(19) DANMARK

(10) DK/EP 2618285 T3

(12) Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

(51) Int.Cl.: *G 06 F 21/62 (2013.01)* *G 06 Q 10/10 (2012.01)* *H 04 L 29/06 (2006.01)*

(45) Oversættelsen bekendtgjort den: **2017-03-27**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2017-01-04**

(86) Europæisk ansøgning nr.: **13000661.2**

(86) Europæisk indleveringsdag: **2004-05-18**

(87) Den europæiske ansøgnings publiceringsdag: **2013-07-24**

(30) Prioritet: **2003-05-23 CH 9292003**

(62) Stamansøgningsnr: **04733604.5**

(84) Designerede stater: **AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR**

(73) Patenthaver: **Die Schweizerische Post AG, Wankdorfallee 4, 3030 Bern, Schweiz**

(72) Opfinder: **Gobet. Jean, Avenue de Miremont 8, 1206 Genève, Schweiz**

(74) Fuldmægtig i Danmark: **Larsen & Birkeholm A/S Skandinavisk Patentbureau, Banegårdspladsen 1, 1570 København V, Danmark**

(54) Benævnelse: **Secure computer network system for personal data management**

(56) Fremdragne publikationer:
WO-A-02/05061
DESWARTE Y ET AL: "Intrusion tolerance in distributed computing systems", PROCEEDINGS OF THE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY. OAKLAND, MAY 20 - 22, 1991; [PROCEEDINGS OF THE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY], LOS ALAMITOS, IEEE COMP. SOC. PRESS, US, vol. SYMP. 12, 20 mai 1991 (1991-05-20), pages 110-121, XP010024218, DOI: 10.1109/RISP.1991.130780 ISBN: 978-0-8186-2168-0

The present invention concerns a secure computer network system for the management of data, notably personal data. The invention concerns in particular a secure computer network system for the management of medical files in a health system of a region or a country.

There exist numerous projects aimed at creating, developing and maintaining computerized health networks with the aim, *inter alia*, of improving services to patients and reducing the costs of the health systems. The conversion to electronic form of data on patients in current health systems has the general objective of improving one or more of the following processes: the administrative flow, notably concerning the reimbursement of medical services; the sharing and the filling out of the medical file for the treating doctors, hospitals and emergencies; and the prescription of drugs, notably for its appropriateness to the diagnosis and interactions to limit prescription errors, as well as its circulation to the pharmacist or to the insurer for reimbursement.

In the systems in operation or in the form of pilot projects in different countries or regions, there is proposed either the storage of certain data on the patient in smart cards or the storage of data on the patient on a centralized server, or a combination of the two, the data on the patient ranging from simple administrative data (for example on insurance cover and social security benefits, as well as the identification of the person) to the medical information of the patient. Health systems based on a smart card or centralization of computerized data on a patient are summarized hereinafter:

SESAM-Vitale card, France

The inhabitants of France are supplied with a smart card containing information on their social security benefits, used for communication between patients, doctors and insurers.

Social health network, France	The French social health network makes possible improved communication between patients and insurers and offers secure messaging between health professionals. This network supports the smart card.
German project	The German network proposes a computerized medical file and tools for secure communication and for supporting the day to day work of doctors. Each patient is provided with a health card.
Picnic, Denmark	A secure network onto which services such as secure messaging can be grafted is being developed as an open source facility and has the object of making the European telecommunications industries and enterprises more uniform.
Rimouski, Quebec	An experimental health card was distributed to the inhabitants of the Rimouski region. It contained all the patient's medical information (vaccinations, allergies, drugs).
Laval, Quebec	The same experimental health card as that for Rimouski was distributed to the inhabitants of Laval, but the architecture of the data network was modified, with a centralized patient file.
Hygeianet, Crete	The Cretan health network proposes improved communication of the patient's computerized medical file between professionals and remote management of medical resources.

Slovenian project	Each inhabitant of Slovenia is issued with a health card carrying information on their social security benefits, prescribed drugs and emergency information (vaccinations, allergies, etc.).
Danish project	The object of this project is to enquire into and to study the various projects existing in the country, or even in other Nordic countries, and to derive federating guidelines therefrom.
Banque Carrefour	This Belgian project proposes a government portal to all social services, including health services, a unique and national identification of the inhabitants of Belgium and secure transfer of their data between services to avoid re-entering data.

One of the main disadvantages of systems based on using a smart card to store data, notably data in the medical file of a patient, is that the data may be lost. On the other hand, in an emergency access to the file will depend on the presence of the smart card. Another disadvantage of storing the data of a medical file on a smart card is that, even with the agreement of the patient, the health professionals (care providers, pharmacists, doctors, nurses, hospitals and other medical service providers) do not have access to the data at all times.

These disadvantages are eliminated by the storage of the data concerning a patient on a server of a computer network accessible by the various service providers. A major disadvantage of such a system is encountered at the level of security and the confidentiality of sensitive data. Protection of personal data, such as the documents of a medical file of a patient, is important not only in relation to unauthorized third parties but also in relation to authorized users who might abuse their right of access

to this data, or who might be negligent, and through such negligence enable third parties to obtain the data.

Although secure networks and the exchange of encrypted information makes it possible to alleviate the risks of hacking a computerized health network and illicit access to the personal data stored in a server or circulating on the network between users, abuse of or negligence in relation to this data by an authorized user remains a problem.

In view of the disadvantages cited above, one of the objects of the invention is to provide a secure computer network system for the management of data that makes it possible to ensure a high level of protection of the data. In particular, the invention aims to provide a secure computer network system for the management of medical data in a regional, national or international health system.

Another object of the invention is to provide a secure computer network for the management of personal medical data that makes it possible on the one hand to improve the quality of the information accessible to authorized users and on the other hand to reduce the administrative costs linked to processing the data at the same time as offering a high level of protection of the data from unauthorized third parties or against abuse or negligence on the part of authorized persons.

It is advantageous to provide a secure computer network system for the management of personal medical data in a health system that enables rapid access to the information in a medical file.

It is advantageous to provide a secure computer network system for the management of personal medical data in which access to the data constituting a medical file can be defined in a variable manner in relation to the accessible documents and over time for each authorized user.

It is advantageous to provide a secure computer network system for the management of medical data that is flexible so as to ensure its longevity and the possibility of integrating into other existing or future computer networks.

Objects of the invention are realized by a secure computer network system in accordance with Claim 1 for managing confidential data and by a method in accordance with Claim 18 of managing data in a secure computer network system.

WO 02/05061 A1 describes the features of the preamble of claims 1 and 18.

In the present invention, a secure computer network for the management of protected data comprises at least one gateway infrastructure connected via a closed backbone communication network to a plurality of data logging server systems, each data logging server system comprising at least one database in which protected data constituting medical documents on patients is stored, and a logging service technical mediator for managing access to the documents stored in the database, different documents forming a medical file relating to a person possibly being distributed across a plurality of data logging server systems located on different sites, the gateway infrastructure comprising at least one file access mediator in the form of a server system with applications that monitor and manage access of users to the documents stored in the data logging server systems.

The dependent claims describe other advantageous aspects of the invention.

The use of a plurality of distributed data logging servers to store data from a medical file accessible by means of a secure closed network (backbone network) makes it possible to ensure a high level of protection of the data because even in the event of illicit (forced) entry into the secure network system the recovery of data constituting a medical file necessitates an attack on a plurality of protected servers and is therefore extremely difficult. At least two levels of access rights, i.e. the authorization to access the backbone network and the personal data of a patient by means of a smart card and

access to different data of a specific medical file, make it possible to reduce greatly the risk of abuse of the data and to define access to the various elements of the file as a function of the role and the identity of the authorized user. The logging of access to the data and other operations on the servers makes it possible to identify users and therefore to prevent abuse by users. Access to the protected data is nevertheless possible in an emergency by certain health professionals such as hospitals and treating doctors, the security being provided on the one hand by the access log and on the other hand by the necessity of using strong authorization and authentication means with a smart card.

Other objects and advantageous aspects of the invention will emerge from the claims, from the following description, and from the appended drawings, in which:

Figure 1 is a representation of the physical architecture of a computer network system in accordance with the invention for the management of data;

Figure 1a is a representation of a part of the physical architecture in accordance with a variant;

Figure 2 is a representation of the logic architecture of a computer network system in accordance with the invention for the management of data;

Figure 3 is a representation of the logic architecture of a computer network system in accordance with the invention for the management of data based on a J2EE (Java 2 Enterprise Edition) platform;

Figure 4 is a simplified representation of the physical architecture of two gateways of a computer network system in accordance with the invention;

Figure 5 is a representation of the logic architecture of a part of the computer network system in accordance with the invention relating to access to value-added services;

Figure 6 is a graphical representation of the logic architecture of a part of the computer network system in accordance with the invention relating to a value-added service, in the example shown a drug prescription aid service;

Figure 7 is a representation of the logic architecture of a part of the computer network system in accordance with the invention relating to a value-added service, in the example shown a logistics database;

Figure 8 is a diagram showing the principal actions of opening a session in the computer network system;

Figure 9 is a diagram illustrating the sequences of actions in the creation (publication) of a document relating to a patient to be stored in the computer network system in accordance with the invention;

Figure 10 is a diagram showing the sequences of actions in searching for documents in a computer network system in accordance with the invention;

Figure 11 is a diagram showing the sequence of actions for consulting a document stored in the computer network system;

Figure 12 is a diagram showing the sequence of actions for modifying access rights to the computer network system or to a file stored in the system;

Figure 13 is a diagram showing the sequence of actions for the use of a value-added service, in this instance for the use of drug prescription aid tools.

Referring to Figures 1 and 2, a computer network system 1 (hereinafter: computerized health system) for the management of personal (confidential) medical data comprises at least one gateway infrastructure 2a, 2b, a plurality of data logging server systems 3a, 3b, 3c and a closed backbone communication network 4 connecting the gateway

infrastructures to the data logging server systems. The data logging server systems and the gateway infrastructures are located on different sites. The decentralization of the data, both physically (data distributed across different databases) and geographically (databases located on different sites), offers a high level of protection of the data. The computerized health system may further comprise one or more interconnection point server systems 5 connected on the one hand to the backbone communication network and on the other hand to external computer networks, for example computer networks of other regional or national computerized health systems. Users 6 access the gateway infrastructure 2a, 2b of the computerized health system via the Internet 7 using a secure connection, for example a VPN (virtual private network) type encrypted connection. The users may be health professionals (doctors, nurses, pharmacists) or patients.

Each user is provided with a smart card 8 and a personal code (password) for their authentication and authorization to access the computerized health system. The station from which the user accesses the computerized health system must therefore be provided with a smart card reader 9. This reader may take various forms, but is preferably compatible with the personal computer/smart card (PC/SC) standard or the RSA standard in order to ensure interworking with all the components of the authentication system (smart card, smart card reader, interface and application). The reader may be provided with a double slot in order to allow the insertion of two cards, for example the card of a health professional and the card of the patient, when consulting the medical file of the patient. This makes it possible to reassure the patient as to the protection of their personal data, notably at the time of their first consultation with the health professional.

The smart card 8 constitutes an important element in the authentication of the user, whether that be the health professional or the patient. The data stored in a memory of the microprocessor of the card includes a unique identifier of the card holder, an authentication certificate, at least one private electronic key, and administrative data, such as name, forename, date of birth, insurance or social security number, etc. The

card does not contain any medical data, however. When the card is connected to the smart card reader, it can be unlocked using the user's personal code. The user is authenticated on the computerized health system by the transmission of the authentication certificate. The private key stored in the microprocessor of the smart card enables encryption and signing of data exchanged between the user and the computerized health system. For security reasons, a plurality of private keys may be stored in the smart card, namely a private key for each of the authentication, signature, data and encryption operations.

The gateway infrastructure comprises an external VPN area 8 connected to the Internet network 7 via an access router 19a and a firewall 10a, a service area 11 connected to the external area 8 via a firewall 10b, a test area 13 connected to the external area 8 via a firewall 10b, an internal VPN area 22 connected to the service area 11 via a firewall 10b, a high-security area 15 and a management area 16 connected to the service area 11 via a firewall 10c.

The gateway infrastructure may further comprise a public area 12 connected to the Internet 7 via an access router 19a and a firewall 10a. The service area 11 is connected via a firewall 10b and an internal access router 19b to the backbone communication network 4 connecting the gateway infrastructure 2a, 2b to the data logging server systems 3 and to the interconnection point server systems 5.

The public area 9 is independent of the internal part of the secure network system used for managing the patient files. It contains a web server 20 and a public domain name server (DNS) 21.

The integration tests of the various components of the network are effected in the test area 13 before integrating those components into the network. It is also here that updates are launched to the network.

In the external VPN area 8, all the network connections from user stations are established. It is here that the secure tunnel between the user station and the gateway infrastructure terminates. It is this tunnel that enables secure and encrypted access between the user station and the computerized health system. It is also here that the first system access controls and the first intrusion detection are effected.

All access to the external components of the backbone network 4 is effected from the internal VPN area 22, such as access to the data logging server systems 3 and to the interconnection point server systems 5 for the internetwork connection. It is here that new secure communication tunnels are established between the access mediators 25 and the external components of the backbone network 4.

All so-called "public" services are situated in the service area 11. This area is accessible by the user stations 6 to enable them to access the various services offered by the computerized health system.

Services linked to network security are situated in the high-security area 15. This area is accessible only by the servers that host the applications of the computerized health system and by administration personnel.

All services linked to the management of the infrastructure of the computerized health system are situated in the management area 16. This area is accessible only by administration personnel responsible for infrastructure management operations.

Routers 19a, 19b are used to connect the network to other networks where the various participants are situated. These routers are placed at the periphery of the backbone network 4, the gateway infrastructure 2a, 2b, the interconnection point server systems 5 and the data logging server systems 3. Their parameters are set to offer a first level of protection of the elements of the secure network that they connect. The routers deployed within the computerized health system support packet filtering, event logging and network intrusion detection functions.

Firewalls are machines that make it possible to protect all or part of a network by analyzing the content of packets, or even of sessions. These machines are placed inside the network, just behind the router 19a, and are an obligatory point of passage for entry into the part of the network that they protect.

The firewalls 10a, 10b, 10c deployed in the computerized health system support packet filtering, packet inspection, event logging, antivirus and active defence functions.

Three types of firewall are used:

- Peripheral firewalls 10a: these machines are used in all the gateways. They are situated between the periphery router 19a and the VPN concentrator 23 and make it possible to protect the network of the health system from external attacks. At the time of a "normal" access to the network of the health system, these machines are not able to inspect the content of packets because they are encrypted in a secure tunnel (see below). The parameters of these firewalls are set to effect control at the packet level (addresses and source and destination ports). The periphery firewalls are accessed by all the user stations 6 of the secure network system as well as for all "public" access to the servers 20, 21 of the public area 12.
- Internal firewalls 10b: these machines are used in all parts of the secure network system connected to the backbone network 4. They are situated in the parts of the system that communicate with the backbone network 4 and make it possible to inspect packets outside the secure tunnels in order to protect the public part of the system accessible during sessions by the care providers or the patients. The internal firewalls of the interconnection server systems 5 are accessed by access technical mediators 25 and service mediators 24. They do not necessitate supplementary functions other than those referred to above. The internal firewalls of the gateway infrastructures 2a, 2b are accessed by all the user stations. Since the service, high-security and management areas use private Internet Protocol

(IP) addresses, these firewalls effect IP network address translation (NAT) in addition to the functions listed above.

