceso están mostrados en la Fig. 12.

(0118) La Fig. 13 muestra como el servicio de valor añadido (31a, 31b), en este caso, la ayuda de prescripción de medicamentos, está integrado dentro de la red segura.

(0119) La prescripción de medicamentos electrónica incluye un valor añadido real si está apoyado por un sistema para detectar interacciones de medicamentos. En el contexto del sistema de salud informatizado, el servicio de

medicamentos obtiene información de todas las prescripciones actuales de los pacientes afectados de los mediadores del servicio de registro (29, 29') para detectar posibles incompatibilidades entre los medicamentos prescritos por diferentes profesionales.

(0120) Para prevenir problemas relacionados con incompatibilidades de medicamentos, el sistema de ayuda de prescripciones busca todas las prescripciones actuales publicadas en la red del sistema de salud informatizado, a pesar de las restricciones de acceso definidas por el paciente. Sin embargo, en el caso de que esté probada la incompatibilidad, la persona que prescribe es avisada, pero de modo que la información a la cual no tienen acceso normalmente, no se les revela.

(0121) Haciendo referencia a las Fig. 1 y 2, el sistema de servidor del punto de interconexión (5) incluye un mediador del servicio externo (30) que actúa como un portal entre el sistema de salud informatizado y otras redes de valor añadido o redes médicas. Las funciones principales de este sistema de servidor de punto de interconexión (5) son las siguientes:

- Autentificación mutua;
- Conversión de formato y protocolo;
- Transmisión de mensajería;
- Aplicación "proxy";
- Gestión de errores;
- Administración: responde a las órdenes definidas por el interfaz común de administración de la aplicación.

(0122) El sistema de salud informatizado incluye además registros aplicativos (55, 58, 59) para guardar un registro de las operaciones efectuadas por uno o más componentes de la red, siendo accesibles estas aplicaciones por cualquier componente local. Para no crear un punto de centralización de los datos confidenciales, cada mediador técnico está provisto de su propio registro de aplicación que hace posible desarrollar a posteriori controles en el caso de problemas (acceso ilícito, decisión terapéutica pobre a la vista de la información suministrada por la red, etc.). Los datos procesados por el registro de aplicación incluyen una marca del tiempo (en inglés: "timestamp"), la identificación de los usuarios que participan en la operación, la naturaleza de la operación, la identificación de los documentos afectados, y otros parámetros pertinentes de la operación.

(0123) Las funciones principales de los registros de la aplicación son las siguientes:

- Almacenamiento de un registro;
- Interrogación: búsqueda y suministro de registros correspondientes a un criterio de búsqueda que contienen los parámetros almacenados;
- Limpieza de los registros obsoletos, si fuera necesario;
- Administración: responde a las órdenes definidas por el interfaz común de administración de la aplicación.

(0124) La red troncal (4) es una red de comunicación de alta velocidad de bits entre las infraestructuras del portal (2a, 2b) y los sistemas de servidor de registro de datos (3), así como los sistemas de servidor de punto de interconexión (5). Todos los datos que circulan en la red troncal están codificados, la función de codificación/ descodificación de datos es tratada por los concentradores VPN situados en las infraestructuras del portal y en cada sistema de servidor de registro de datos y cada sistema de servidor del punto de interconexión. En el ejemplo descrito, la red troncal es una red cerrada del tipo lógico, como una red regional o metropolitana cerrada (red de ciudad) que usa una infraestructura de fibra óptica, dedicada a un grupo de usuarios autorizados. Igualmente es posible, siempre que esté disponible, emplear una red cerrada basada en una infraestructura privada, por ejemplo, de un uso único para el sistema de salud informatizado.

(0125) El sistema de salud informatizado tiene preferiblemente, al menos, dos puntos de infraestructura de acceso (2a, 2b) localizados en diferentes lugares para aumentar la seguridad de los datos técnicos y administrativos almacenados y para proporcionar el acceso a la red y asegurar que funcione en el caso de un fallo de uno o más componentes de una de las infraestructuras del portal.

(0126) Haciendo referencia a la Fig. 4, los portales incluyen la redundancia en dos niveles:

- En el nivel general, cada infraestructura del portal es capaz de funcionar independientemente y hacerse cargo de todo el tráfico tratado por el otro en el caso de un fallo u operación preventiva del mismo.

- En el nivel de cada portal, la redundancia se presenta tanto en el nivel de los cortafuegos (10) (“clusters”) y en el nivel de los conmutadores sensitivos (duplicación de equipos y conexiones entre los mismos).

(0127) Un único fallo de un equipo, por ello, no debería conducir a que la infraestructura del portal se extraiga del servicio. Para ofrecer protección de este modo frente a un fallo de una de las infraestructuras del portal en la red troncal (4), un enlace directo de fibra óptica (17) conecta a los dos concentradores intersite VPN (18) de cada infraestructura del portal.

(0128) Las dos infraestructuras de portal están además conectadas por enlaces directos de fibra óptica al nivel de las áreas de servicio y al área de alta seguridad. Esto hace posible la reproducción de varios servidores y datos que tiene que ser consistente entre ambos lugares sin sobrecargar innecesariamente el acceso a la red troncal o la trayectoria interna a través de uno o incluso dos cortafuegos. Las redes de área local virtuales (VLAN, en inglés: Virtual Local Area Network) comunes a ambas infraestructuras de portal pueden, por ello, ser creadas, por ejemplo, usando el protocolo Ethernet Gigabit 802.1q.

(0129) Por ello, tres pares de fibras ópticas son preferiblemente conectadas a las infraestructuras de portal para proveer funciones de redundancia y reproducción entre los dos portales.

(0130) Por ejemplo, dos plataformas técnicas en las que se basa el sistema de salud informatizado pueden resumirse en la tabla siguiente:

Elemento	Plataforma A	Plataforma B
Sistema operativo	Unix y Linux	Windows (servidor 2003 o posterior)
Servidor web	Apache / Tomcat	IIS con apoyo ASP.NET
Servidor de la aplicación	JBoss	.NET Framework
Middleware	RMI/IIOP + SOAP	.NET Remoting + SOAP
Servidor de base de datos	Oracle	Oracle o servidor SQL
Servidor LDAP	OpenLDAP	Directorio Activo de Windows

(0131) Para la comunicación entre el software del cliente y un mediador de acceso, para permitir a diferentes publicadores de software que integren la publicación del documento, los servicios de búsqueda y consulta en el sistema de salud informatizado, es ventajoso proponer un interfaz de comunicación abierto. En esta línea de pensamiento, un interfaz del tipo de servicios Web basado en SOAP/HTTP puede ser usado en el estado actual de la tecnología.

(0132) Para la comunicación entre el mediador de acceso y el mediador de servicio, siendo los mediadores componentes de software técnico internos al sistema de red de seguridad, la elección de un interfaz estándar entre el último depende de su implementación. Una implementación basada en J2EE puede usar RMI/IIOP, una implementación basada en .NET puede usar .NET Remoting, pero existen otras posibilidades: JXTA (comunicación en el mismo nivel), servicios Web, colas de mensajes, etc.

(0133) El interfaz de base de datos para acceder a las bases de datos (fundamentalmente, por los mediadores de servicio) pueden emplear los estándares clásicos, que son JDBC en el universo Java o ODBC y ADO en el universo Microsoft.

(0134) El interfaz de administración de los componentes gestionados por el sistema de red seguro, tales como los mediadores, pueden usar los estándares más apropiados para la plataforma de implementación (RMI/IIOP, JMX, Servicios Web, WMI, etc.)

(0135) Para el interfaz del directorio, el sistema de red seguro incluye un directorio central de los profesionales de la salud usado por usuarios a través del servicio de mensajería seguro, así como por los profesionales de la salud. El acceso a este directorio puede emplear el estándar LDAP. Por otro lado, el sistema de red segura actualiza un registro del conjunto de los mediadores de servicio que forman parte de la red, para que los mediadores de acceso sepan adónde redirigir las solicitudes de gestión de documentos. Este registro podría ser visto como un recurso LDAP de la red.

(0136) El diagrama de la Fig. 3 ilustra la transposición del modelo de arquitectura lógica de acuerdo con las elecciones tecnológicas descritas más arriba. Esta solución está basada en las tecnologías Java/J2EE, pero otras soluciones que usan otras tecnologías, como .Net son posibles. La arquitectura es del tipo de niveles “n”: está dividida en niveles que separan claramente las responsabilidades respecto a la presentación, la lógica de especialidad y el almacenamiento de datos. La parte superior representa el nivel del cliente, materialmente presente con los profesionales de la salud accediendo al sistema de salud informatizado. La parte central materializa el nivel de presentación y los servicios de especialidad relacionados con el sistema de salud informatizado: mediadores de acceso y de servicio, servidor de mensajería, servicios de valor añadido. Finalmente, la parte baja comprende los componentes técnicos del sistema de salud informatizado y las bases de datos.

(0137) En lo que concierne al acceso por los usuarios (clientes), los interfaces adoptados están basados en las tecnologías abiertas e independientes de cualquier plataforma especifica (HTTP, SOAP, SMTP, POP3, LDAP, etc.).

Los interfaces más técnicos usados dentro del sistema seguro de red están relacionados con las tecnologías del universo Java, en este caso, fundamentalmente RMI/IIOP y JDBC.

(0138) El nivel de presentación Web usa servicios HTTP que se sirven de páginas HTML estáticas (Apache, por ejemplo) y de páginas dinámicas del tipo JSP y Servlet.

REIVINDICACIONES

1ª.- Sistema seguro de red informática para la gestión de datos protegidos, accesibles por usuarios (6) provistos de tarjetas inteligentes para la autentificación y autorización de usuarios al sistema, comprendiendo el sistema, al menos, una infraestructura de portal (2a, 2b) conectada mediante una red de comunicación troncal cerrada (4) a una multitud de sistemas de servidor de registro de datos (3a, 3b, 3c) situados en diferentes lugares, comprendiendo cada sistema de servidor de registro de datos, al menos, una base de datos en la cual se almacenan datos protegidos que constituyen documentos, y un mediador técnico del servicio de registro (29) para gestionar el acceso a los documentos almacenados en la base de datos, siendo distribuidos los diferentes documentos que forman un expediente relativo a una persona, posiblemente, a través de una multitud de sistemas de servidor de registro de datos, comprendiendo la infraestructura de portal, al menos, un mediador de acceso del expediente (25) en la forma de un sistema de servidor con aplicaciones que controlan y gestionan el acceso de los usuarios (6) a los documentos almacenados en los sistemas de servidor de registro de datos, que se caracteriza por que el mediador de acceso de expediente (25) está configurado para distribuir a todos los mediadores técnicos del servicio de registro (29) una petición de búsqueda de documento por un usuario autorizado del sistema de salud informatizado y los mediadores técnicos del servicio de registro (29) están configurados para verificar los derechos de acceso del usuario en base a los perfiles de derechos de acceso, y el mediador de acceso del expediente (25) está configurado de modo que, en el momento de la consulta de un documento, el mediador de acceso del expediente (25) se dirige directamente al mediador técnico del servicio de registro (29) afectado directamente después de un paso de búsqueda del documento y vuelve a verificar los derechos de acceso a los documentos relativos al usuario solicitando la consulta antes de transmitirla al usuario.

2ª.- Sistema conforme a la reivindicación 1ª, caracterizado por que el sistema de servidor de registro de datos comprende un servidor de documento (40) y un registro (61) que contiene información sobre los derechos de acceso a los diferentes documentos almacenados en ese servidor para determinar los derechos de acceso a los documentos de un expediente en función de la identidad ó del cargo del usuario que solicita acceso al expediente.

3ª.- Sistema conforme a la reivindicación 2ª, caracterizado por que el registro de acceso tiene la forma de un registro de excepciones que almacena información sobre los accesos no autorizados.

4ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que comprende un área de servicio en la cual está situado el mediador de acceso de expediente (25) y un área de alta seguridad (15) separada del área de servicio por un cortafuegos (10c), comprendiendo el área de alta seguridad un sistema de servidor de autoridad de certificación (36) en el cual se almacenan datos en certificados electrónicos correspondiendo a certificados electrónicos almacenados en las tarjetas inteligentes de los usuarios.

5ª.- Sistema conforme a la reivindicación precedente, caracterizado por que el área de alta seguridad comprende un directorio electrónico de informaciones sobre los usuarios que contiene la identidad y el cargo de esos usuarios.

6ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que hay, al menos, dos infraestructuras de portal físicamente separadas (2a, 2b) y conectadas por la red de comunicación troncal (4).

7ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que las infraestructuras de portal comprenden un área VPN, Red Privada Virtual, externa (8) conectada a través de un cortafuegos (10b) a un área de servicio (11) en el cual se encuentra el mediador de acceso del expediente (25), conectado a una zona de alta seguridad (15) a través de un cortafuegos (10c).

8ª.- Sistema conforme a la reivindicación precedente, caracterizado por que la zona VPN externa (8) comprende un concentrador VPN, que es un concentrador SSL (25), capa de conexión segura, para la comunicación a través de Internet (7) con estaciones de usuarios (6) a través de un túnel de comunicación seguro.

9ª.- Sistema conforme a una de las reivindicaciones 7ª u 8ª, caracterizado por que el área de servicios comprende un mediador de acceso especializado (24) en la forma de un sistema de servidor con aplicaciones para gestionar el acceso de los usuarios a los servicios electrónicos de valor añadido.

10ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que el servidor de documentos (40) del sistema de servidor de registro de datos está separado del servidor del mediador técnico del servicio de registro (29) y conectado a la red troncal (4) a través de un cortafuegos (10b).

11ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que cada sistema de servidor de registro de datos comprende un registro electrónico para registrar todas las peticiones referentes al almacenamiento o a la lectura de los datos protegidos.

12ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que la infraestructura de portal comprende un área de gestión (16) que comprende sistemas de servidor (33, 38, 28) para la gestión de la infraestructura y las aplicaciones del sistema de red informatizado seguro, estando este área separada del área de servicio en la cual se encuentra el mediador de acceso de expedientes (25) y siendo accesible solamente por el personal administrativo responsable de las operaciones de gestión de la infraestructura.

13ª.- Sistema conforme a la reivindicación precedente, caracterizado por que el área de gestión comprende un sistema de servidor de gestión de seguridad (28) conectado a los sensores del detector de intrusión (27) instalados en las líneas de comunicación del sistema de red seguro (2) y teniendo aplicaciones para reconstituir o trazar los eventos analizando los registros de la infraestructura del portal y los sistema del servidor del registro de datos (3a, 3b, 3c), así como los datos transmitidos por los sensores de detector de intrusión.

14ª.- Sistema conforme a la reivindicación 12ª o 13ª, caracterizado por que el área de gestión comprende un sistema de servidor de gestión de infraestructura (33) que comprende un registro de configuración (57) en el cual está almacenada información relativa a la configuración lógica y física del sistema de red informatizado seguro, incluyendo las direcciones de los mediadores y de los sistemas de servidor para los servicios de valor añadido.

15ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que la infraestructura de portal comprende un servidor de mensajería seguro para enviar los mensajes electrónicos entre los usuarios o para la transmisión de los datos protegidos, usando el servidor de mensajería seguro claves electrónicas privadas de las tarjetas inteligentes de los usuarios para codificar los datos transmitidos.

16ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que comprende uno o más sistemas de servidor de punto de interconexión (5) conectados, por un lado, a las infraestructuras de portal (2a, 2b) a través de la red troncal (4), y por otro lado, a otras redes o a los servicios de valor añadido, comprendiendo el sistema de servidor del punto de interconexión un mediador de servicios externos (30) que actúa como un puente entre el sistema de red informatizado seguro y las otras redes y comprendiendo las funciones de autentificación mutua, de conversión de formato y de protocolo y de transmisión de mensajería.

17ª.- Sistema conforme a cualquiera de las reivindicaciones precedentes, caracterizado por que comprende los registros de aplicación (55, 58, 59) para preservar un registro de las operaciones efectuadas por uno o más componentes del sistema, siendo los datos procesados por los registros de la aplicación la identificación de los usuarios que participan en la operación, la naturaleza de la operación, la identificación de los documentos afectados y una marca del tiempo.

18ª.- Método de gestión de datos en un sistema seguro de red informática comprendiendo, al menos, una infraestructura de portal (2a, 2b) conectada a través de una red de comunicación troncal cerrada (4) a una multitud de sistemas de servidor de registro de datos (3a, 3b, 3c) situados en distintos lugares, cada sistema de servidor de registro de datos comprendiendo, al menos, una base de datos (62) en la que están almacenados los datos protegidos que constituyen documentos, y un mediador técnico de servicio de registro (29) para gestionar el acceso a los documentos que están almacenados en la base de datos, comprendiendo el método la creación y el almacenamiento de dichos documentos en servidores de documentos (40) situados en dichos sistemas de servidor de registro de datos, constituyendo dichos documentos un expediente que es distribuido a través de diferentes sistemas de servidor de registro de datos, comprendiendo la infraestructura de portal, al menos, un mediador de acceso de expediente en la forma de un sistema de servidor con aplicaciones que controlan y gestionan el acceso de los usuarios (6) a los documentos almacenados en los sistemas de servidor de registro de datos, que se caracteriza por que en el momento de una petición de búsqueda de un documento por un usuario autorizado del sistema seguro de red informatizado, la petición de búsqueda es distribuida por el mediador de acceso de expediente (25) a todos los mediadores técnicos del servicio de registro (29) y los derechos de acceso basados en perfiles de derechos de acceso en el nivel de cada mediador técnico de servicio de registro (29) son verificados y caracterizado por que en el momento de la consulta de un documento, el mediador de acceso de expediente (25) se dirige directamente al mediador técnico del servicio de registro (29) afectado después del paso de búsqueda del documento y vuelve a verificar los derechos de acceso al documento relativo al usuario requiriendo la consulta ante de transmitirla al usuario.

19ª.- Método conforme a la reivindicación precedente, caracterizado por que está almacenado un perfil de acceso, por medio de una aplicación de gestión de perfil de acceso (51), definido por un usuario, a los documentos de su expediente en, al menos, uno de los sistemas de servidor de registro de datos (3a, 3b, 3c).

20ª.- Método conforme a la reivindicación precedente, caracterizado por que en cada sistema de servidor de registro de datos, en el que los documentos de un expediente están almacenados, están almacenadas las listas de control de acceso asociadas específicamente a los documentos almacenados y determinando el perfil de acceso solamente para aquellos documentos.

21ª.- Método conforme a cualquiera de las dos reivindicaciones precedentes, caracterizado por que hay almacenada información sobre las identidades y los cargos de los usuarios del sistema seguro de red informática en un directorio del sistema de servidor en un área de alta seguridad de la infraestructura de portal, siendo accedido ese directorio por el mediador de acceso (25) para determinar, entre otros, los derechos de acceso de los usuarios, de acuerdo con su identidad y su cargo.

22ª.- Método conforme a cualquiera de las cuatro reivindicaciones precedentes, caracterizado por que en el momento de la creación y el almacenamiento de un documento, mediante una aplicación de validación, el mediador de acceso de expedientes verifica la conformidad del documento en cuanto a su formato, su sintaxis y sus atributos.

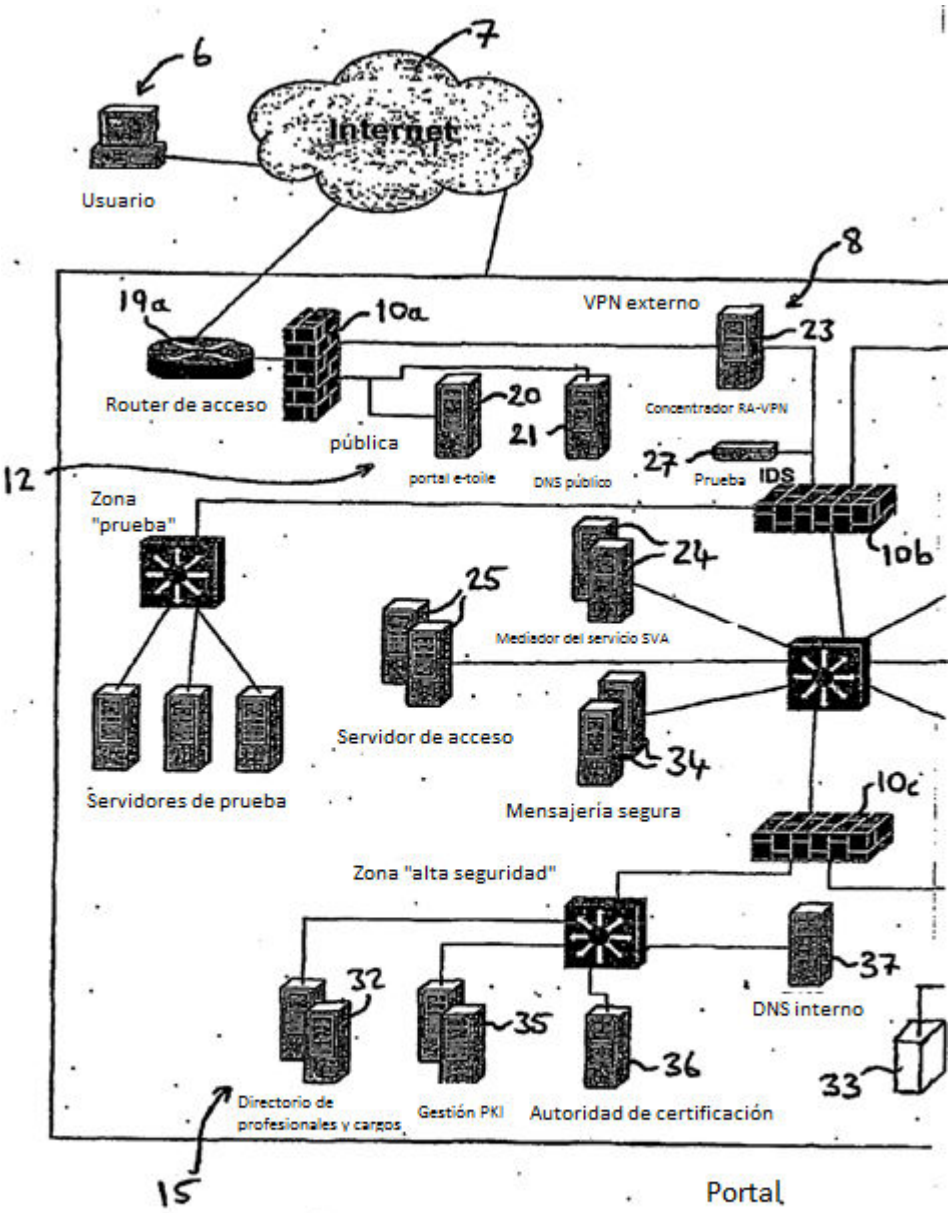


Fig. 1 (continúa en la siguiente página)