- Administrative firewalls 10c: these machines are used in all the gateway infrastructures 2a, 2b. They are situated beyond the service area 11 and make it possible to protect the high-security and management areas 15, 16. The administrative firewalls 10c are accessed by access mediators 25, the VPN concentrators 23 and the personnel responsible for the operation of the infrastructure of the computerized health system and the management of the public key infrastructure (PKI). All the functions referred to above are activated on these machines, the parameters of which are frequently monitored in order to ensure a very high level of security in the areas that they protect.

In order to ensure that sessions are secure, secure (VPN) tunnels are established on all the connections of the network that are not safe. These VPN tunnels will be established in the following cases:

- access to the computerized health system by a user 6;
- access to a data logging server system 3 from the backbone network 4;
- access to an interconnection point server system from the backbone network 4.

Two types of VPN are present in the computerized health system:

- User VPN: these VPN use the secure socket layer (SSL) technology and are established between a user station 6 and the gateway infrastructure 2a, 2b on access to the computerized health system. The SSL protocol is used to establish a session with one of the SSL concentrators 23 of the gateway infrastructure. Authentication by the SSL VPN concentrator 23 uses the authentication certificate recovered from the smart card 8 of the user.
- Network interconnection VPN 26: these VPN use the IPSec or SSL technology and are established between the internal VPN servers of the gateway infrastructures 2a, 2b and the VPN server 26 of the data logging server system 3

or the network interconnection server system 5. These secure tunnels between two sites are permanent and do not necessitate authentication on the part of the users or the access mediators because communication is effected between trusted elements via the backbone network 4. Since only the backbone network 4 that transports the data is judged "unsafe", only this channel will be encrypted. The establishing of these VPN is authenticated by an authentication certificate delivered for each data logging server system and each gateway infrastructure.

Although numerous protection mechanisms are deployed within the infrastructure of the secure network system, an intrusion detection system (IDS) is installed in the gateway infrastructure in order to enable rapid response in the event of intrusion. Another important function of the IDS is to make it possible to reconstitute and to track events by analyzing the logs and other data collected.

These IDS provide detection, logging, alert, reaction and synthesis services in relation to any attempted attack or intrusion within the secure network system. They can interface with other IDS and use a language making it possible to define customized rules. The IDS include "network" (NIDS) and "hardware" (HIDS) type functions.

The architecture of the intrusion detection system is distributed and redundant and comprises the following elements:

- A security management server system 28 containing software that recovers all the data sent by the IDS probes 27 and centralizes that data to analyze it and, where appropriate, reacts in order to alert the operators and/or to block these intrusion attempts. This software is present in the management area 16 of each gateway infrastructure 2a, 2b in order to offer an adequate level of redundancy. All the security management server systems communicate with one another in order to exchange information that is pertinent to and necessary for the correct functioning of everything.

- IDS probes 27, which are specialized "sniffers" that analyze all packets, protocols and sessions that transit via the equipment that they monitor. The probes are present in all the critical equipments of the secure network system, in particular in the external router 19 of the gateway infrastructure and in the internal and external firewalls. The probes 27 communicate with the nearest security management server system 28 and feed back all the information necessary to this server system to fulfil its mission properly.

The service area 11 of the gateway interface 2a, 2b includes a server system acting as an access technical mediator (hereinafter: "access mediator") to the protected data, notably to the medical files, the access mediator including for example an access server 25. The access mediator materializes the point of entry into the computerized health system of applications linked to the confidential medical data distributed across the network and used by health professionals and patients. The access mediator 25 conceals the internal structure of the network and makes it possible to retain control of security and of the interfaces exposed to the users 6. It should be noted that the computerized health system in accordance with the invention may include a plurality of access servers 25, each being shared by different user groups, for example. To simplify the operation of the access servers and to increase their efficiency and speed, it is however preferable that they be grouped in the gateway infrastructures 2a, 2b. The access servers store in memory essentially only technical data and not medical data, although they can include technical caches for temporarily storing certain search results, such as addresses of servers and data constituting the medical file of a patient in order to be able to access it faster when a session on the network is opened by a user. However, once the session is closed, the data stored in this cache is deleted/lost.

The principal functions of the access technical mediator 25 are (see the interactions in Figure 2):

- authentication of users, including verification of possible revocation (see also Figure 8);
- authorization: the access mediator effects a first level of filtering of requests according to the role linked to the identity of the person submitting a request;
- management of sessions with users, in particular recovery of the access profile of the patient from a logging service technical mediator 29 in one of the data logging server systems 3;
- creation and verification of the validity of the documents (format, encoding, attributes, etc.) and transmission to the server system of logging data from the health professional concerned (see also Figure 9);
- searching for data from a medical file (see also Figure 10) at the request of a consultation application, where the file access mediator interrogates all the logging service mediators on submitting the document request to them and then collects the responses or absences of a response, consolidates the result and returns it to the application that initiated the request; the result of a search consists in a list of references to documents that can be consulted; documents to which access is not authorized are not listed;
- consultation of data from a medical file (see also Figure 11): based on a precise reference supplied by a consultation application, the file access mediator 25 interrogates the logging service mediator 29 concerned and recovers the content of the referenced document; the access to the document is logged by the access mediator;
- display of access rights: at the request of a profile management application, the access mediator obtains the profile of the access rights of the patient from a data logging server system (via the search system described above) and then returns the latter to the application that initiated the request;
- modification of access rights (see also Figure 12): at the request of the profile management application, the file access mediator 25 updates the access profile stored by the logging service mediator 29 of the trusted doctor of the patient concerned;

- logging of access: a record of each request is retained locally by the file access mediator;
- searching records of access by a given patient by interrogation of the application logs;
- administration: response to commands defined by the application administration common interface.

To this end, the access mediator collaborates with a number of components of the secure computer network system, the principal collaborations being as follows:

- the access mediator is used by the patient file management component, the virtual file consultation component 50 and the access profile management component 51;
- the access mediator uses the security services 53 for authentication and authorizations based on rolls, thanks to the certificates contained in the smart cards of the patient and the health professional;
- the access mediator uses the service 54 for validating published documents;
- the access mediator accesses all the logging service mediators 29 for the publication, searching, consultation and management of access profiles;
- the mediator uses the local application log service 55;
- the access mediator accesses all the application logs to reconstitute the instances of access to the file of a patient;
- the access mediator accesses the register (directory) 56 of health professionals to obtain the necessary information, such as the identifier of the logger of the health professional or their role;
- the access mediator accesses the configuration information of the computerized health system 57, such as the address of the loggers.

The service area 11 further includes a server system acting as the specialized technical access mediator 24 (hereinafter: "specialized access mediator") that materializes the gateway for user applications to value-added electronic services (hereinafter: "value-

added services" or VAS) such as the drug prescribing aid forming part of the computerized health system. The drug prescription aid electronic system 31 may comprise a database storing in electronic form a compendium of drugs and software to determine the appropriateness of a diagnosis as a function of the interaction between drugs, allergies and other conditions emerging from the medical file of the patient. The specialized access mediator 31 may include a server that essentially stores only technical data and has the following functions:

- receiving requests coming directly from user software via a secure communication tunnel;
- authenticating the user and authorizing the request in accordance with the rights linked to their identity and their role;
- transmitting requests to the value-added service 31a, 31b to which it is linked and returning responses to the user; thus it performs a classic "proxy" role for the value-added service protocol;
- at the request of the value-added service, interacting with the rest of the computerized health system, notably the logging service mediators 29, in order to obtain information (for example in the case of the drug prescribing aid);
- locally logging the actions effected.

For the aforementioned purposes, the specialized access mediator interacts with users and other components of the secure computer network system in the following principal collaborations (see Figures 2 and 5):

- the specialized access mediator is used by the value-added service clients 6a;
- the specialized access mediator calls and is called by the value-added service 31a, 31b to which it is linked;
- the specialized access mediator 24 (24a, 24b) accesses the logging service mediators 29 in order to search and consult medical documents;

- the specialized access mediator uses the security electronic services 53 provided in the high-security area 15 for authentication and authorizations based on the roles of users;
- the specialized access mediator uses the local application access log electronic service 58;
- the specialized access mediator accesses the electronic directory 56 of health professionals and roles provided in the high-security area 15 (such as the identifier of the data logging server system 3a of the health professional concerned);
- the specialized access mediator accesses the configuration information of the infrastructure of the secure computer network system (such as the addresses of the logging server systems), this information being stored in a management server system of the infrastructure 33 in the management area 16.

Value-added services, such as drug databases and logistical support, may be implemented in a centralized manner because they do not store information relating to patients. This centralization is only "logical", however, and does not exclude a "physical" decentralization for reasons of performance and accessibility.

At the architecture level, these value-added services can therefore be seen as black boxes of the computerized health system. They are made available to users via a specialized access mediator providing the junction between the VAS and the rest of the network.

Figure 6 shows one possible logic architecture for the prescribing aid electronic service. This service is invoked from a value-added service mediator 24b in turn invoked by a specialized access mediator 24a (not shown in Figure 6).

This VAS has its own data, notably a drug database (pharmacopia) 58 and potential interactions between drugs. Moreover, the interaction detection engine has access 59 to the patient's current prescriptions.

Referring to Figures 1 and 2, the service area 11 may further include a secure messaging server 34 used primarily for sending electronic messages between users 6b of the computerized health system or for transmission and storage of protected data, such as medical data of a patient, in a data logging server system 3a. In order to protect the data transmitted, the electronic messages are signed with the private key of the smart card of the health professional and sent to an address corresponding to another participant, for example 123456789@e-toile.ch where 123456789 is the identifier of the participant. The mail server accepts only mail coming from the VPN and the signature of which corresponds to a health professional known to the secure network system. The health professional can therefore add a message by way of a document attached to the patient in the document base of the data logging server system of the sending health professional.

The high-security area 15 includes a server system 32 including a health professionals electronic directory 57 (hereinafter: PDS directory) used to authorize user access as a function of their roles, an electronic certificate management system 35 (hereinafter: PKI manager), which stores and manages electronic certificates and lists of revoked certificates that have been sent, and a certification electronic authority 36 (hereinafter: certification authority) which acts as an authority for certification of the organization of the computerized health system. When production of the smart cards is subcontracted to an external organization, the electronic certificate management system 35 and the electronic certification authority 36 may be outside the secure computer network system in an external secure system under the control of the organization responsible for the production of the smart cards.

The high-security area 15 may further include an internal domain name server (hereinafter: internal DNS) 37 for managing the names of the internal hosts. Each of the components of the high-security area may take the form of a server system. The principal role of the PDS directory server system 32 is to inventory the health professionals affiliated to the computerized health system and to group together the necessary information on this subject. The PDS directory server system 32 essentially

stores administrative data, such as name, forename, address, speciality, etc. of the health professional, digital certificates of each health professional, information on the roles and/or the authorizations of the health professionals, and the addresses or other information on the data logging server system 3a associated with the user. The principal functions of the health professionals directory are as follows:

- creation of a new entry in the directory;
- modification of the attributes of an existing entry;
- deactivation of an entry;
- searching for and consulting entries in the directory;
- batch importing and exporting;
- establishing lists and reports via an administration human-machine interface (HMI);
- administration: response to commands defined by the application administration common interface.

The directory 57 of health professionals is used by the secure messaging service 34 in order to obtain the public key of the addressee of an encrypted message. The access mediators 25 also use the directory in order to authorize requests according to the role of a health professional.

The PKI manager 35 may be a standard market product for the production, distribution, revocation and verification of electronic certificates.

The certification authority server system 36 has the role of authenticating a user of the network and of authorizing certain requests as a function of their role. The certification authority server system essentially stores data on the certificates of the certification authority that issued the certificate of the smart cards of the users as well as revocation or access lists. The principal functions of the certification authority 36 are as follows:

- checking the authenticity of the certificate presented;
- verifying revocation lists;
- verifying authorizations linked to the role of a user;
- if necessary: establishing the security context of the session;
- administration: responding to the commands defined by the application administration common interface.

The certification authority is above all else used by the access mediators 25 or the specialized access mediators 24. It should be noted that the data from the revocation lists can also be stored on other servers and in this case the certification authority 36 will access those servers in order to verify the list of revocations.

The management area 16 includes a server system for the management of the infrastructure 33 of the computerized health system that makes the use of the infrastructure of the computer network possible by providing the following electronic services:

- surveillance of critical events (breakdown, overload, capacity overshoot, etc.);
- centralized record of events;
- history of use of network traffic;
- centralization of network configurations;
- centralization of server images (of Ghost type);
- generation of alarms in the event of critical events;
- possibilities for distributing updates;
- management of alarms by equipment and notification of the most severe alarms to the trouble ticketing system (TTS) of the help desk;
- managing the inventory of equipments and software versions deployed.

The management area 16 further includes an application electronic management system 38 for administering and managing the applications of the computerized health system, notably administration of applications and management of the

configuration of the various components and applications of the system, as well as teledistribution to the client-stations (see also under the heading deployment server).

As described above, the management area 16 may equally include a security management server system 28 for reconstituting or tracking events by analyzing the logs and from other data collected by the intrusion detection probes 27 installed at the critical points of the computerized health system.

The management area may also include a system 39 for producing compact disks or other media to supply the file to patients who request it, for example when they travel abroad.

The infrastructure management system 33 includes a configuration register 57 that retains the common information concerning the logical and physical configuration of the computerized health system. The data stored in this register further includes the addresses of the mediators, the value-added services and the common services such as the logs. The register, which is accessible by all the internal components of the computerized health system, has the following functions:

- searching for a configuration element and accessing its value(s);
- batch importing and exporting;
- where possible; automatic discovery of certain elements (for example mediators) included in the configuration;
- via HMI or administration interface: creating a new configuration entry, modifying or deleting an existing entry, producing lists.

It should be noted that the private configurations specific to each application component of the computerized health system are in principle not retained in the configuration register, but by a local ad hoc mechanism.

The application management server system 38 that enables use and control of the application components of the computerized health system may have the following functions:

- interrogating and displaying the status of the components (automatically and in response to an operator request);
- starting and stopping components;
- modifying the operating parameters of the components (if they allow this);
- detecting problems and reporting to operators;
- collecting and displaying statistics (for example response times, counters);
- scheduling actions on components (for example automatic starting of background maintenance tasks;
- automatic action as a function of certain events (e.g. restarting in the event of an error).

The management area 16 may also include a deployment server that makes available to health professionals updated software enabling access to the services of the computerized health system.

In the public area 9, the information portal server system (web server) has the principal role of supplying information to the public and to health professionals. This server system stores static HTML data and data structured in accordance with what is required, this server communicating with the administration area 16, notably with the infrastructure management server system 33 and the management and application server system 38 in order to obtain the status of the system. The principal functions of the information portal server system 20 are as follows:

- distributing basic static information (history, mission, modes of use, contact addresses, etc.);
- distributing service information (status of the system, problems, maintenance windows, announcements, events, etc.).

The portal server system is accessible without a VPN connection.

The data logging server system 3 that is connected to the backbone network 4 by an internal router 19b and an internal VPN secure tunnel 26 via an internal firewall 10b includes a server system acting as logging service technical mediator 29 (hereinafter: logging service mediator) and a document server 40. The logging service mediator 29 manages access to the data stored in the document server 40 when invoked by the access mediators 24, 25 in order to access the various components of the data logging server system 3. The logging service mediator also accesses the local log services 59 in order to retain a record of all operations effected by one or more components of the data logging server system. The principal functions of the data logging mediator are as follows:

- publication: receives a document to be published on behalf of the file access mediator 25 and confides it to the document server 40 for storage; creates and also stores on the server 40 the unique reference of each document of a patient;
- on publication of the first document of a patient on the logger concerned: creation of the file and of the access profile of the patient;
- searching: on reception of a document search request from a file access mediator, the logging service mediator searches the document server 40 for the references of documents corresponding to the search criteria, verifies and returns the results to the file access mediator and verifies the correct application of access rights;
- consultation of documents: on reception of a document consultation request from a file access mediator, the logging service mediator, if necessary, verifies the reference (e.g. whether it is correctly formulated and still valid), verifies the applicable access rights and obtains the document from the logger;
- verification of access rights relative to the access profiles and to the exceptions specified by the patient;
- updating of the default access profiles of the patients (not specific to a document);
- updating of exceptions (specific to a document) in the access rights;
- logging of requests;

- managing logging errors: as far as possible, the logging service mediator protects the rest of the network against logging errors (including processing of any time outs);
- administration: responding to commands defined by the application administration common interface.

It should be noted that each data logging mediator knows only the documents that it manages and the patients for which it holds a document, and the complete file of a patient may therefore be distributed across a plurality of data loggers, thereby avoiding the storage of a complete medical file on a single server or central register. This greatly enhances the protection of a patient's medical data given that it is extremely difficult for a third party to hack a plurality of secure systems in order to reconstitute the complete file.

For performance reasons, the service logging mediator is preferably physically near the reference server 41 and the document server 40. The role of the reference server is to make it possible to retrieve the references to the logged documents on the basis of search criteria. The data stored on the reference server essentially consists of the references to the documents stored in the document server 40, the attributes of those documents and the indexes.

The reference server may also include, or at least access, a (basic) register 60 of the access rights specific to the documents, this register preferably being located in at least one data logging server system 30, notably the logging server system of the trusted doctor of the patient.

The principal functions of the reference server 41 are as follows:

- storing the references to documents;
- storing attributes necessary for searches;
- creating and managing indexes necessary for searches;

- searching for references using criteria based on attributes (identity of patient, type of document, data, etc.), taking into account access restrictions imposed by the patient.

It should be noted that the reference server 41 could be integrated into or form part of the document server 40 or at least share the same data structures.

When searching for documents (see also Figure 10), a file access mediator interrogates all the logging service mediators and awaits from each of them a positive or negative response. This leads to loading the network, the access mediator (which must manage a large number of participants simultaneously) and each service mediator that has to respond to each request reaching it. This constitutes a risk that the performance of the request operations will be below the threshold of acceptability and that the eventual increase in the number of service loggers (and therefore the number of service mediators and reference servers) will degrade the overall performance of the network.

With the aim of preventing these potential problems, it is possible to install intermediary reference servers indexing the existence of documents or, more broadly, a file relating to a patient in a particular logger, as shown in Figure 1a.

The register 61 of access rights specific to documents has the role of managing the list of access exceptions, notably those that are required by the patient. This register can be integrated into the reference server using the same data structures as the latter but could equally be an entity distinct from the reference server. The register 61 of access rights specific to documents (also referred to as the "exceptions register") has the following principal functions:

- storing exceptions authorizing access by specific persons to certain documents;
- searching these exceptions using criteria relating to the patient, the health professional, the document or other data associated with the medical file.

The interactions of the register 61 of access rights specific to documents are principally as follows:

- consultation by the logging service mediator 29 at the time of searching for and consulting documents;
- updating by the logging service mediator in the context of management of rights by the patient;
- the logging service mediator registering a new exception the first time that a professional consults a document in order to guarantee them subsequent access even in the event of modification of the restrictions by the user;
- collaborating with the other components of the maintenance operations logger (e.g. preservation of referential integrity in the event of deleting documents).

The document server system 40 has the role of reliably and permanently storing the documents of the medical file of a patient. The data stored on the database of this server may be encrypted or not. The principal functions of the document server system are as follows:

- it accepts and stores new documents;
- on presentation of their reference, it delivers the requested documents for consultation;
- it deletes obsolete documents, in accordance with rules imposed by the system administrator;
- it imports and exports documents (separately or in batches);
- where applicable: it manages versions of documents.

The data logging mediator 29 accesses the document base of the document server 40 at the time of publication, searching and consultation of documents, as shown in Figures 9, 10 and 11.

In the present application, the term "publication" is used in relation to file documents for the operation of creating and storing documents on a document server, making it available to users of the computerized health system. In order to be able to publish the patient file, the computerized health system includes a patient file publication application 63 that generates and stores new documents in accordance with the procedure as shown in Figure 9. The publication application accesses the certificates and the functions of the smart card 8 via the smart card reader 9 and delegates all requests from the network to the file access mediator 25 of the gateway infrastructure 2a, 2b.

The principal functions of this application are as follows:

- authenticating the health professional by means of their smart card;
- transmitting documents to be published over the network (the documents are prepared locally either by dedicated applications or by conventional office automation tools);
- where applicable: holding the list of published documents and their references in the secure network system.

It should be noted that the smart card of the patient is not necessary for publishing documents, but the identifier of the patient is. The application does not enable modification of the published documents, in order to prevent abuse, and in the event of modification it is necessary to produce new versions of the documents. The application could be implemented via a classic graphical user interface (GUI) or a WEB presentation server accessed via a browser.

The computerized health system also includes a file consultation application 50 in order to enable a health professional or a patient to consult their file stored in the various data logging server systems, in accordance with their authorizations and their access profile. This application accesses the certificates and the functions of the smart card via the smart card reader and delegates all requests to the file access mediator

25 in the gateway infrastructure 2a, 2b. This application is also able to communicate with external applications for viewing certain types of documents (for example Acrobat, Graphic Viewer). As for the publication application, this consultation application could be implemented via a classic GUI client or via a WEB presentation server accessed via a browser.

The principal functions of the file consultation application are as follows:

- authentication of the health professional and the patient by means of their smart cards;
- searching for references of documents constituting the virtual file of the patient, on the basis of criteria to be defined (document type, publication date, source, etc.);
- consultation: searching for and displaying documents selected from the references returned by the search;
- printing of a displayed document, with inclusion of tracking information;
- where applicable: storing the references of documents already consulted;
- access to the information in an emergency without the card of the patient (but always with the card of the professional).

Another application separate from or integrated into the patient file publication application is a document validation application 54 that ensures that published documents satisfy the requirements of the secure network. This application is used by the file access mediator 25 at the time of publication and has the following principal functions:

- verification of conformance (format, encoder, syntax, structural rules, size);
- where applicable, completion of the attributes of the document;
- administration: responds to commands defined by the application administration common interface.

One important application of the computerized health system is the access profile management application 51 enabling a patient to manage their access rights profile and to view the log of access to their file. This application accesses the certificates and the functions of the smart card 8 via the card reader 9 and delegates all requests to the file access mediator 25. This application could be implemented by a classic GUI or by a WEB presentation server accessed via a browser. The principal functions of the access profile management application 51 are as follows:

- authentication of the patient by means of their smart card;
- searching for and displaying the access rights profile of the patient;
- modifying the access rights profile and updating it on the network;
- searching (in the logs) for access to the patient's file in a given period, followed by displaying the results;
- renewing the certificate of the smart card: a client application of the secure network must have the function of renewing the certificate inscribed in the smart card; the access profile management application may therefore have this function.

The access profile of a patient is stored in an access profile register 60 (also referred to as the access rights base) that is preferably stored in a logging service mediator 29 in a decentralized manner to make it more difficult to obtain illicit access to the document access restrictions. Instead of storing the access profiles register on the logging service mediator 29, it may equally well be located on the document server 40 in which the document concerned is stored. This register is used by the logging service mediator at the request of the file access mediator 25 at the time of initialization of a session or in the context of the management of the patient's access rights. The principal functions of the access profile register are as follows:

- creating an access profile on the first visit of the patient;
- modifying the access restrictions;
- deleting an access profile of a given patient;
- selection of the access profile of a given patient;

- administration: responds to commands defined by the application administration common interface.

Access by a health professional to documents published on the network of the computerized health system is subordinate to verification with three levels of control. The first level corresponds to the role of the issuer of a request. This may be a doctor, nurse or pharmacist, for example, and this level is linked to certain authorizations for access to the functions of the network. For example, a nurse could consult but not publish. The second level consists of the access profile defined by the patient. For example, this makes it possible to prohibit access to all gynaecological files and documents by the treating professionals but authorize it for trusted doctors. The third level is materialized by exceptions specific to particular documents or files and doctors. For example, it is possible to authorize access to the report of the gynaecological visit to doctor X at a specific date where doctor X is the treating doctor but not the trusted doctor.

The second and third levels are therefore processed together in order to authorize an access prohibited by the second level but authorized under exceptional circumstances by the third level.

One solution consists in retaining the access profile with the data logging the trusted doctor and providing access control lists (ACL) for each document, these ACL including only the access exceptions, not the profile itself.

In order to apply the access controls linked to the profile, the file access mediator 25 must supply it to the logging service mediators 29 at the time of each request. For a search request (see Figure 2 and 10), the file access mediator must therefore recover the access profile in the access rights space 60 from the logging service mediator 29 of the document logging server system of the trusted doctor, before interrogating all the access rights bases 60', 60" of the other logging mediators 29', 29". In order to

avoid this additional sub-request on each request by the client software, the access mediator 25 can retain the access profile temporarily in the session information.

Modification of the access profile by the patient (see also Figure 12) involves only updating the profile stored by the document logging the trusted doctor without modifying the ACL of all the documents.

Another solution for implementing the access control strategy would be for the ACL of each document to include the access profile defined by the patient, so that compliance with the ACL would alone suffice to apply the second and third control levels 2 and 3. For its part, the access profile is always stored in the data logging server system of the trusted doctor. At the time of updating the profile, it is then necessary to update the profile stored in the document logging the trusted doctor and to modify all the ACL of all the documents already published.

Referring to Figures 1, 2 and 8, a session is opened by a user application after the VPN secure tunnel is established between the station of the health professional 6 and the gateway infrastructure 2a, 2b. Given that establishing the VPN involves authentication of the VPN server 23 by the user and that all the servers in the gateway infrastructure may be considered safe, it is not necessary for the user application to authenticate again the servers with which it communicates (for example an access mediator).

On the other hand, it is necessary to identify and to authenticate the user to the certification authority server 36 (also referred to as the "security server") in order for the latter to know the identity of the person opening an application session and effect actions in accordance with this identity and the associated rights.

A health professional is attached to a specific data logging server system 3a, 3b, 3c that they may choose. At the time of the publication of a document, the latter is stored

in this data logging server system after passing various levels of authorization and validation, as shown in Figure 9.

Figure 10 shows the progress of a document search request that uses two very important mechanisms:

- the distribution of the search requests by the file access mediator to all the logging service mediators;
- the verification of the access rights based on restriction profiles and exception lists at the level of each logging service mediator (and therefore in a totally decentralized manner).

It may be noted that the access profile is transmitted by the access mediator to the various service mediators at the time of the search. This access profile is first recovered by exhaustively searching the service mediators in order to discover which one has the patient's access profile (the logging service mediator (MS) of the patient's trusted doctor will alone respond positively). Once the profile has been recovered, the access mediator may retain it as session data in order to accelerate subsequent requests (other searches or consultations).

Referring to Figure 11, the consultation of a document consists in obtaining the whole of a document based on its reference. To this end the file access mediator 25 communicates directly with the logging service mediator 29 concerned. Although the access rights were verified at the time of the search step, they must be verified again at the time of consultation in order to guard against the situation in which a reference has been passed to another person not having the required rights.

Moreover, a professional having accessed a document once must be able to access it again, even if the patient changes the access rights in the meantime. This is achieved by inscribing the identity of the professional in the list of exceptions linked to the document at the time of the first consultation.

As described above, the patient can modify the information access profiles, the rights being divided into two distinct types: restrictions based on document profiles and exceptions authorizing access to specific documents or files by particular persons.

To update the access profile (see Figure 12), the file access mediator 25 contacts the logging service mediator 29 of the patient's trusted doctor and provides them with the new profile to be saved. To update the access exceptions, the file access mediator transmits to each logging service mediator 29' the exceptions that concern it. The exceptions are stored in the access rights base 60' of the logging server system of the corresponding files. The steps modifying the access rights are shown in Figure 12.

Figure 13 shows how the value-added service 31a, 31b, in this instance the drug prescribing aid, is integrated into the secure network.

Electronic prescribing of drugs includes a real added value if it is backed up by a system for detecting drug interactions. In the context of the computerized health system, the prescribing service obtains information on all current prescriptions for the patient concerned from the logging service mediators 29, 29' in order to detect possible incompatibilities between drugs prescribed by different professionals.

In order to prevent problems linked to drug incompatibilities, the prescribing aid system searches all the current prescriptions published on the network of the computerized health system, despite the access restrictions defined by the patient. Nevertheless, in the event that incompatibility is proven, the prescriber is advised, but in such a manner that information to which they do not normally have access is not disclosed to them.

Referring to Figures 1 and 2, the interconnection point server system 5 includes an external service mediator 30 that acts as a gateway between the computerized health system and other medical or value-added networks. The principal functions of this interconnection point server system 5 are as follows:

- mutual authentication;
- format and protocol conversion;
- messaging relay;
- application proxy;
- error management;
- administration: responds to commands defined by the application administration common interface.

The computerized health system further includes application logs 55, 58, 59 for keeping a record of the operations effected by one or more components of the network, these applications being accessible to any local component. In order not to create a point of centralization of confidential data, each technical mediator is provided with its own application log that makes it possible to carry out *a posteriori* controls in the event of problems (illicit access, poor therapeutic decision in the light of the information supplied by the network, etc.). Data processed by the application logs includes a timestamp, the identification of the users participating in the operation, the nature of the operation, the identification of the documents concerned, and other pertinent parameters of the operation.

The principal functions of the application logs are as follows:

- storing a record;
- interrogation: searching for and supplying records corresponding to a search criterion bearing on the stored parameters;
- cleaning up obsolete records, if necessary;
- administration: responds to commands defined by the application administration common interface.

The backbone network 4 is a high bit rate communication network between the gateway infrastructures 2a, 2b and the data logging server systems 3 as well as the interconnection point server systems 5. All the data circulating on the backbone

network is encrypted, the data coding/decoding function being handled by the VPN concentrators situated in the gateway infrastructures and in each data logging server system and each interconnection point server system. In the example described, the backbone network is a closed network of logic type, such as a closed regional or metropolitan network (city network) using a fibre optic infrastructure, dedicated to a group of authorized users. It is equally possible, in so far as this is available, to employ a closed network based on a private infrastructure, i.e. of single use for the computerized health system.