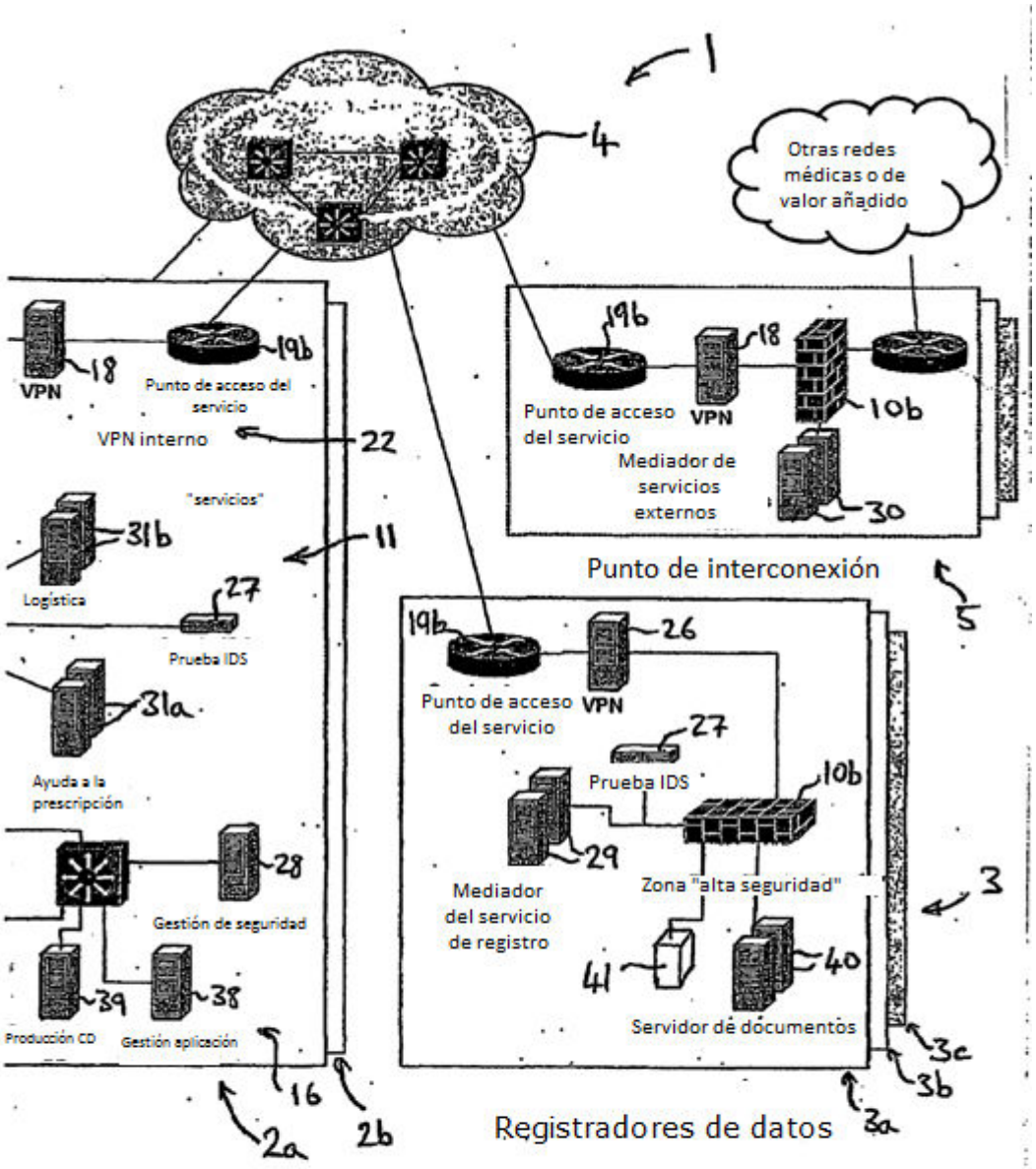


Fig. 1 (continúa en la página anterior)

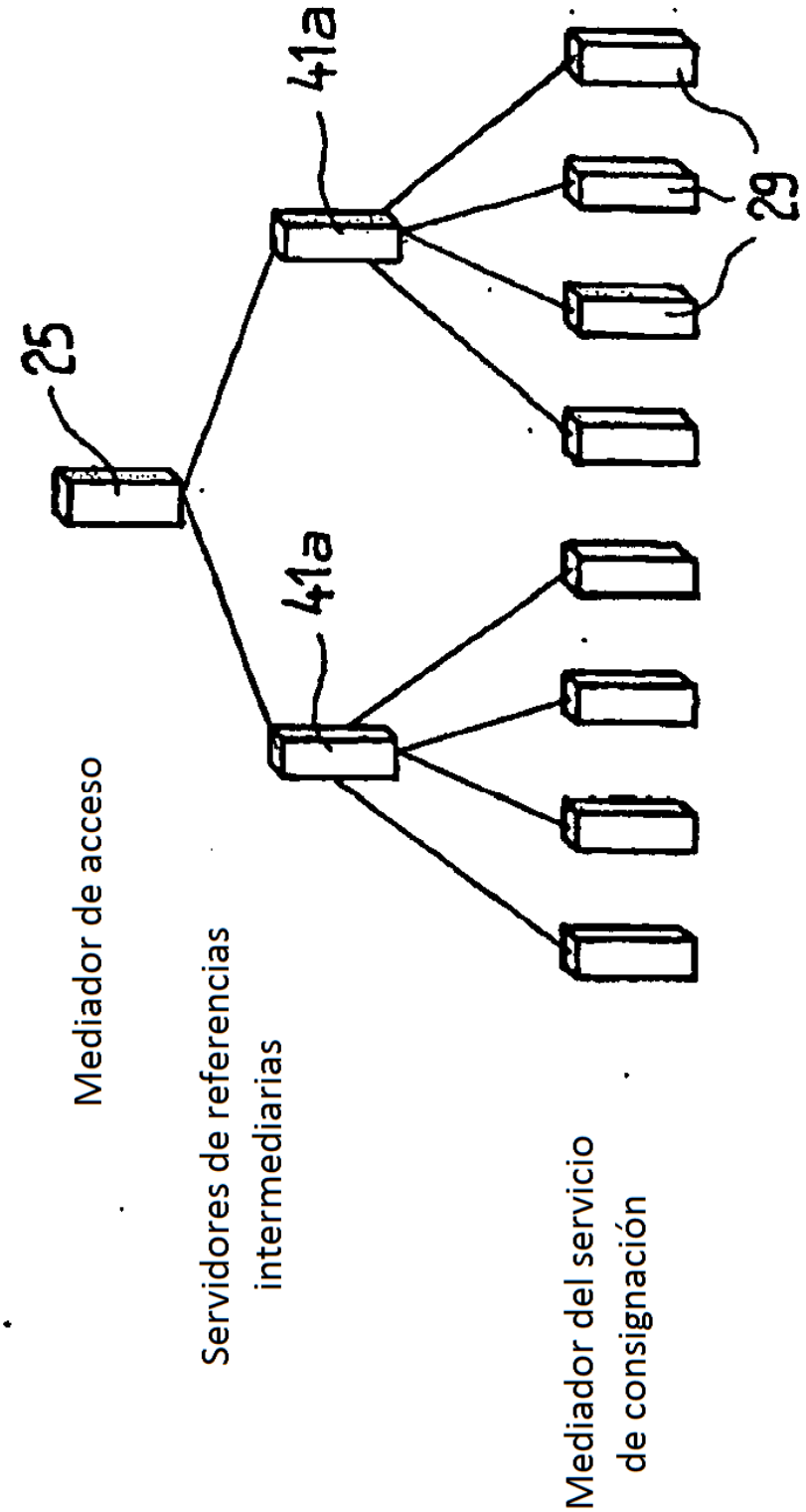

25
41a
41a
29
Mediador de acceso
Servidores de referencias intermediarias
Mediador del servicio de consignación

Fig.1a

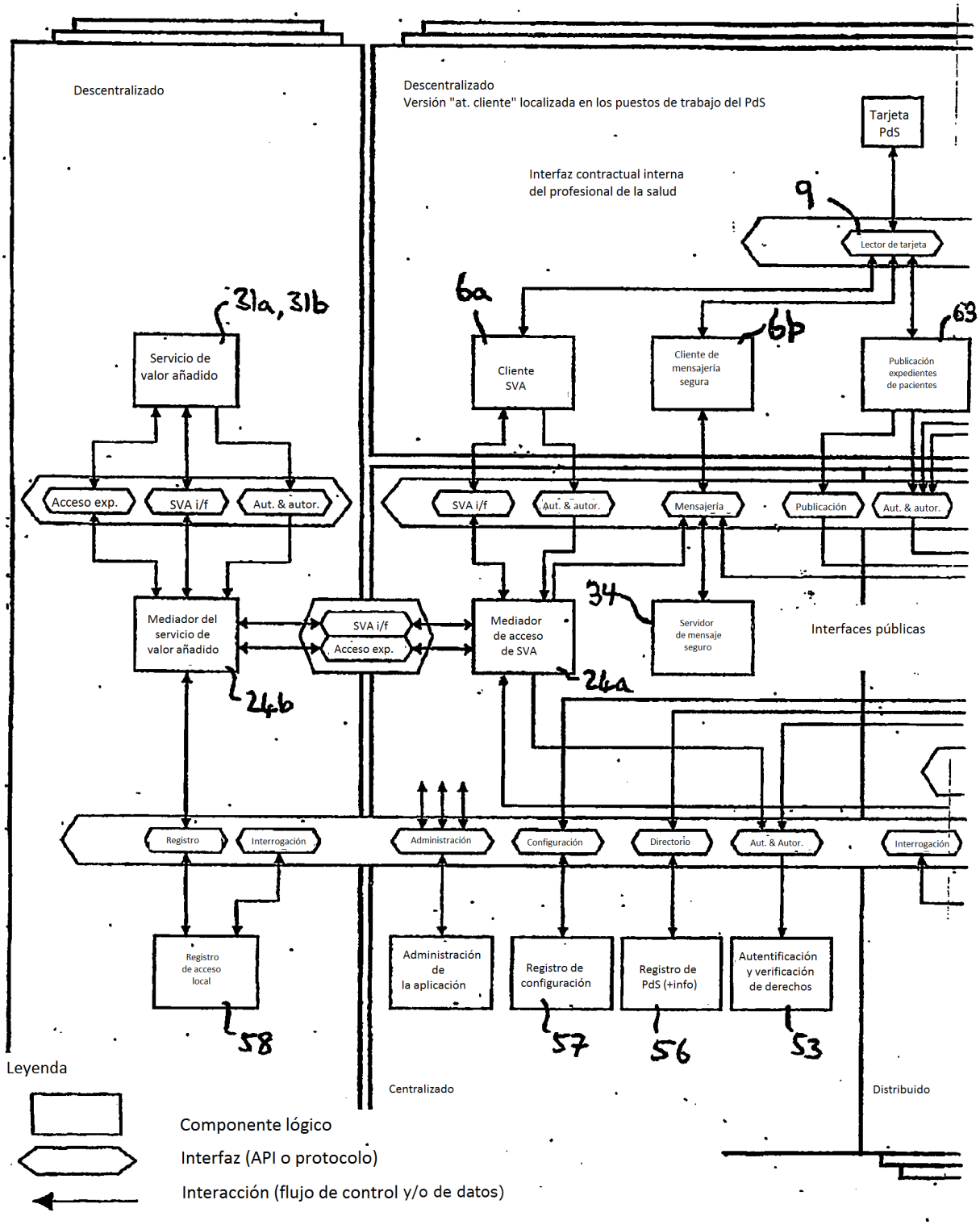


Fig. 2 (continúa en la página siguiente)

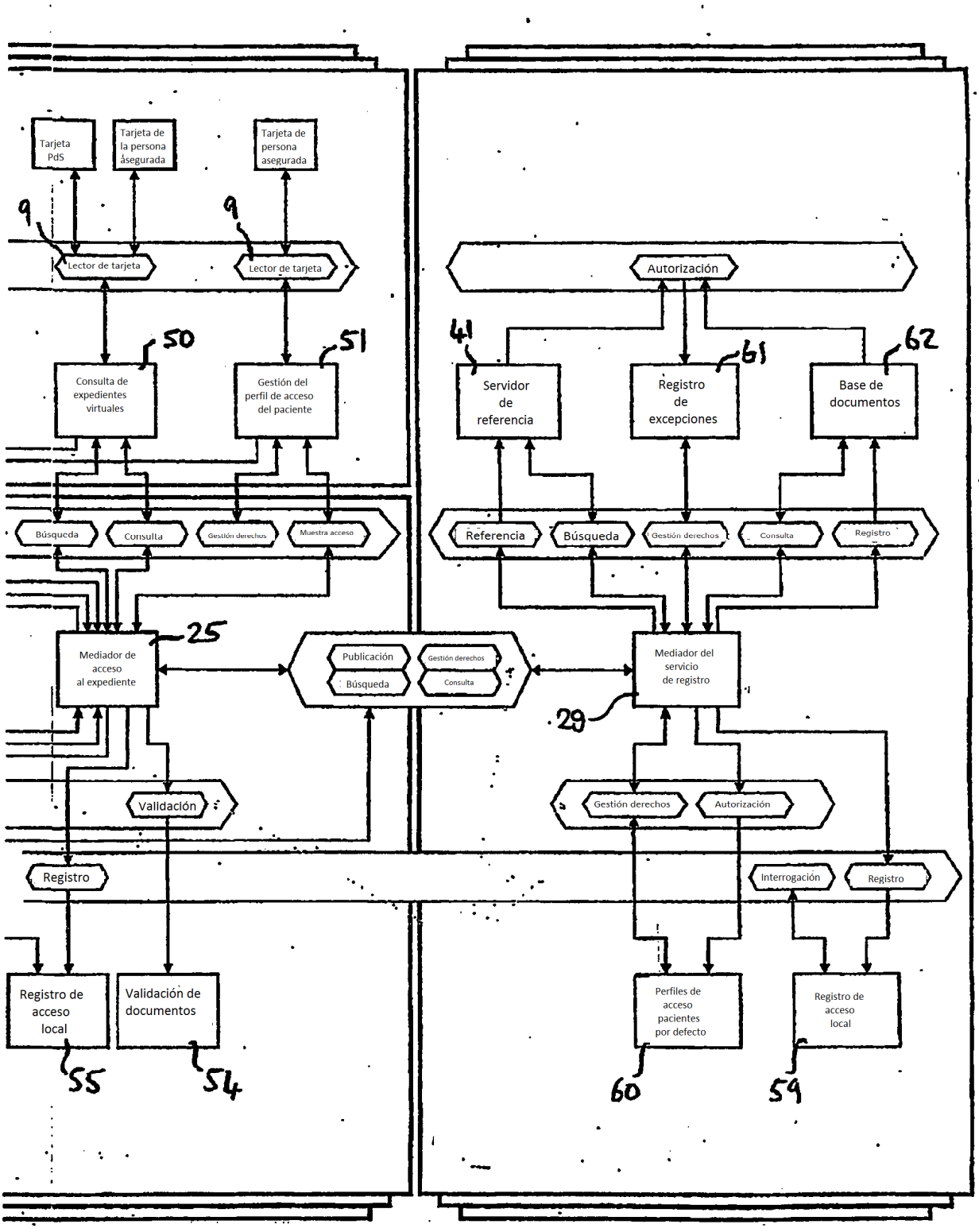


Fig. 2 (continuación de la página anterior)

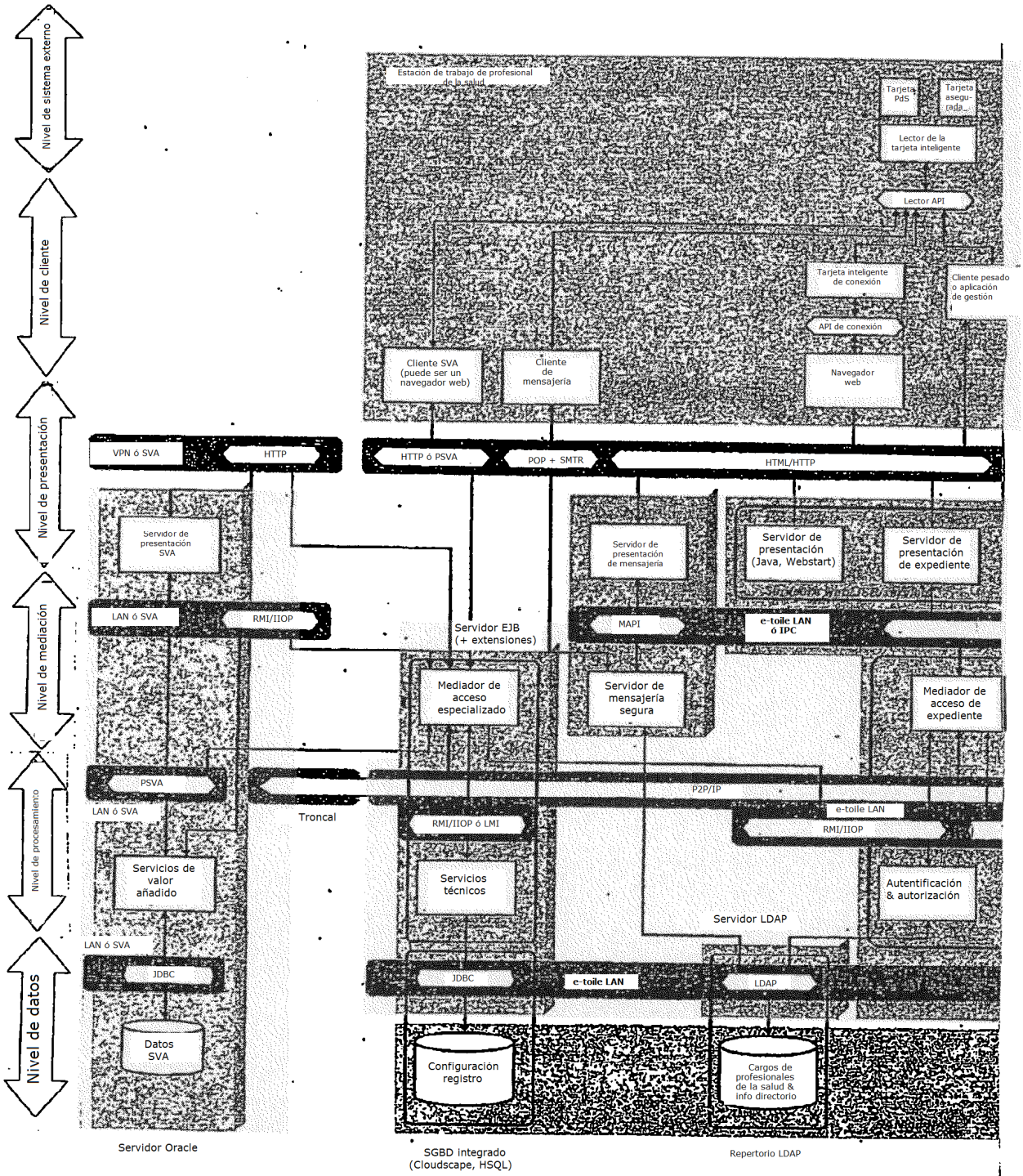


Fig. 3 (Continúa en la página siguiente)