The computerized health system preferably has at least two access infrastructure points 2a, 2b located on different sites in order to increase the security of stored technical and administrative data and to provide access to the network and ensure that it functions in the event of failure of one or more components of one of the gateway infrastructures.

Referring to Figure 4, the gateways embody redundancy at two levels:

- At the overall level, each gateway infrastructure is capable of functioning independently and of taking over all of the traffic handled by the other one in the event of failure or preventive operation thereof.
- At the level of each gateway, redundancy is introduced both at the level of the firewalls 10 (clusters) and at the level of the sensitive switches (duplication of equipments and connections between them). A single failure of an equipment should therefore not lead to the gateway infrastructure being taken out of service. To guard in this way against failure of one of the infrastructures of the gateways to the backbone network 4, a direct fibre optic link 17 connects the two intersite VPN concentrators 18 of each gateway infrastructure.

The two gateway infrastructures are moreover connected by direct fibre optic links at the level of the service areas and the high-security area. This enables replication of the various servers and data that has to be consistent between the two sites without

unnecessarily overloading access to the backbone network or the internal path through one or even two firewalls. Virtual local area networks (VLAN) common to the two gateway infrastructures may therefore be created, for example using the Ethernet Gigabit 802.1q protocol.

Three pairs of optical fibres therefore preferably connect the gateway infrastructures to provide the functions of redundancy and replication between the two gateways.

For example, two technological platforms on which the computerized health system may be based are summarized in the following table:

Element	Platform A	Platform B
Operating system	Unix and Linux	Windows (2003 Server or later)
Web server	Apache/Tomcat	IIS with ASP.NET support
Application server	JBoss	.NET Framework
Middleware	RMI/IIOP + SOAP	.NET Remoting + SOAP
Database server	Oracle	Oracle or SQLserver
LDAP server	OpenLDAP	Windows Active Directory

For communication between client software and an access mediator, in order to enable different software publishers to integrate the document publication, search and consultation services on the computerized health system, it is advantageous to propose an open communication interface. In this line of thinking, a Web services type interface based on SOAP/HTTP may be used in the current state of the technology.

For the communication between an access mediator and a service mediator, the mediators being technical software components internal to the secure network system,

the choice of an interfacing standard between the latter is dependent on their implementation. An implementation based on J2EE can use RMI/IIOP, an implementation based on .NET can use .NET Remoting, but there are other possibilities: JXTA (peer to peer communication), Web services, message queues, etc..

The database interface for accessing the databases (essentially by the service mediators) may employ the classic standards, which are JDBC in the Java universe or ODBC and ADO in the Microsoft universe.

The administration interface of the components managed by the secure network system such as the mediators can use the most appropriate standards for the implementation platform (RMI/IIOP, JMX, Web Services, WMI, etc.).

For the directory interface, the secure network system includes a central directory of the health professionals used by users via the secure messaging service as well as by health professionals. Access to this directory may employ the LDAP standard. Moreover, the secure network system maintains an up to date register of all the service mediators forming part of the network in order for the access mediators to know of or to redirect document manipulation requests. This register may be seen as an LDAP resource of the network.

The Figure 3 diagram illustrates the transposition of the logic architecture model according to the technological choices described above. This solution is based on the Java/J2EE technologies, but other solutions using other technologies such as .Net are possible. The architecture is of the n-tiers type: it is divided into layers clearly separating responsibilities in respect of presentation, specialism logic and data storage. The upper part represents the client layer, materially present with the health professionals accessing the computerized health system. The central part materializes the presentation layer and the specialism services linked to the computerized health system: access and service mediators, messaging server, value-added services.

Finally, the lower part encompasses the technical components of the computerized health system and the databases.

Where access by users (clients) is concerned, the interfaces adopted are based on open technologies and independent of any specific platform (HTTP, SOAP, SMTP, POP3, LDAP, etc.). The more technical interfaces used within the secure network system are linked to the technologies of the Java universe, in this instance essentially RMI/IIOP and JDBC.

The Web presentation layer uses HTTP services serving static HTML pages (Apache, for example) and JSP and Servlet type dynamic pages.

PATENTKRAV

1. Sikret it-netværkssystem til håndtering af beskyttede data, hvilket system er tilgængeligt for brugere (6), der er udstyret med chipkort til godkendelse og autorisation af brugere i systemet, idet systemet omfatter mindst én adgangspunktinfrastruktur (2a, 2b), der gennem et lukket backbone-kommunikationsnetværk (4) er forbundet med en flerhed af serversystemer til modtagelse af data (3a, 3b, 3c), som er placeret på forskellige steder, hvor hvert serversystem til modtagelse af data omfatter mindst én database, hvor beskyttede data, der udgør dokumenter, er lagret, og en teknisk formidler af logningstjeneste (29) til at styre adgangen til de dokumenter, der er lagret i databasen, idet flere dokumenter, der udgør en sagspakke vedrørende en person, kan være fordelt over flere serversystemer til modtagelse af data, og idet adgangspunktinfrastrukturen omfatter mindst én formidler af adgang til sagspakkerne (25) i form af et serversystem med applikationer, der kontrollerer og styrer brugeres (6) adgang til de dokumenter, der er lagret i serversystemerne til modtagelse af data, **kendetegnet ved**, at formidleren af adgang til sagspakkerne (25) er konfigureret til at fordele en anmodning fra en autoriseret bruger af det sikrede it-netværkssystem om at søge et dokument til samtlige de tekniske formidlere af logningstjenester (29), og de tekniske formidlere af logningstjenester (29) er konfigureret til at kontrollere brugerens adgangsrettigheder med udgangspunkt i adgangsrettighedsprofiler, og formidleren af adgang til sagspakkerne (25) er konfigureret således, at formidleren af adgang til sagspakkerne (25) ved opslag i et dokument henvender sig direkte til den pågældende tekniske formidler af logningstjenester (29) efter et trin med søgning efter dokumentet og på ny kontrollerer adgangsrettighederne til dokumenterne i forhold til den bruger, der anmoder om opslag, inden det overføres til brugeren.

2. System ifølge krav 1, **kendetegnet ved**, at serversystemet til modtagelse af data indeholder en dokumentserver (40) og et register (61), der omfatter oplysninger om adgangsrettighederne til forskellige dokumenter, der er lagret på denne server, for at bestemme adgangsrettighederne til dokumenterne i en sagspakke afhængigt af identiteten eller rollen af den bruger, der anmoder om adgang til sagspakken.

3. System ifølge krav 2, **kendetegnet ved**, at adgangsregistret er i form af et register over undtagelser, hvor der lagres oplysninger om uautoriserede adgange.

4. System ifølge et af de foregående krav, **kendetegnet ved**, at det omfatter et serviceområde, hvor formidleren af adgang til sagspakkerne (25) befinder sig, og et højsikkerhedsområde (15), der er adskilt fra serviceområdet gennem en firewall (10c), idet højsikkerhedsområdet omfatter et serversystem med certificeringsmyndighed (36), hvor der lagres data om elektroniske certifikater, der svarer til de elektroniske certifikater, som er lagret på brugernes chipkort.

5. System ifølge det foregående krav, **kendetegnet ved**, at højsikkerhedsområdet omfatter en elektronisk fortegnelse over brugeroplysninger, herunder disse brugeres identitet og rolle.

6. System ifølge et af de foregående krav, **kendetegnet ved**, at der er mindst to adgangspunktinfrastrukturer (2a, 2b), der er fysisk adskilt, og som forbindes af backbone-kommunikationsnetværket (4).

7. System ifølge et af de foregående krav, **kendetegnet ved**, at adgangspunktinfrastrukturerne omfatter et ydre VPN-område (Virtual Private Network) (8), der er forbundet med et serviceområde (11) gennem en firewall (10b), hvor formidleren af adgang til sagspakkerne (25), der er forbundet med et højsikkerhedsområde (15) gennem en firewall (10c), befinder sig.

8. System ifølge det foregående krav, **kendetegnet ved**, at det ydre VPN-område (8) omfatter en VPN-koncentrator, såsom en koncentrator af typen SSL 25 (Secure Socket Layer), til kommunikation over internettet (7) med brugerstationer (6) gennem en sikret kommunikationstunnel.

9. System ifølge et af kravene 7 eller 8, **kendetegnet ved**, at serviceområdet omfatter en dedikeret adgangsformidler (24) i form af et serversystem med applikationer til at styre brugernes adgang til elektroniske tjenester med merværdi.

10. System ifølge et af de foregående krav, **kendetegnet ved**, at dokumentserveren (40) i serversystemet til modtagelse af data er adskilt fra serversystemet i den tekniske formidler af logningstjenester (29) og er forbundet med backbone-netværket (4) gennem en firewall (10b).

11. System ifølge et af de foregående krav, **kendetegnet ved**, at hvert serversystem til modtagelse af data omfatter en elektronisk logfil til at logføre alle forespørgslerne vedrørende lagring eller læsning af beskyttede data.

12. System ifølge et af de foregående krav, **kendetegnet ved**, at adgangspunkt-infrastrukturen omfatter et styringsområde (16), der omfatter serversystemer (33, 38, 28) til styring af infrastrukturen og applikationerne i det sikrede it-netværkssystem, idet dette område er forskelligt fra det tjenesteområde, hvor formidleren af adgang til sagspakkerne (25) befinder sig, og det kun er tilgængeligt for det administrative personale, der er ansvarligt for operationerne til styring af infrastrukturen.

13. System ifølge det foregående krav, **kendetegnet ved**, at styringsområdet omfatter et serversystem til sikkerhedshåndtering (28) forbundet med indtrængningsdetektionssonder (27), der er installeret på kommunikationslinjer i det sikrede it-netværkssystem (2), og som har applikationer med henblik på at rekonstruere eller spore hændelser ved at analysere logfilerne i adgangspunktinfrastrukturen og i serversystemerne til modtagelse af data (3a, 3b, 3c) såvel som de data, der sendes af indtrængningsdetektionssonderne.

14. System ifølge krav 12 eller 13, **kendetegnet ved**, at styringsområdet omfatter et system til infrastrukturstyring (33), der omfatter et konfigurationsregister (57), hvor oplysningerne om den logiske og fysiske konfiguration af det sikrede it-netværkssystem

er lagret, herunder adresserne på formidlerne og på serversystemerne til tjenester med merværdi.

15. System ifølge et af de foregående krav, **kendetegnet ved**, at adgangspunkt-infrastrukturen omfatter en sikret meddelelsesserver til afsendelse af elektroniske meddelelser mellem brugere eller til transmission af beskyttede data, idet den sikrede meddelelsesserver anvender de private elektroniske nøgler på brugernes chipkort til at kryptere de transmitterede data.

16. System ifølge et af de foregående krav, **kendetegnet ved**, at det omfatter ét eller flere serversystemer af typen sammenkoblingspunkter (5), der dels er forbundet med adgangspunktinfrastrukturerne (2a, 2b) gennem backbone-netværket (4), og dels med andre netværk eller tjenester med merværdi, idet serversystemet af typen sammenkoblingspunkt omfatter en formidler af ydre tjenester (30), der fungerer som en gateway mellem det sikrede it-netværkssystem og de andre netværk, og som omfatter funktionerne til gensidig godkendelse og til format- og protokolkonvertering samt mail-relæer.

17. System ifølge et af de foregående krav, **kendetegnet ved**, at det omfatter serverlogs (55, 58, 59) til at gemme et spor af de operationer, der udføres af én eller flere komponenter i systemet, idet de data, der behandles af serverloggene, er identifikation af de brugere, der deltager i operationen, operationens art, identifikation af de pågældende dokumenter og et tidsstempel.

18. Fremgangsmåde til håndtering af data i et sikret it-netværkssystem, der omfatter mindst én adgangspunktinfrastruktur (2a, 2b), som gennem et lukket backbone-kommunikationsnetværk (4) er forbundet med en flerhed af serversystemer til modtagelse af data (3a, 3b, 3c), som er placeret på forskellige steder, hvor hvert serversystem til modtagelse af data omfatter mindst én database (62), hvor beskyttede data, der udgør dokumenter, er gemt, og en teknisk formidler af logningstjenester (29) til at styre adgangen til de dokumenter, der er lagret i databasen, idet fremgangsmåden

omfatter oprettelse og lagring af dokumenterne i dokumentservere (40), der befinder sig i serversystemerne til modtagelse af data, og idet dokumenterne, der udgør en sagspakke, er fordelt over forskellige serversystemer til modtagelse af data, og idet adgangspunktinfrastrukturen omfatter mindst én formidler af adgang til sagspakkerne i form af et serversystem med applikationer, der kontrollerer og styrer brugeres (6) adgang til de dokumenter, der er lagret i serversystemerne til modtagelse af data, **kendetegnet ved**, at anmodningen om søgning i forbindelse med udstedelsen af en anmodning fra en autoriseret bruger af det sikrede it-netværkssystem om at søge et dokument fordeles af formidleren af adgang til sagspakkerne (25) til samtlige de tekniske formidlere af logningstjenester (29), og adgangsrettighederne med udgangspunkt i adgangsrettighedsprofilerne ved hver teknisk formidler af logningstjenester (29) kontrolleres, **kendetegnet ved**, at formidleren af adgang til sagspakkerne (25) ved opslag i et dokument henvender sig direkte til den pågældende tekniske formidler af logningstjenester (29) efter trinnet med søgning efter dokumentet og på ny kontrollerer adgangsrettighederne til dokumenterne i forhold til den bruger, der anmoder om opslag, inden det overføres til brugeren.

19. Fremgangsmåde ifølge det foregående krav, **kendetegnet ved**, at der ved hjælp af en applikation til styring af adgangsprofilen (51) lagres en profil, der defineres af en bruger, for adgang til dokumenterne fra vedkommendes sagspakke i mindst ét af serversystemerne til modtagelse af data (3a, 3b, 3c).

20. Fremgangsmåde ifølge det foregående krav, **kendetegnet ved**, at der i hvert serversystem til modtagelse af data, hvor der lagres dokumenter fra en sagspakke, lagres adgangskontrollister, der er specifikt forbundet til de lagrede dokumenter, og som kun bestemmer adgangsprofilen for disse dokumenter.

21. Fremgangsmåde ifølge et af de foregående krav, **kendetegnet ved**, at der lagres oplysninger om identiteter af og roller for brugerne af det sikrede it-netværkssystem, i en fortegnelse i serversystemet i et højsikkerhedsområde i adgangspunktinfrastrukturen, idet formidleren af adgang (25) har adgang til denne fortegnelse for bl.a. at bestemme brugernes adgangsrettigheder alt efter brugernes identitet og rolle.

22. Fremgangsmåde ifølge et af de fire foregående krav, **kendetegnet ved**, at formidleren af adgang til journalerne under oprettelsen og lagringen af et dokument ved hjælp af en valideringsapplikation kontrollerer dokumentets overensstemmelse, hvad angår dets format, dets syntaks og dets attributter.