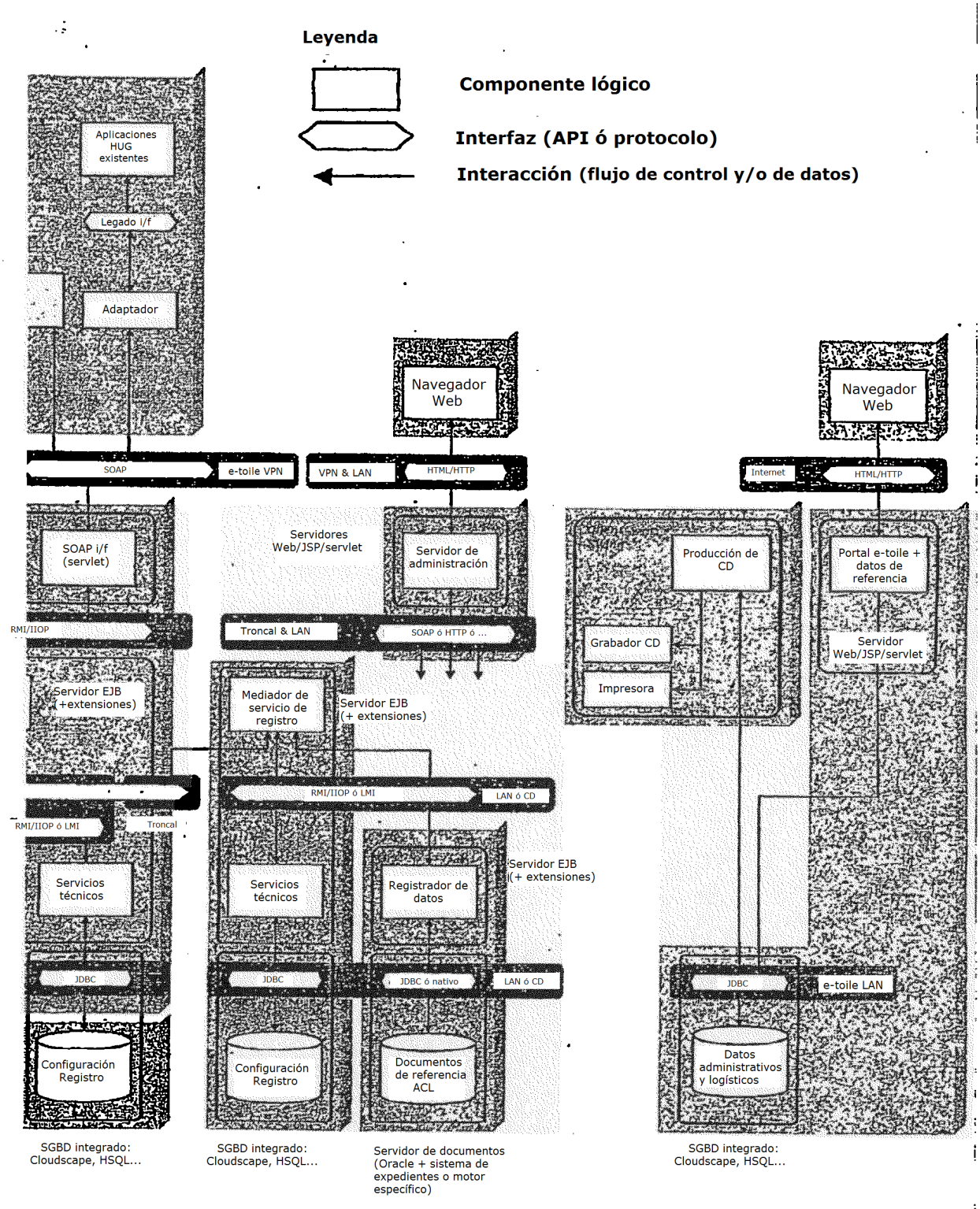
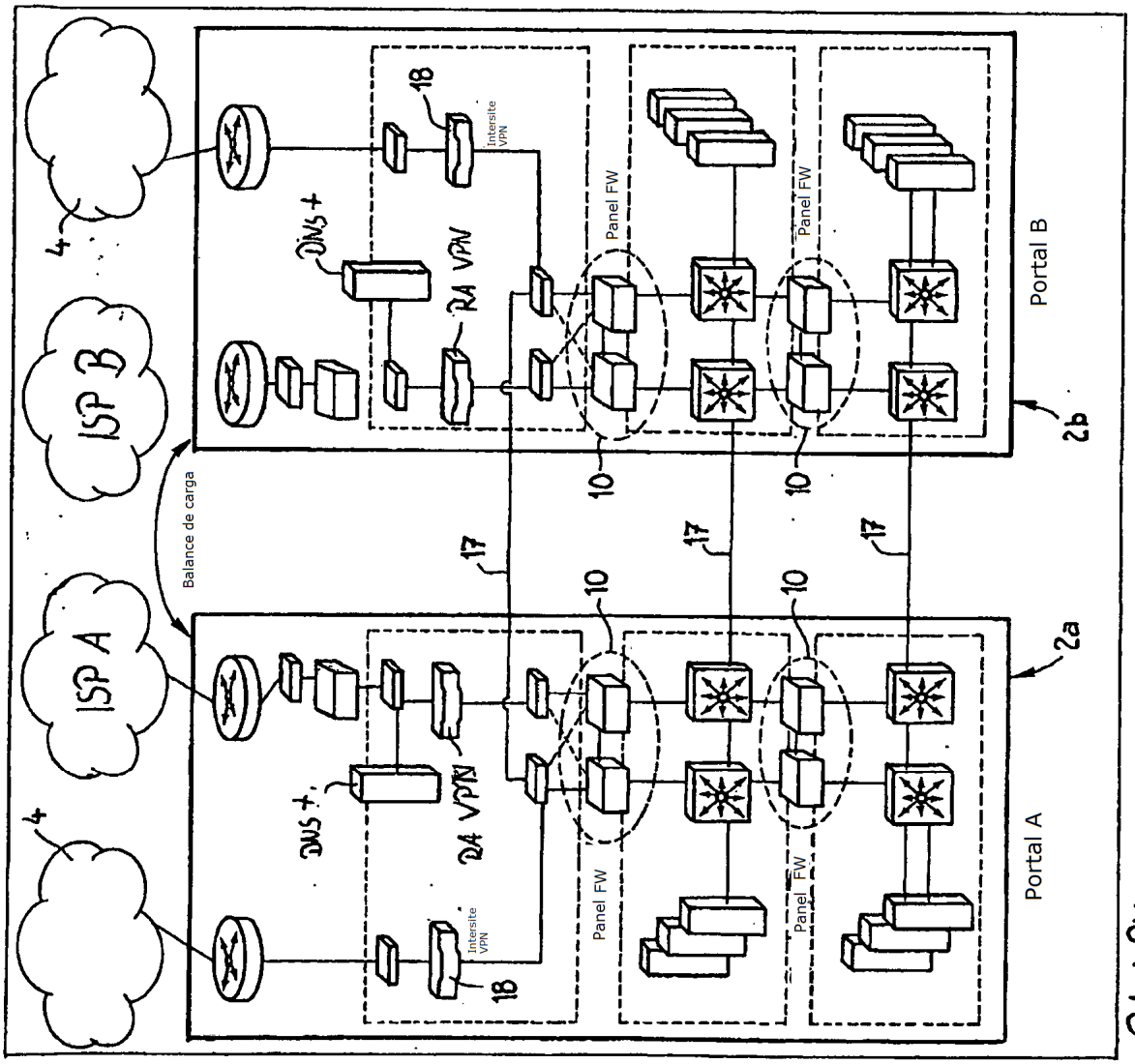


Fig. 3 (continuación de la página anterior)

Fig.4


ISP A
ISP B
Balance de carga
Portal A
Portal B
2a
2b
Panel FW
Intersite VPN
RA VPN
DNS
10
17
18
4
RA VPN: Acceso remoto VPN
ISP : Suministro de Servicio de Internet

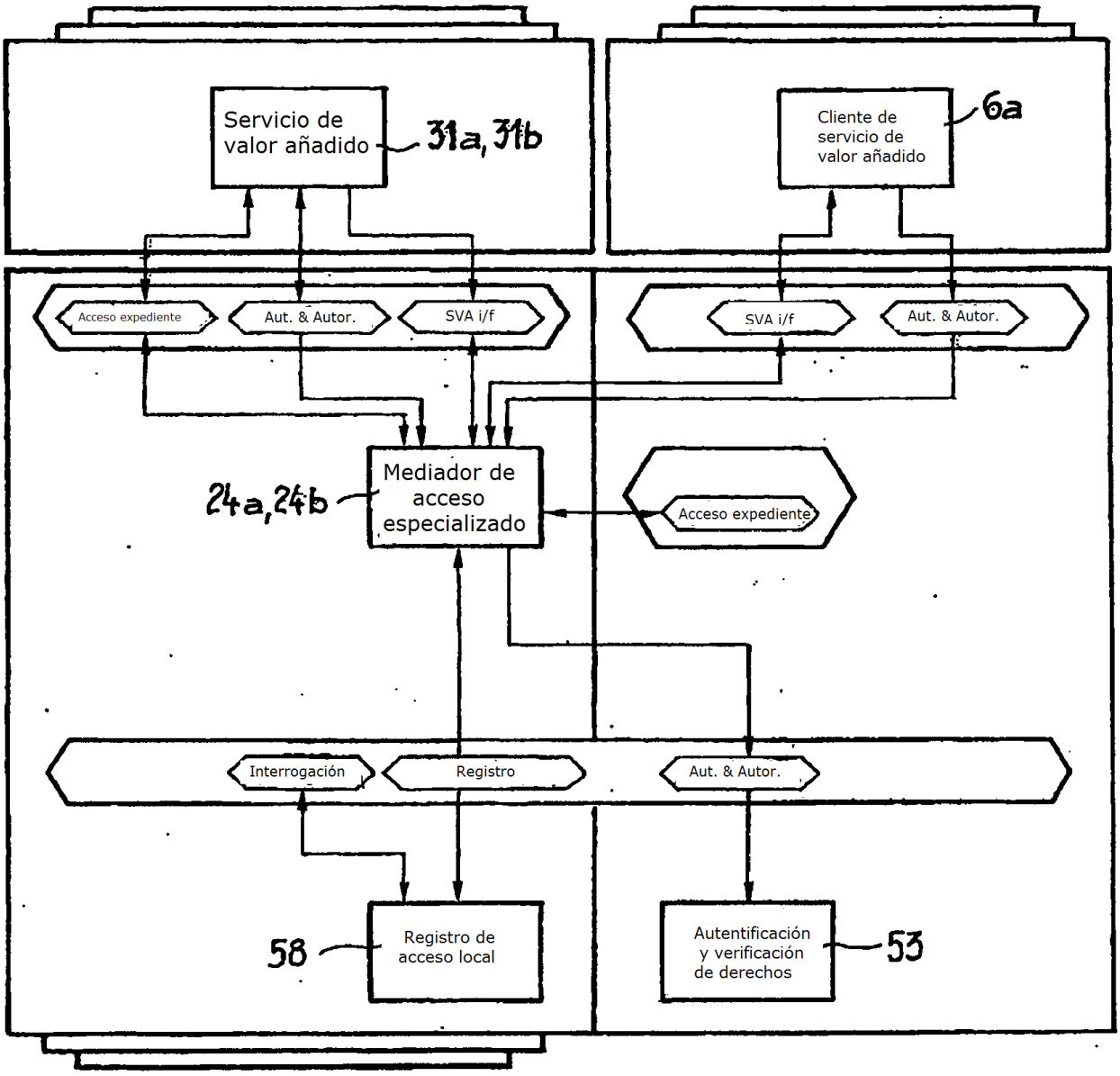

Servicio de valor añadido
31a, 31b
Cliente de servicio de valor añadido
6a
Acceso expediente
Aut. & Autor.
SVA i/f
SVA i/f
Aut. & Autor.
24a, 24b
Mediador de acceso especializado
Acceso expediente
Interrogación
Registro
Aut. & Autor.
58
Registro de acceso local
Autentificación y verificación de derechos
53
Leyenda
Componente lógico
Interfaz (API ó protocolo)
Interacción (flujo de control y/o de datos)

Fig.5

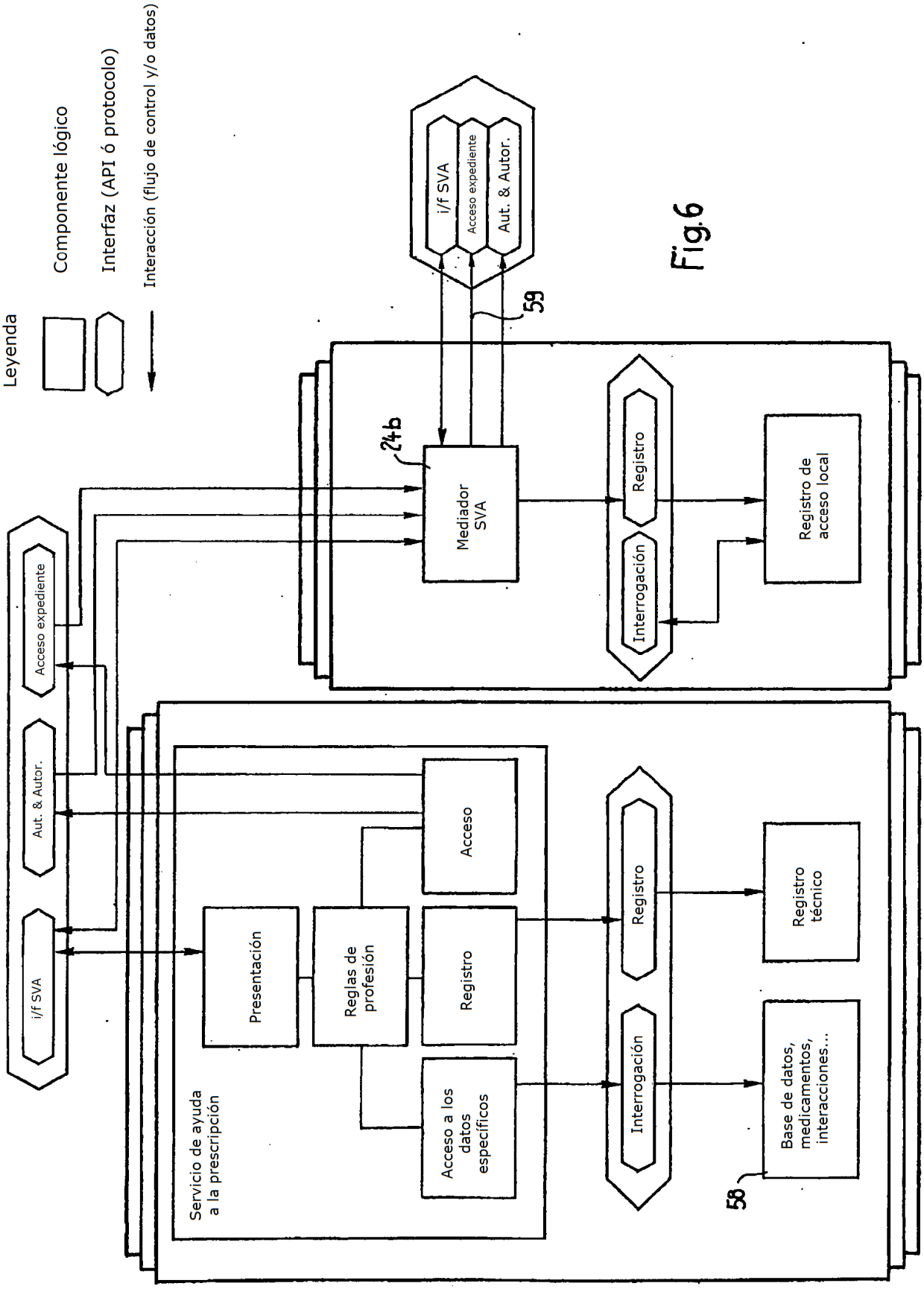

Leyenda
Componente lógico
Interfaz (API ó protocolo)
Interacción (flujo de control y/o datos)
i/f SVA
Acceso expediente
Aut. & Autor.
Mediador SVA
24b
59
Registro
Interrogación
Registro de acceso local
Servicio de ayuda a la prescripción
Presentación
Reglas de profesión
Acceso
Registro
Acceso a los datos específicos
Registro
Interrogación
Registro técnico
Base de datos, medicamentos, interacciones...
58

Fig.6

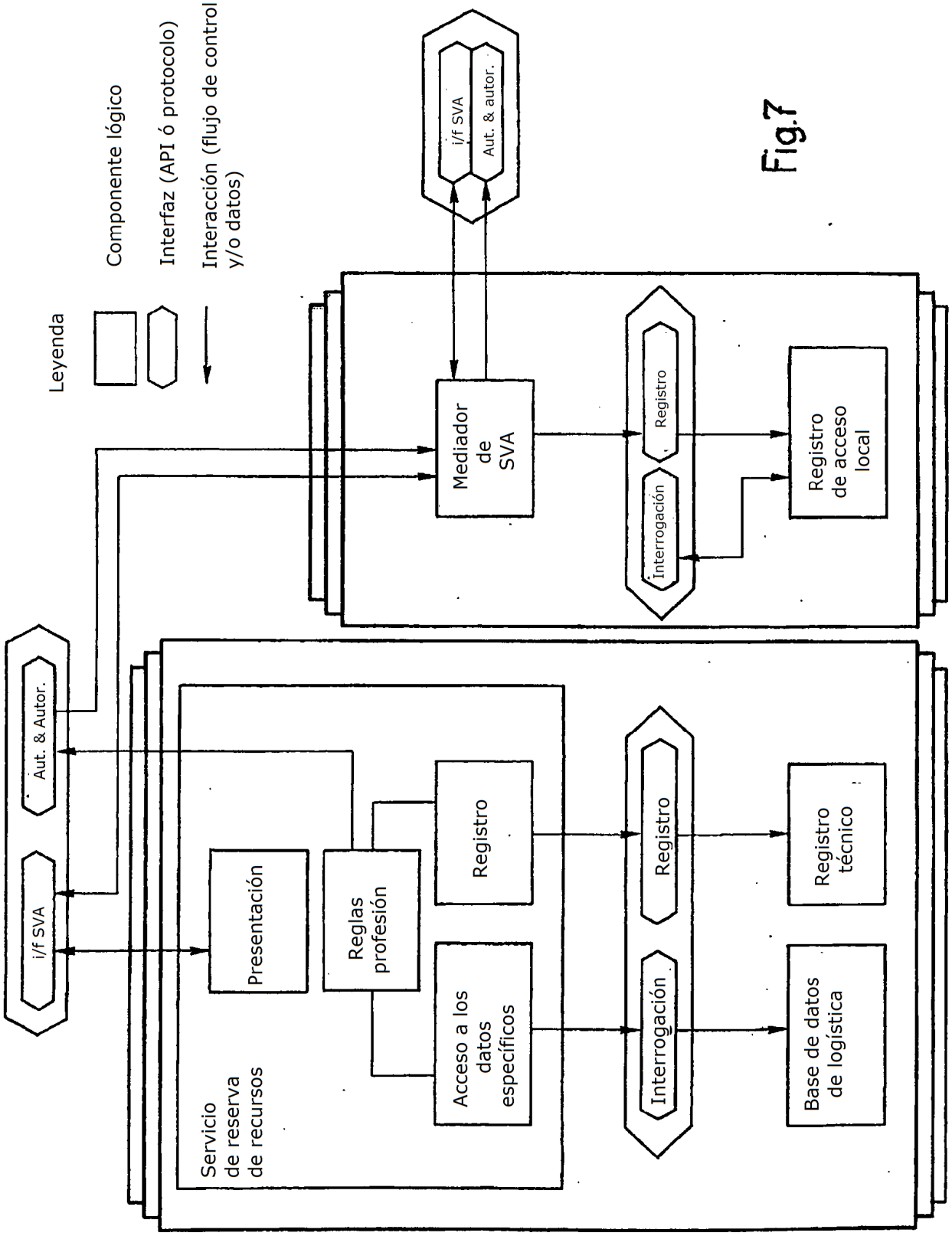

Leyenda
Componente lógico
Interfaz (API ó protocolo)
Interacción (flujo de control y/o datos)
i/f SVA
Aut. & autor.
Mediador de SVA
Registro
Interrogación
Registro de acceso local
i/f SVA
Aut. & Autor.
Servicio de reserva de recursos
Presentación
Reglas profesión
Registro
Acceso a los datos específicos
Registro
Interrogación
Registro técnico
Base de datos de logística

Fig.7

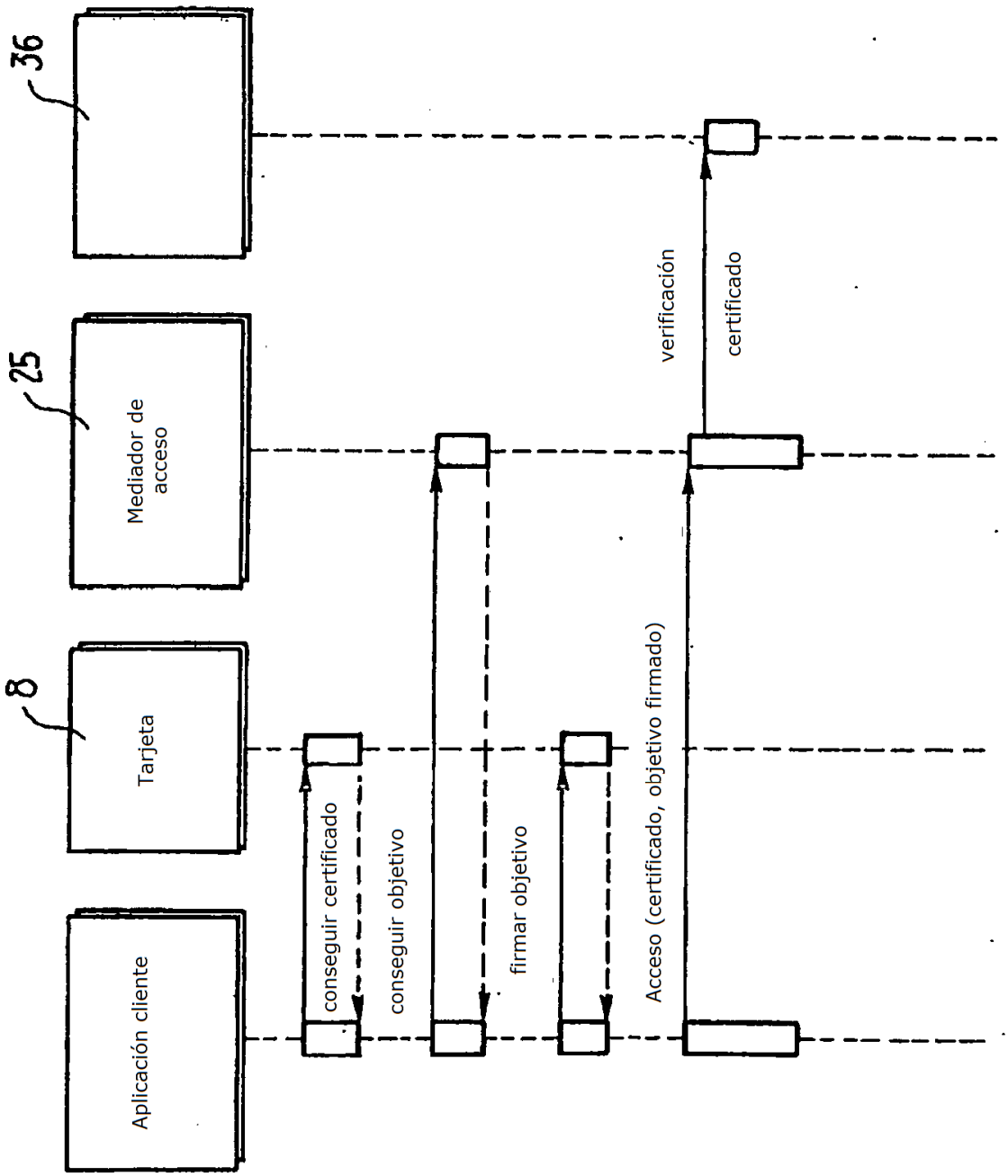

36
25
Mediador de acceso
8
Tarjeta
Aplicación cliente
conseguir certificado
conseguir objetivo
firmar objetivo
Acceso (certificado, objetivo firmado)
verificación
certificado