5

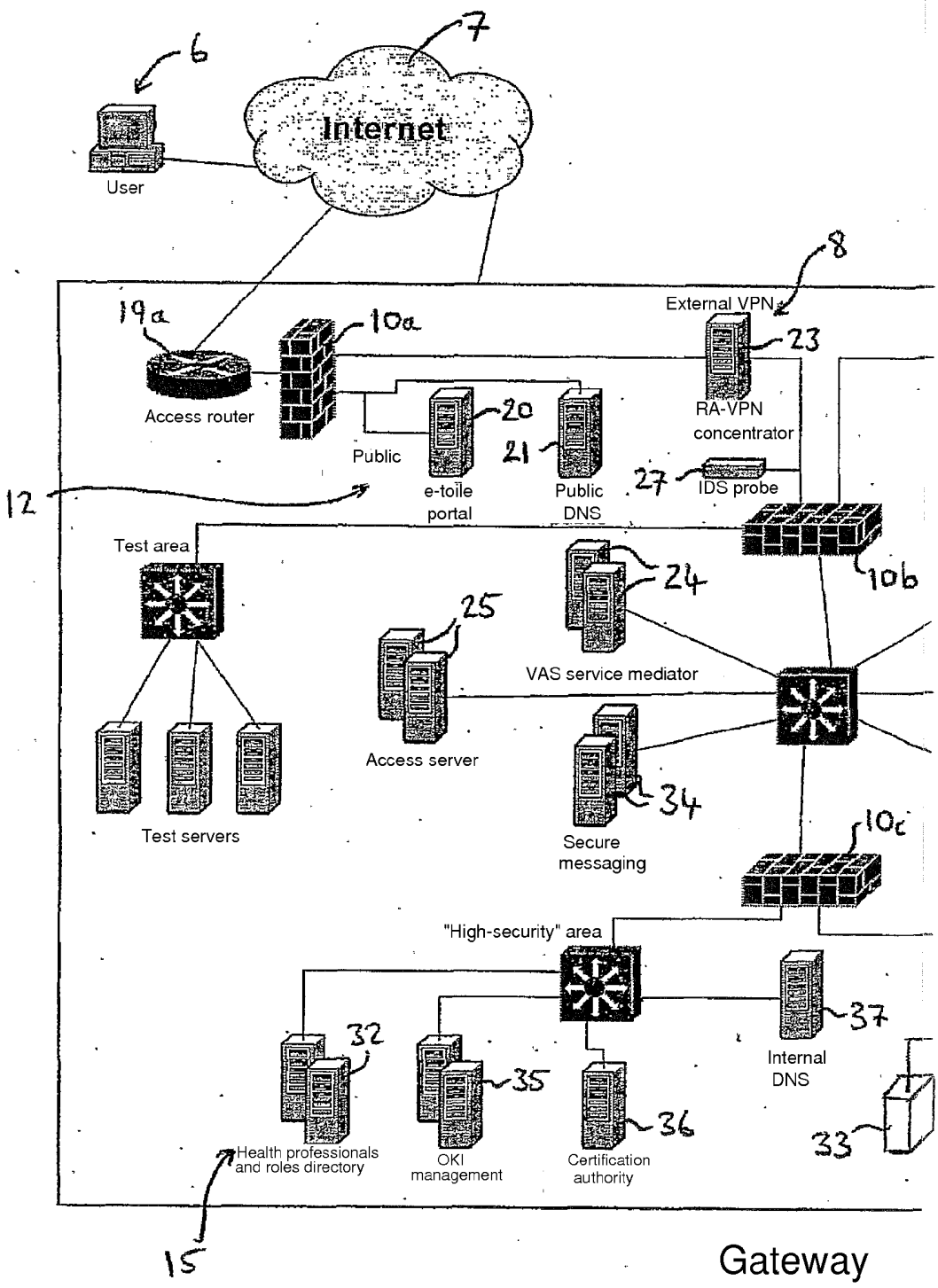

Fig. 1 (continued on the next page)

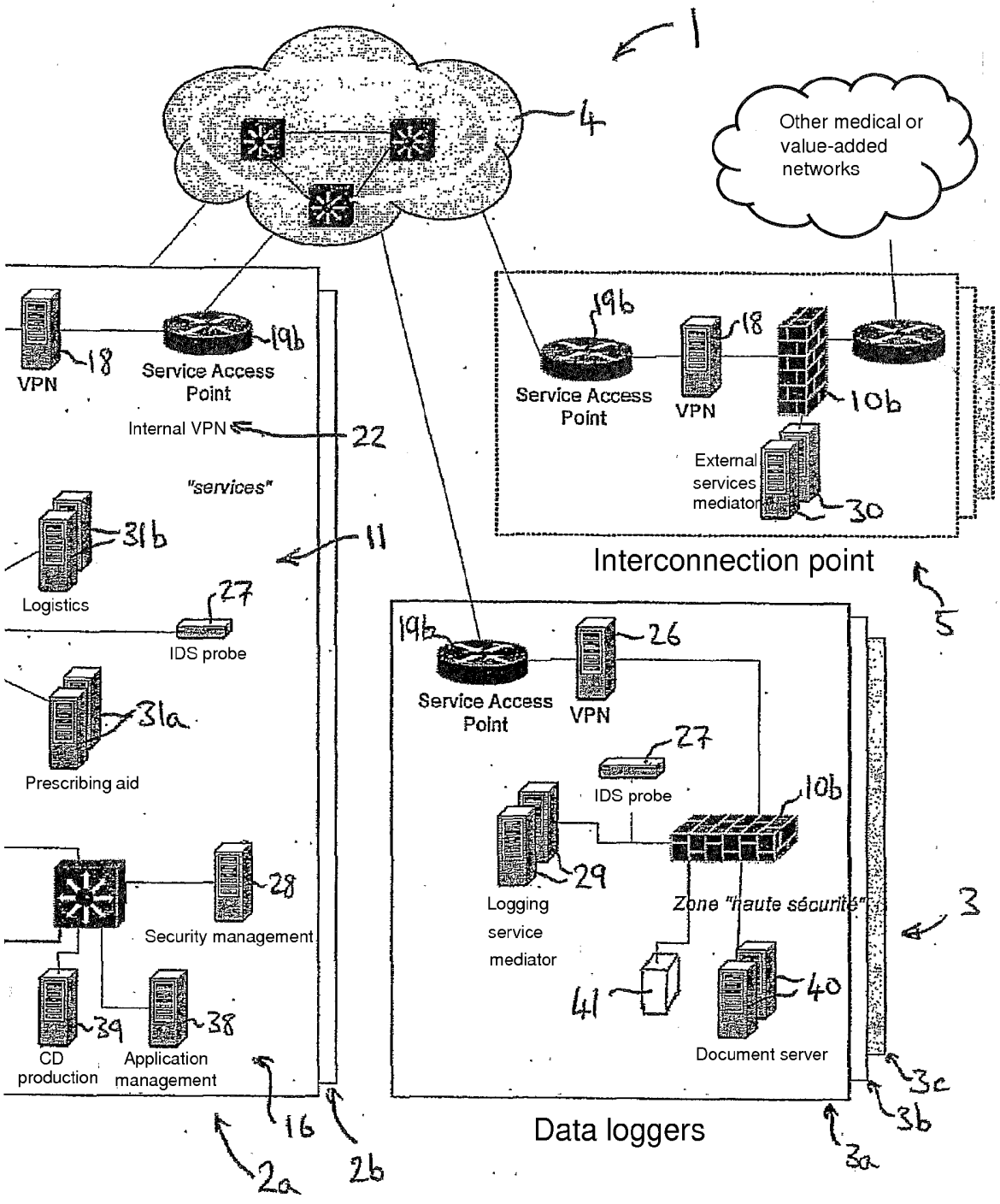

Fig. 1 (continued on the previous page **)**

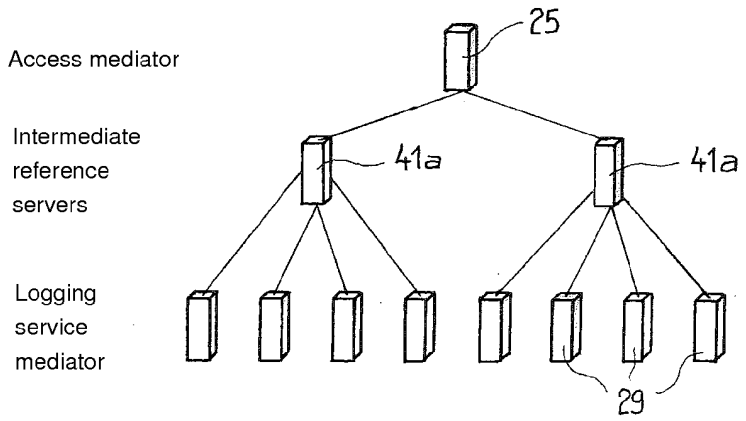
Access mediator
Intermediate reference servers
Logging service mediator
25
41a
41a
29

Fig.1a

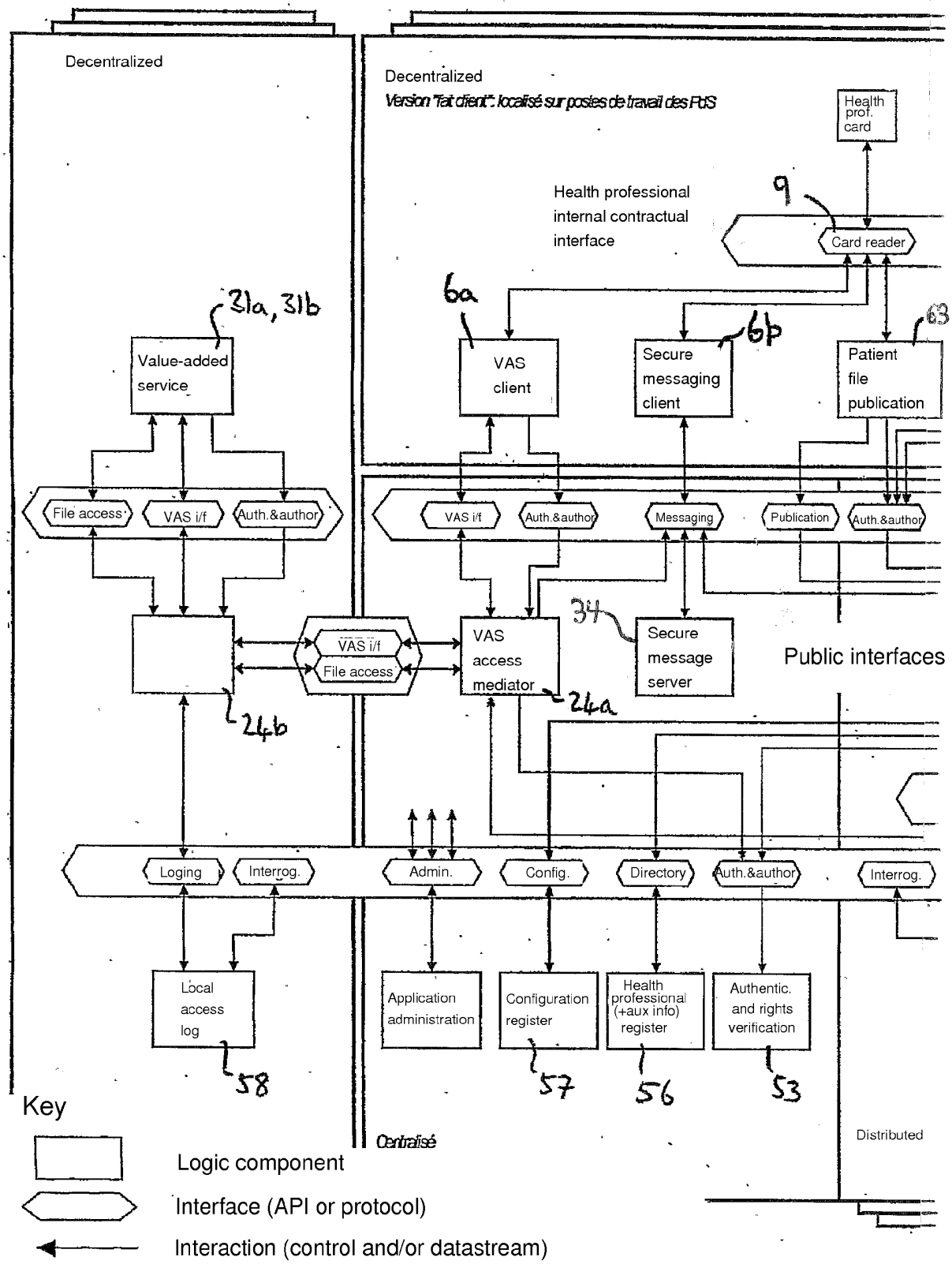

Fig. 2 (continued on the next page)