Fig.8

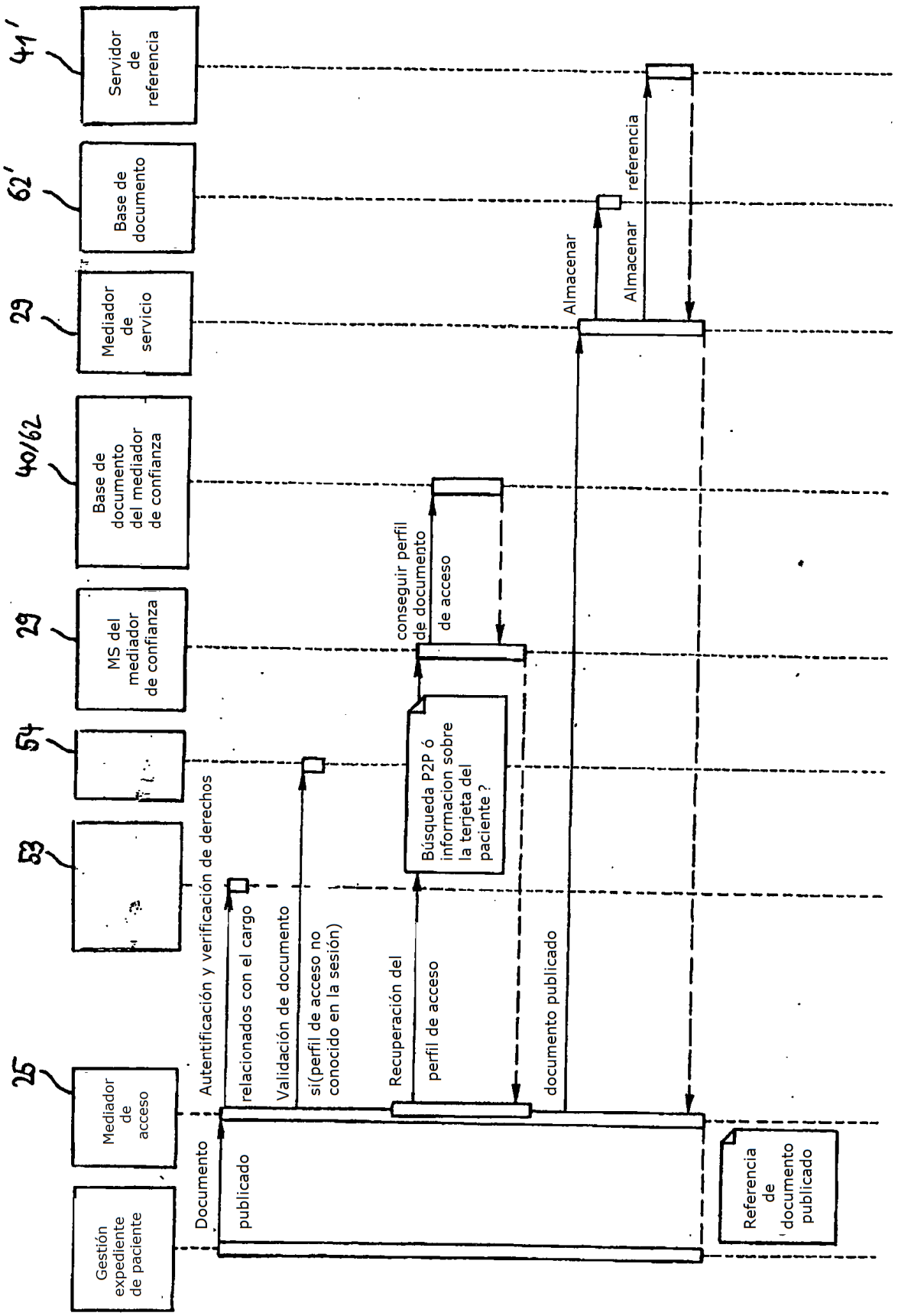

Gestión expediente de paciente
25
Mediador de acceso
53
54
29
MS del mediador de confianza
40/62
Base de documento del mediador de confianza
29
Mediador de servicio
62'
Base de documento
41'
Servidor de referencia
Documento publicado
Autentificación y verificación de derechos relacionados con el cargo
Validación de documento si(perfil de acceso no conocido en la sesión)
Recuperación del perfil de acceso
Búsqueda P2P ó informacion sobre la terjeta del paciente ?
conseguir perfil de documento de acceso
documento publicado
Almacenar
Almacenar referencia
Referencia de documento publicado

Fig.9

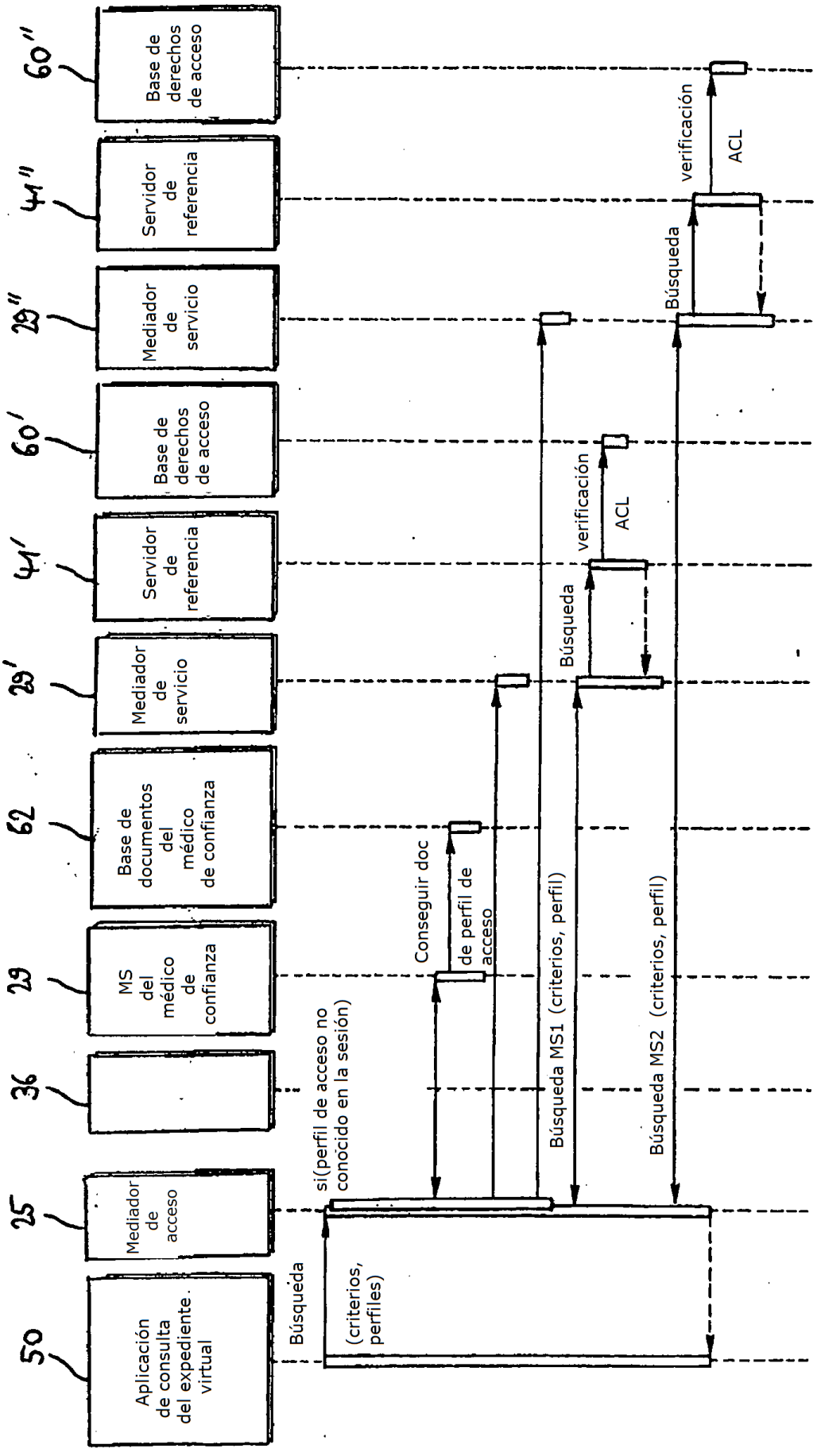

Aplicación de consulta del expediente virtual
50
Mediador de acceso
25
36
MS del médico de confianza
29
Base de documentos del médico de confianza
62
Mediador de servicio
29'
Servidor de referencia
41'
Base de derechos de acceso
60'
Mediador de servicio
29"
Servidor de referencia
41"
Base de derechos de acceso
60"
Búsqueda
(criterios, perfiles)
si(perfil de acceso no conocido en la sesión)
Conseguir doc de perfil de acceso
Búsqueda MS1 (criterios, perfil)
Búsqueda MS2 (criterios, perfil)
Búsqueda
verificación
ACL
Búsqueda
verificación
ACL

Fig.10

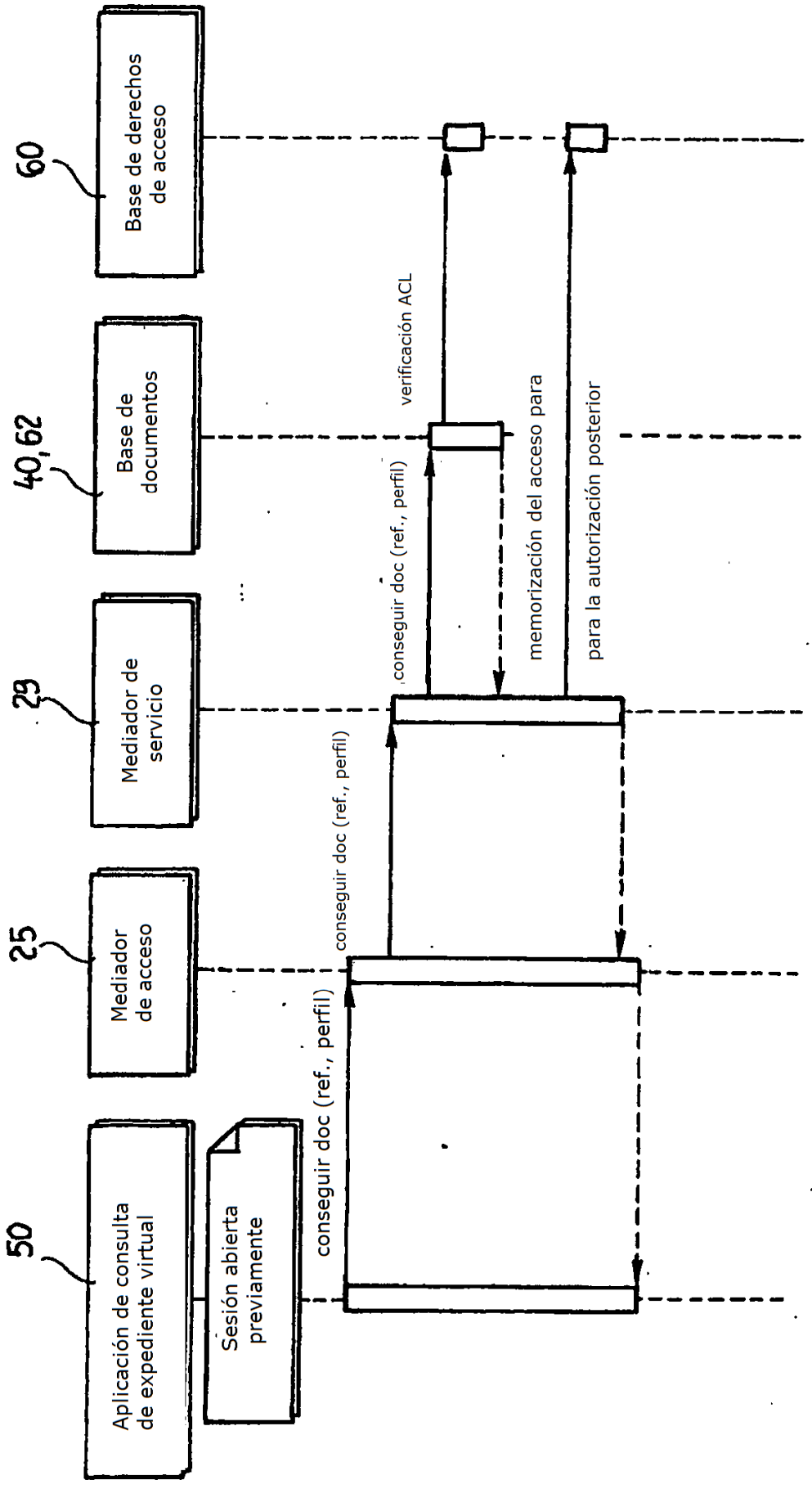

50
Aplicación de consulta de expediente virtual
Sesión abierta previamente
25
Mediador de acceso
29
Mediador de servicio
40, 62
Base de documentos
60
Base de derechos de acceso
conseguir doc (ref., perfil)
conseguir doc (ref., perfil)
conseguir doc (ref., perfil)
verificación ACL
memorización del acceso para
para la autorización posterior

Fig. 11

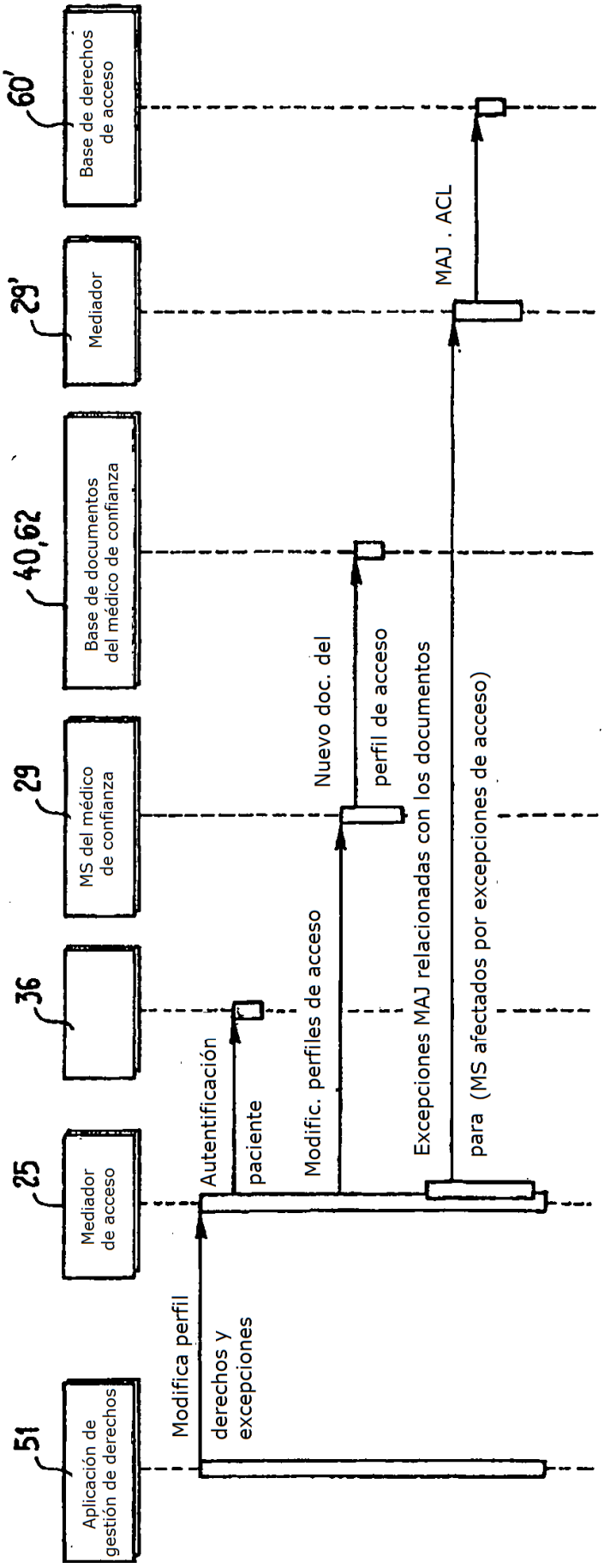

51
Aplicación de gestión de derechos
25
Mediador de acceso
36
29
MS del médico de confianza
40,62
Base de documentos del médico de confianza
29'
Mediador
60'
Base de derechos de acceso
Modifica perfil derechos y excepciones
Autentificación paciente
Modific. perfiles de acceso
Nuevo doc. del perfil de acceso
Excepciones MAJ relacionadas con los documentos para (MS afectados por excepciones de acceso)
MAJ . ACL

Fig.12

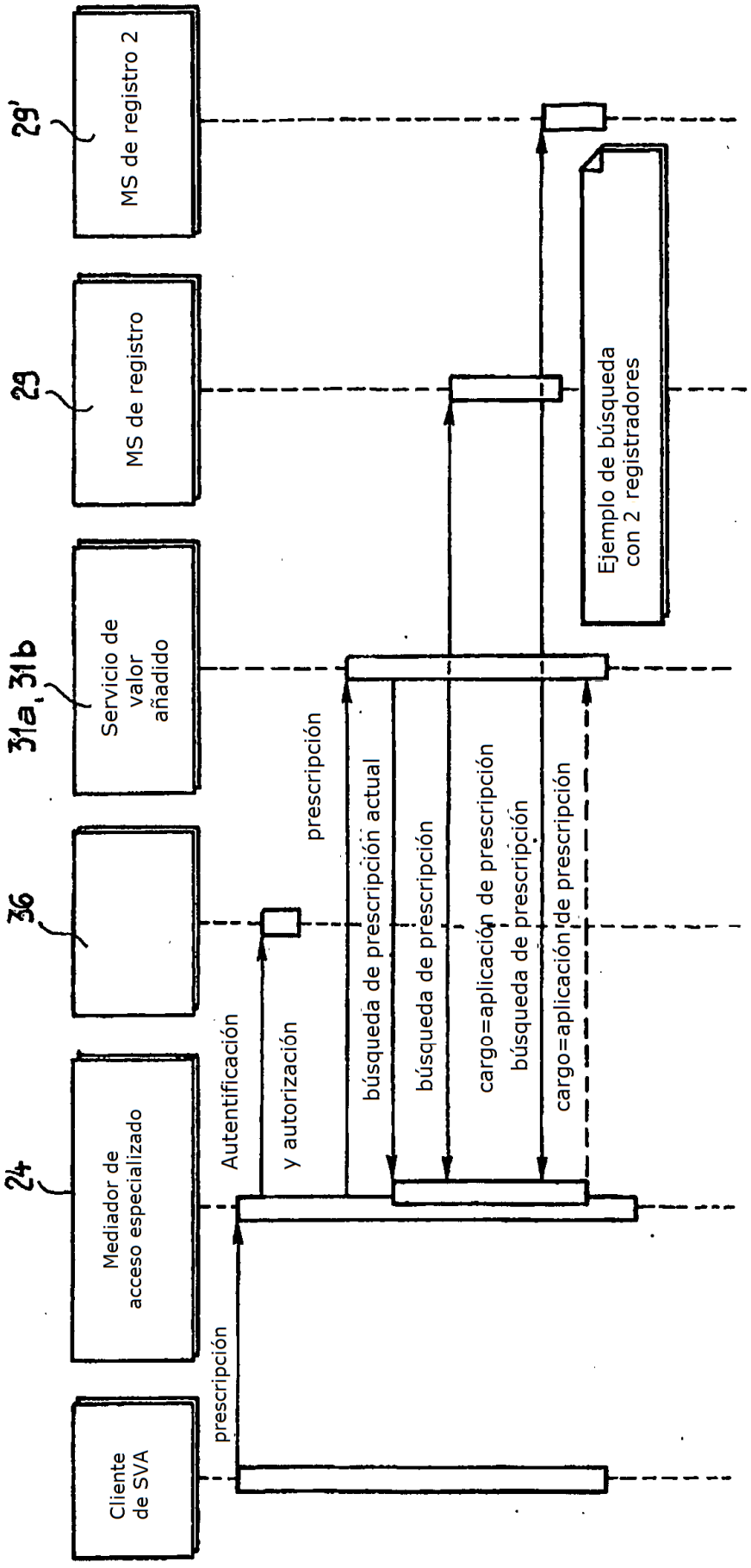

Cliente de SVA
Mediador de acceso especializado
24
36
Servicio de valor añadido
31a, 31b
MS de registro
29
MS de registro 2
29'
prescripción
Autentificación
y autorización
prescripción
búsqueda de prescripción actual
búsqueda de prescripción
cargo=aplicación de prescripción
búsqueda de prescripción
cargo=aplicación de prescripción
Ejemplo de búsqueda con 2 registradores

Fig.13