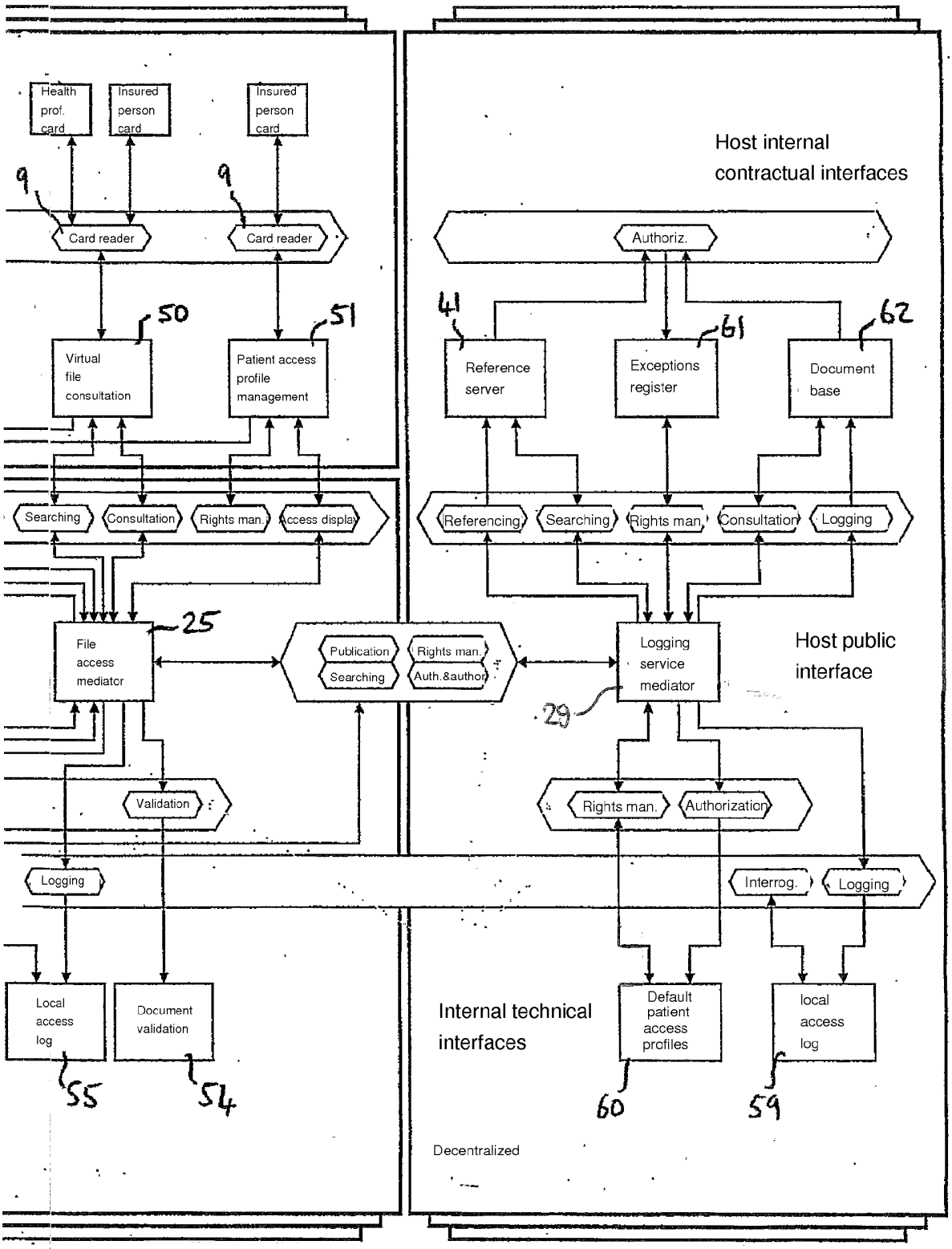

Fig. 2 (continued on the previous page **)**

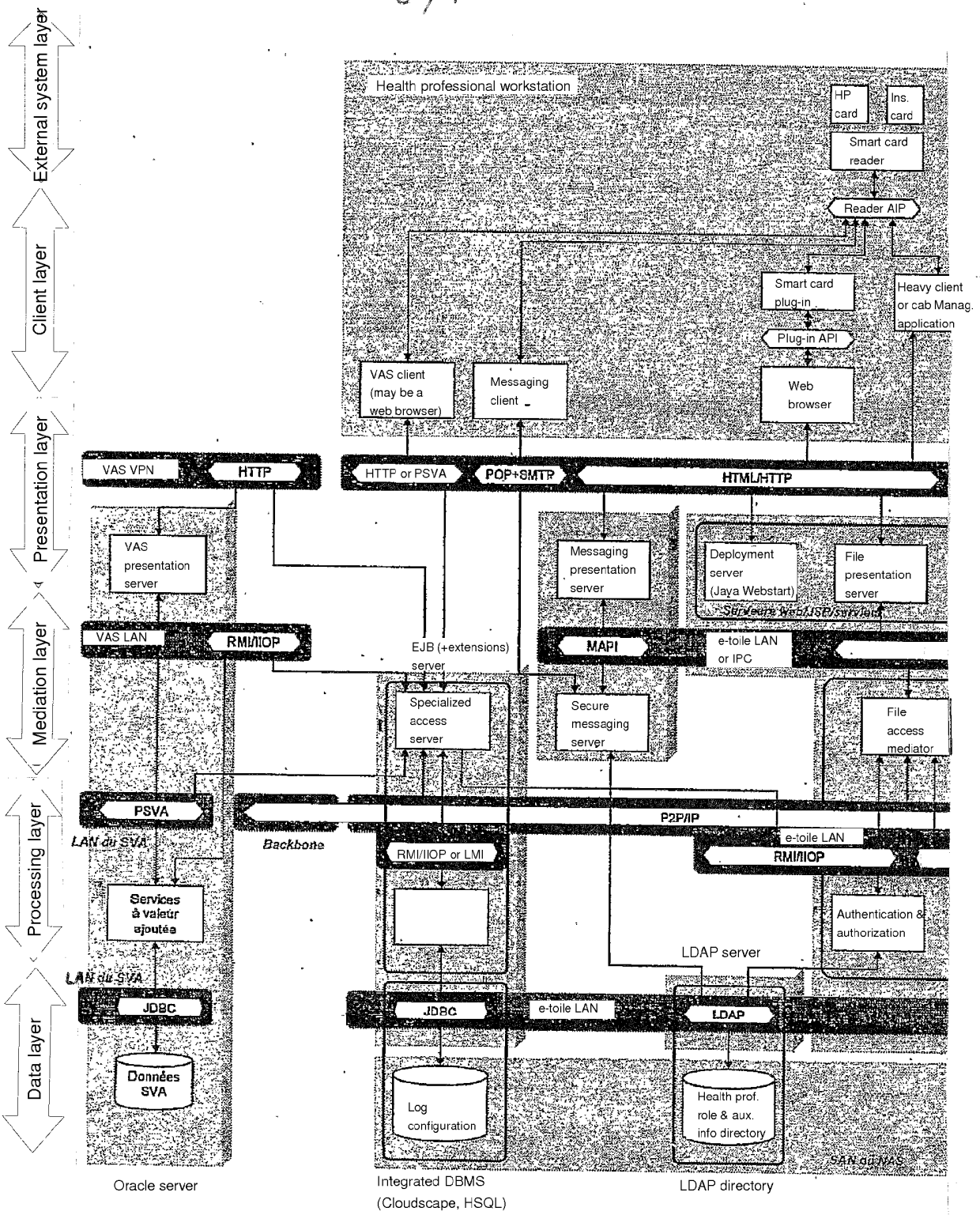

Fig. 3 (continued on the next page)

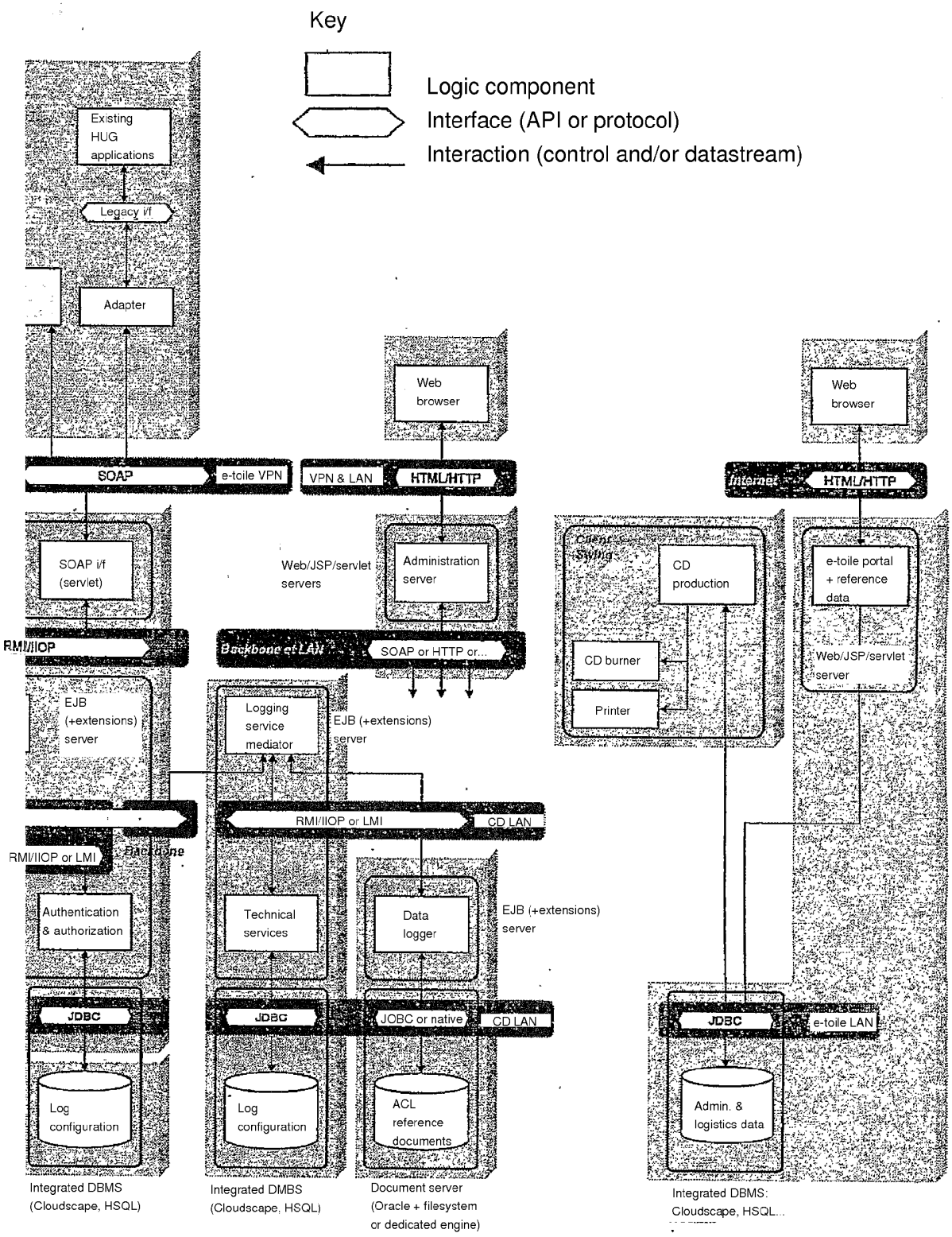

Fig. 3 (continued on the previous page **)**

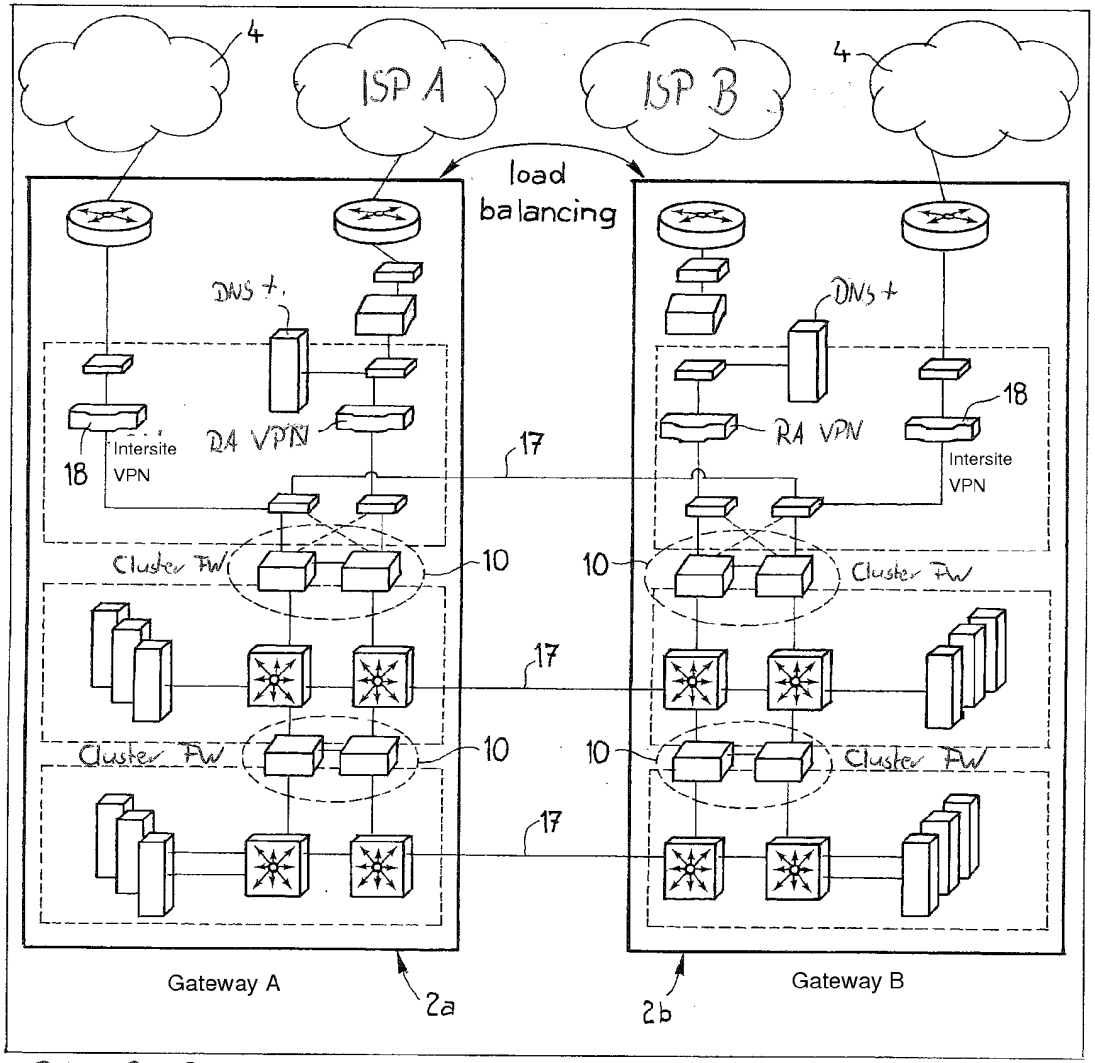

Fig.4

RA VPN: Remote access VPN
ISP : Internet Service Provider

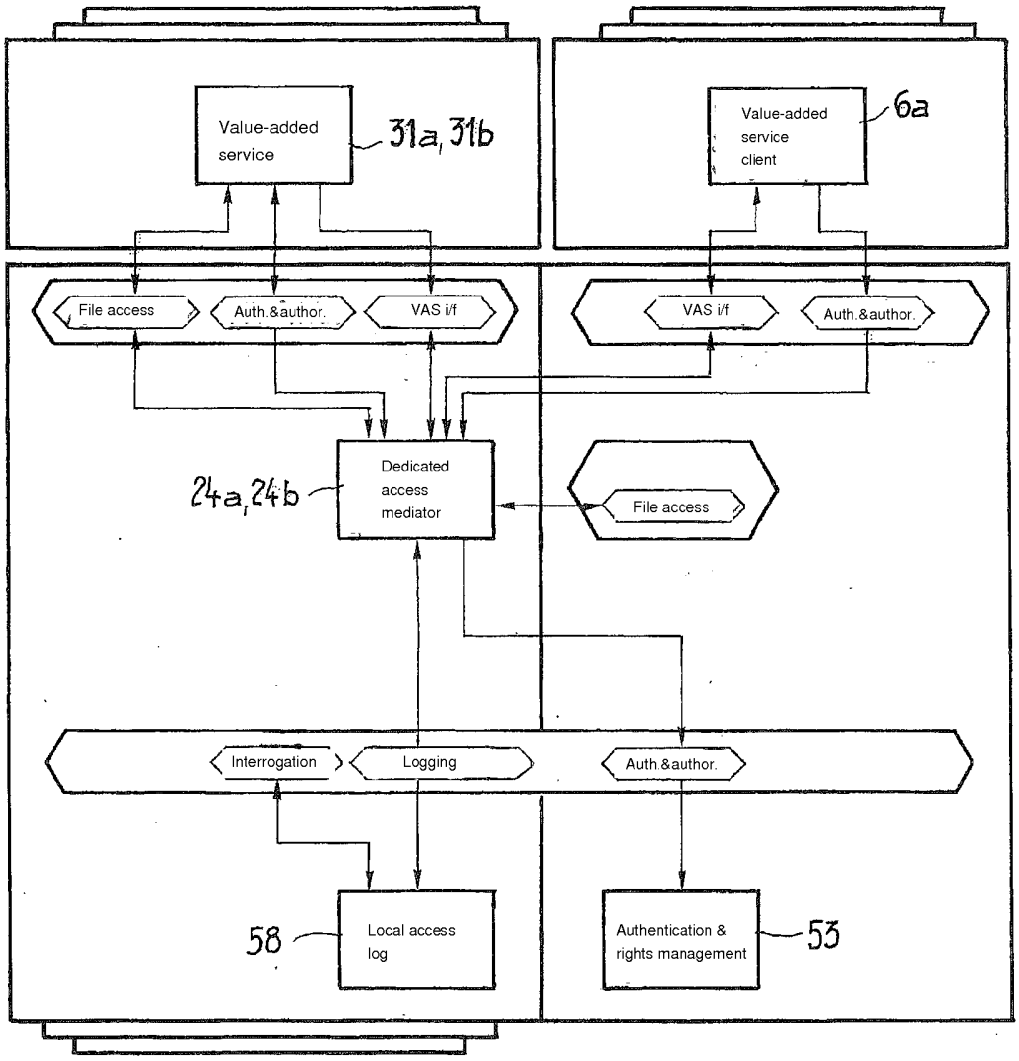
Value-added service
31a, 31b
Value-added service client
6a
File access
Auth.&author.
VAS i/f
VAS i/f
Auth.&author.
24a, 24b
Dedicated access mediator
File access
Interrogation
Logging
Auth.&author.
58
Local access log
Authentication & rights management
53
Key
Logic component
Interface (API or protocol)
Interaction (control and/or datastream)

Fig.5

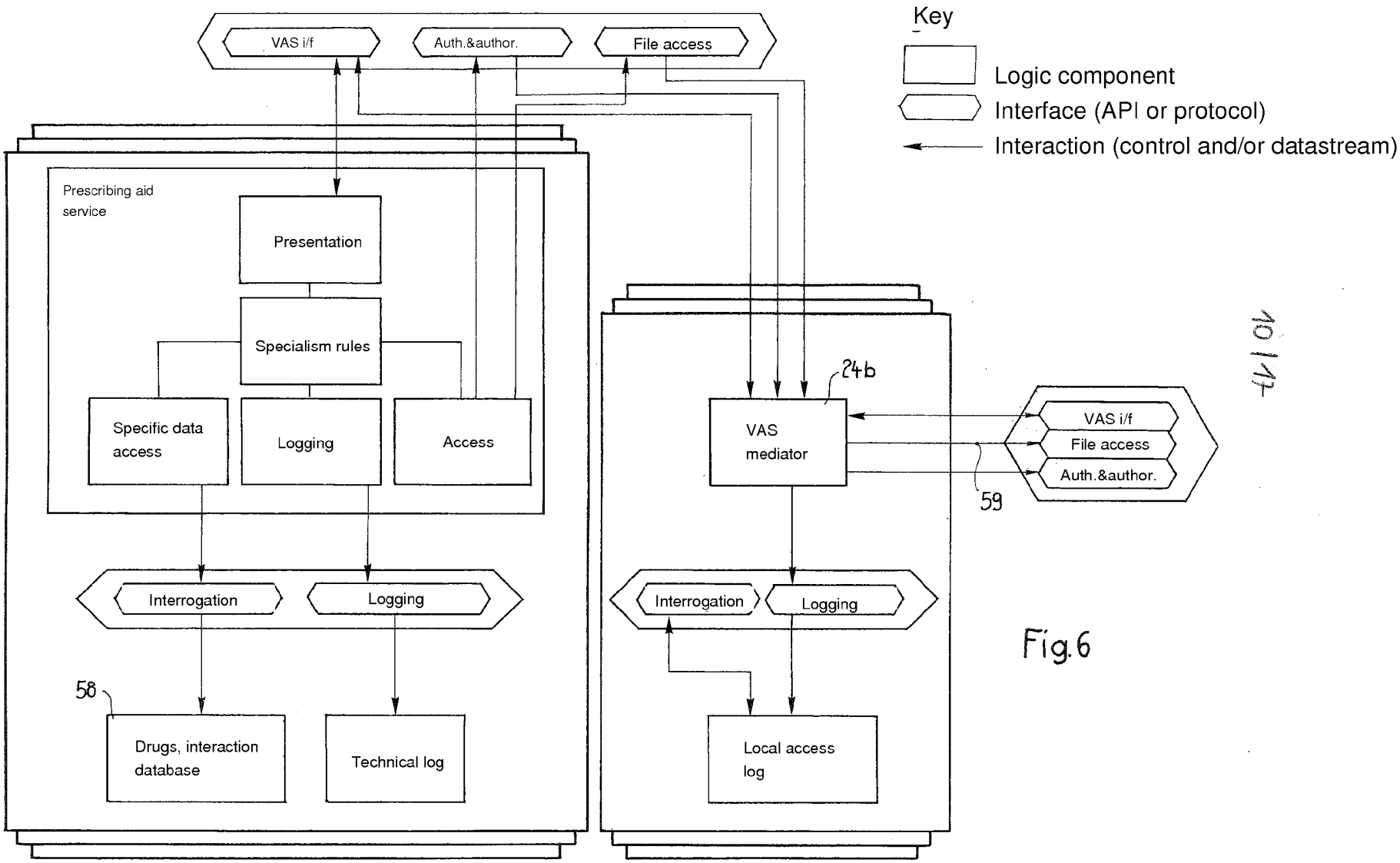
Key
Logic component
Interface (API or protocol)
Interaction (control and/or datastream)
VAS i/f
Auth.&author.
File access
Prescribing aid service
Presentation
Specialism rules
Specific data access
Logging
Access
Interrogation
Logging
58
Drugs, interaction database
Technical log
24b
VAS mediator
VAS i/f
File access
Auth.&author.
59
Interrogation
Logging
Local access log

Fig.6

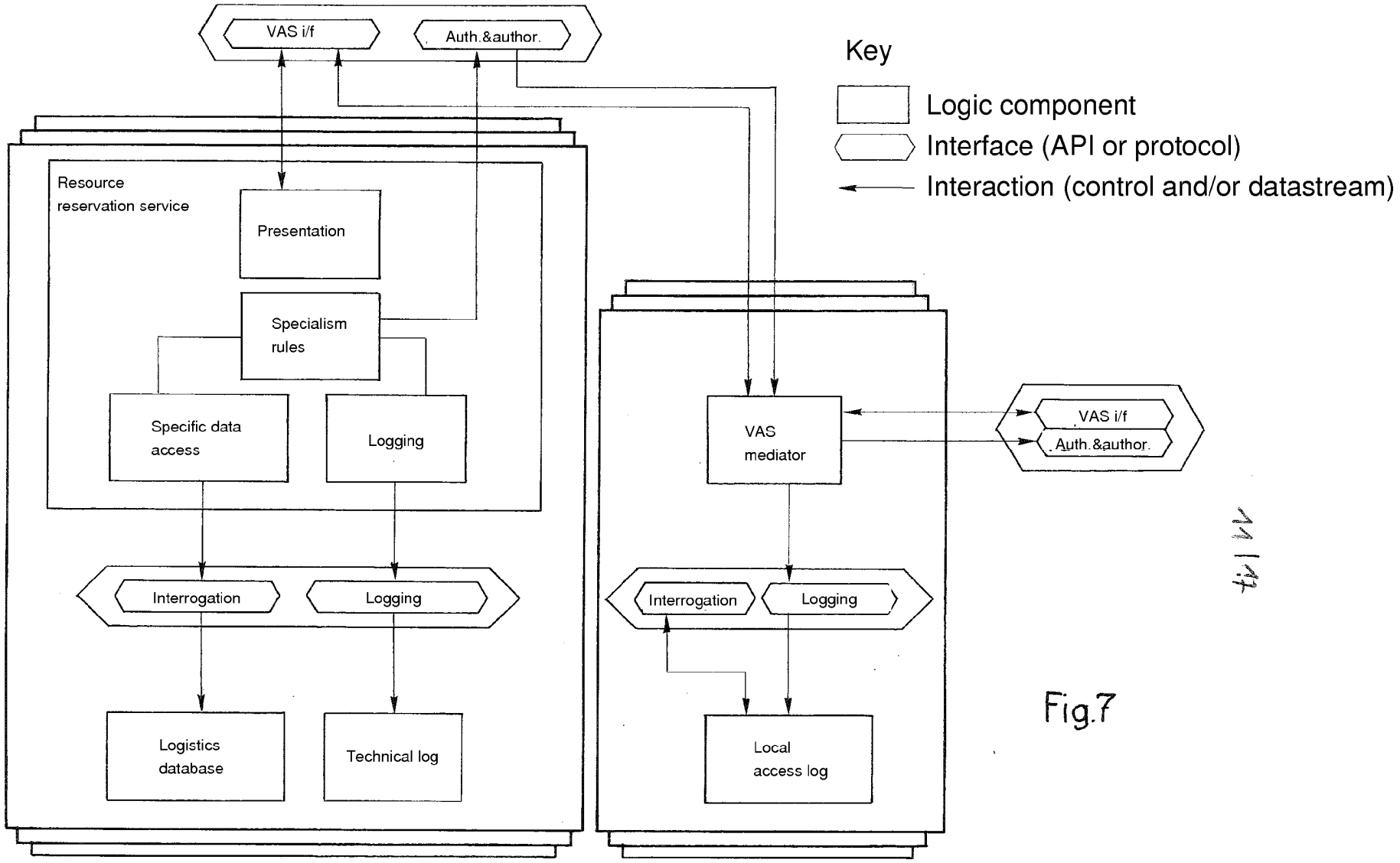
VAS i/f
Auth.&author.
Key
Logic component
Interface (API or protocol)
Interaction (control and/or datastream)
Resource reservation service
Presentation
Specialism rules
Specific data access
Logging
Interrogation
Logging
Logistics database
Technical log
VAS mediator
VAS i/f
Auth.&author.
Interrogation
Logging
Local access log

Fig.7

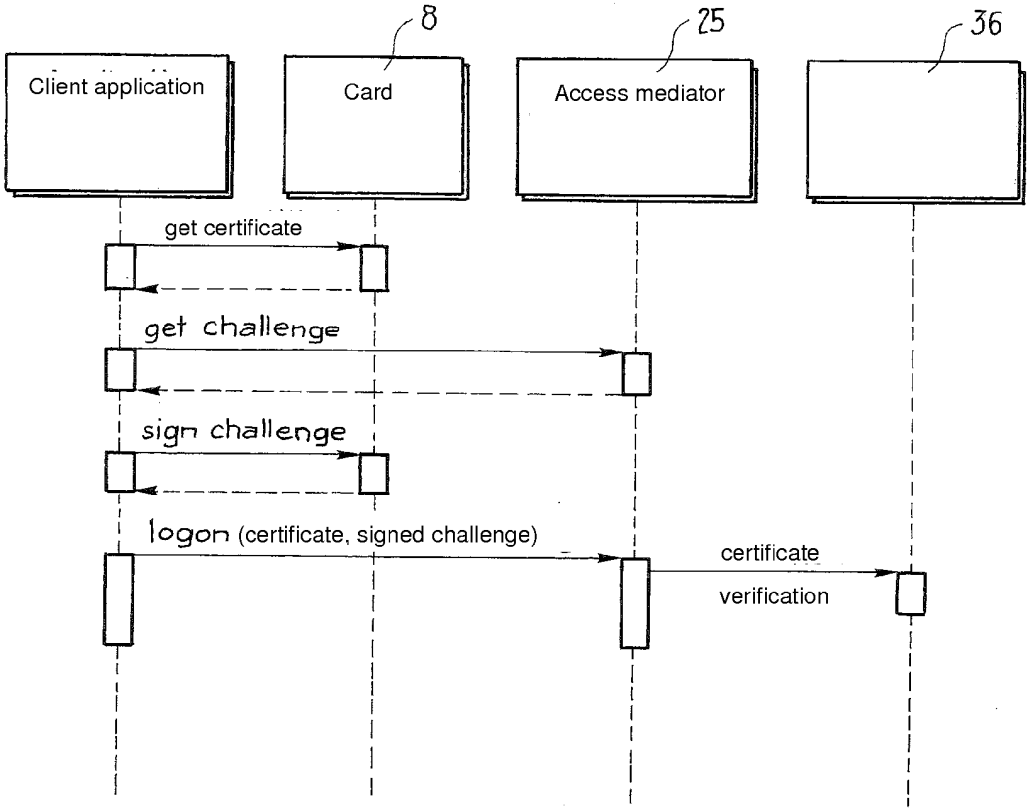
8
25
36
Client application
Card
Access mediator
get certificate
get challenge
sign challenge
logon (certificate, signed challenge)
certificate
verification

Fig.8

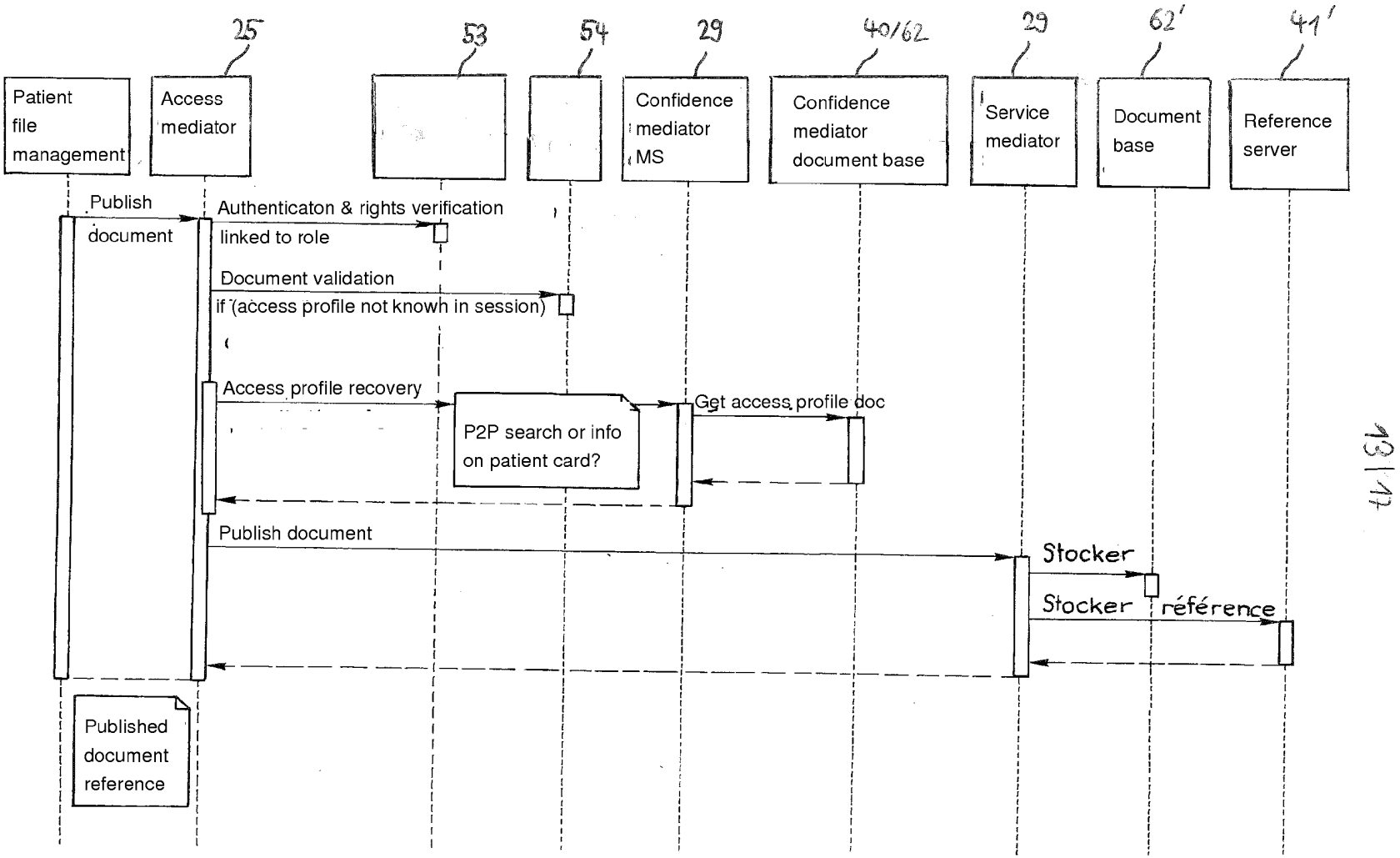
25
53
54
29
40/62
29
62'
41'
Patient file management
Access mediator
Confidence mediator MS
Confidence mediator document base
Service mediator
Document base
Reference server
Publish document
Authenticaton & rights verification linked to role
Document validation
if (access profile not known in session)
Access profile recovery
P2P search or info on patient card?
Get access profile doc
Publish document
Stocker
Stocker référence
Published document reference

Fig.9

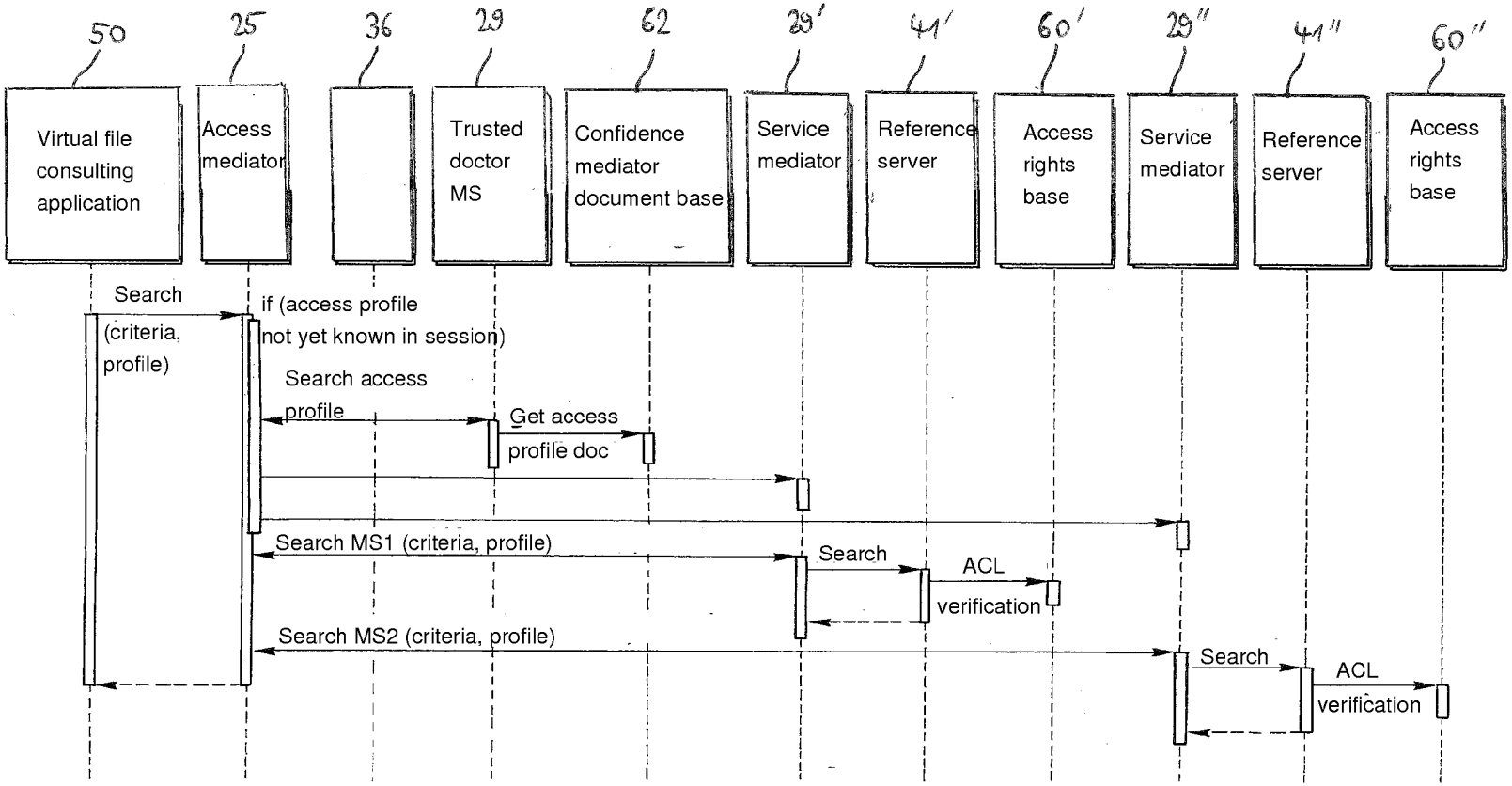
50
25
36
29
62
29'
41'
60'
29"
41"
60"
Virtual file consulting application
Access mediator
Trusted doctor MS
Confidence mediator document base
Service mediator
Reference server
Access rights base
Service mediator
Reference server
Access rights base
Search (criteria, profile)
if (access profile not yet known in session)
Search access profile
Get access profile doc
Search MS1 (criteria, profile)
Search
ACL verification
Search MS2 (criteria, profile)
Search
ACL verification

Fig.10

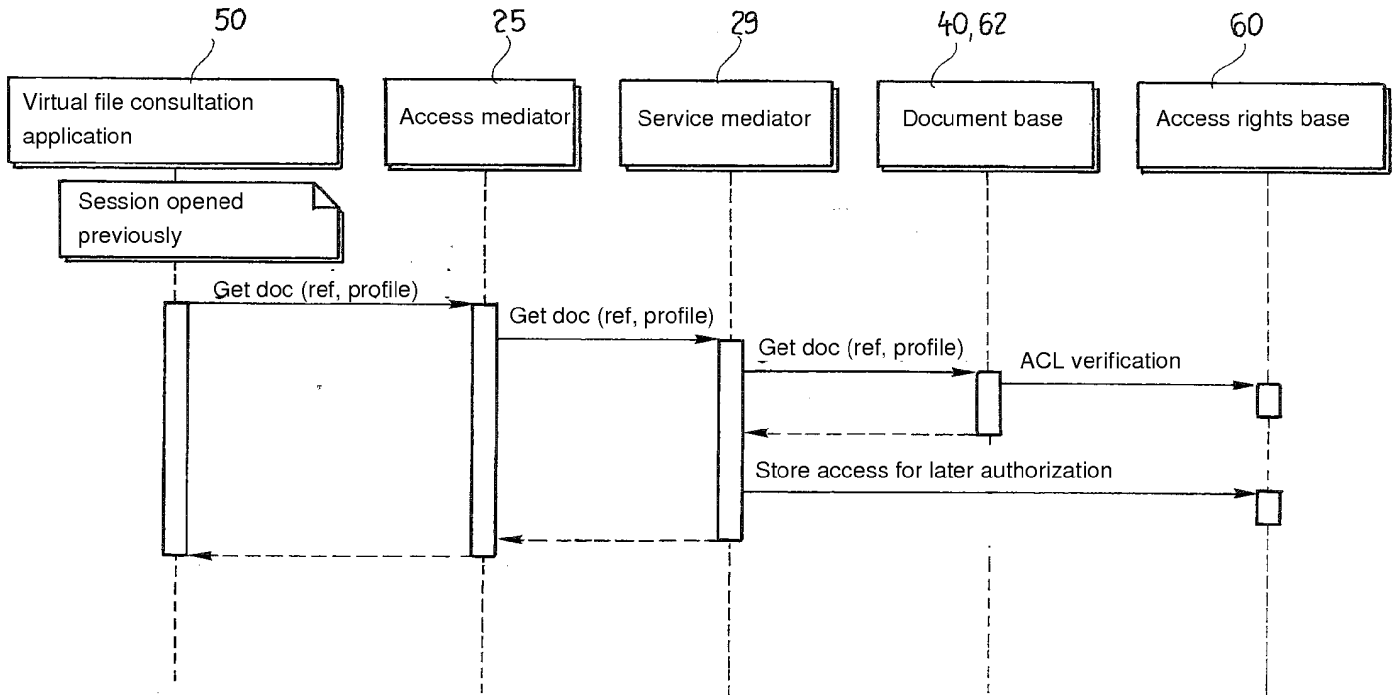
50
25
29
40,62
60
Virtual file consultation application
Access mediator
Service mediator
Document base
Access rights base
Session opened previously
Get doc (ref, profile)
Get doc (ref, profile)
Get doc (ref, profile)
ACL verification
Store access for later authorization

Fig. 11

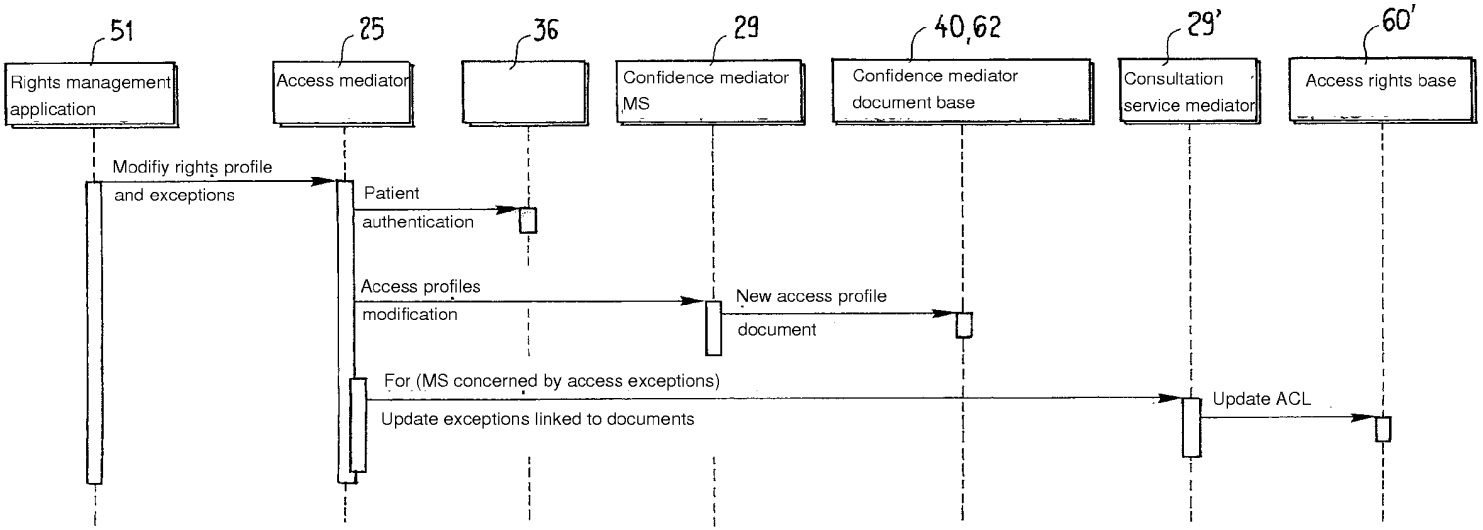
51
25
36
29
40,62
29'
60'
Rights management application
Access mediator
Confidence mediator MS
Confidence mediator document base
Consultation service mediator
Access rights base
Modifiy rights profile and exceptions
Patient authentication
Access profiles modification
New access profile document
For (MS concerned by access exceptions)
Update exceptions linked to documents
Update ACL

Fig.12

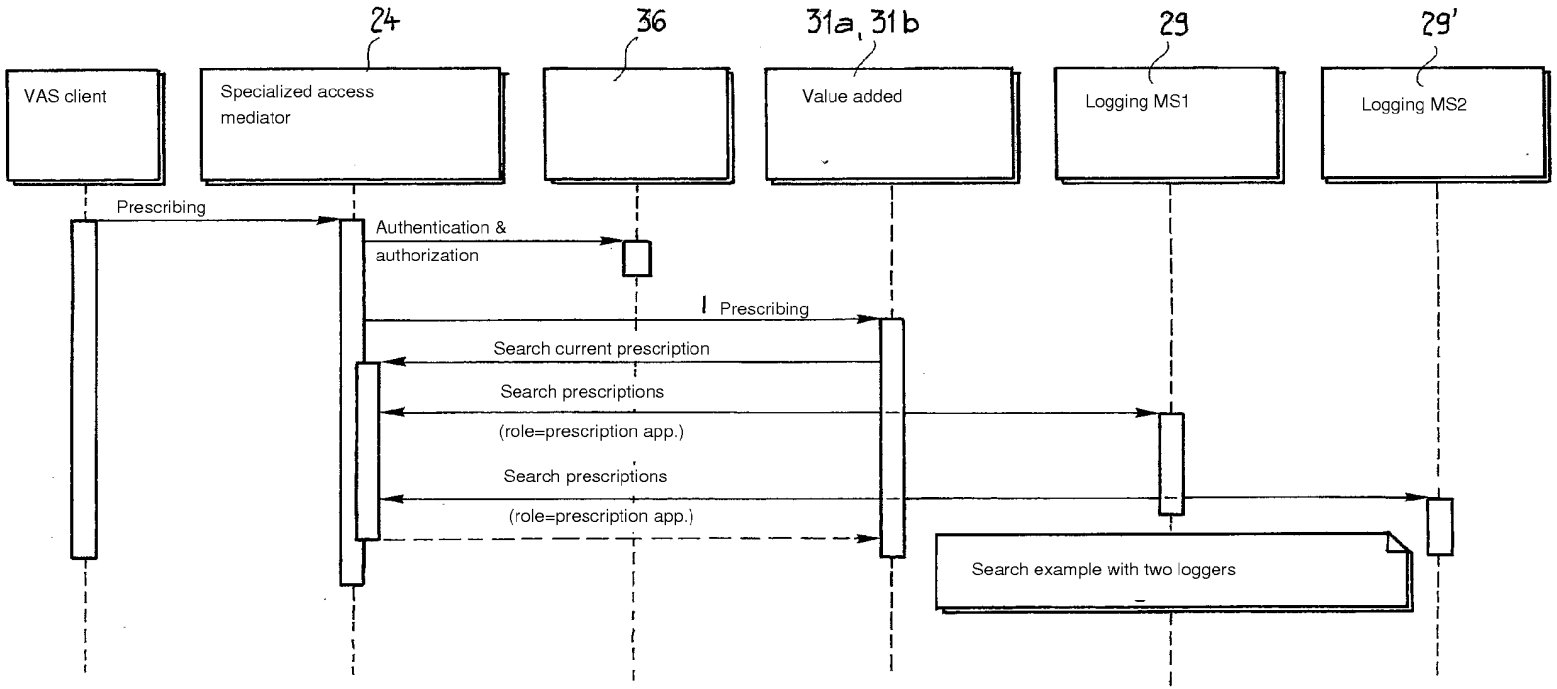
24
36
31a, 31b
29
29'
VAS client
Specialized access mediator
Value added
Logging MS1
Logging MS2
Prescribing
Authentication & authorization
1 Prescribing
Search current prescription
Search prescriptions
(role=prescription app.)
Search prescriptions
(role=prescription app.)
Search example with two loggers

Fig.13