Authorisation & Security aspects in the Middleware-based healthcare information system

Jose Andany[1] - Christer Bjorkendal[2] - Fabrizio Massimo Ferrara[3]
Jean-Raoul Scherrer[4] - Stéphane Spahni[1]

[1] *Medical informatics division, University Hospitals of Geneva, 24 rue Micheli-du-Crest, 1211 Geneva 14, Switzerland*

[2] Enator Medical, Margaretavagen 1, 22100 SE, Lund, Sweden

[3] GESI Gestione Sistemi per l'Informatica srl & Consorzio EDITH - Via Rodi, 32 - 00195 Roma, Italy

[4] Health On the Net foundation, Medical informatics division, University Hospitals of Geneva, 24 rue Micheli-du-Crest, 1211 Geneva 14, Switzerland

Abstract: The integration and evolution of existing systems represents one of the most urgent priorities of health care information systems in order to allow the whole organisation to meet the increasing clinical organisational and managerial needs. The CEN ENV 12967-1 'Healthcare Information Systems Architecture'(HISA) standard defines an architectural approach based on a middleware of business-specific common services, enabling all parts of the local and geographical system to operate on the common information heritage of the organisation and on exploiting a set of common business-oriented functionality.

After an overview on the key aspects of HISA, this paper discusses the positioning of the authorisation and security aspects in the overall architecture. A global security framework is finally proposed.

1 THE MIDDLEWARE-BASED ARCHITECTURAL APPROACH

Figure 1 shows the layered structure formalised by the CEN ENV 12967-1 standard 'Healthcare Information Systems architecture'.

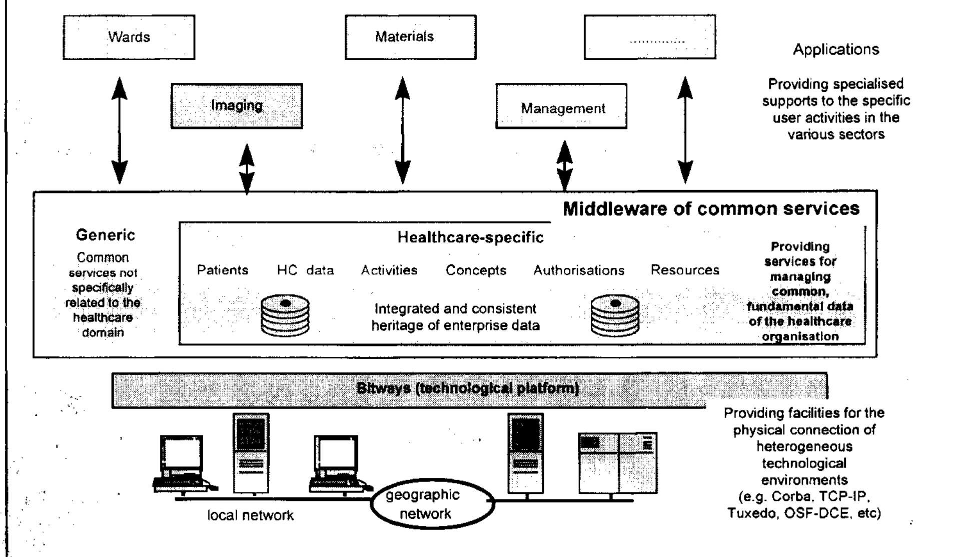
Wards
Materials
....
Applications
Imaging
Management
Providing specialised supports to the specific user activities in the various sectors
Middleware of common services
Generic
Common services not specifically related to the healthcare domain
Healthcare-specific
Patients
HC data
Activities
Concepts
Authorisations
Resources
Integrated and consistent heritage of enterprise data
Providing services for managing common, fundamental data of the healthcare organisation
Bitways (technological platform)
Providing facilities for the physical connection of heterogeneous technological environments (e.g. Corba, TCP-IP, Tuxedo, OSF-DCE, etc)
local network
geographic network

Figure 1. The 3-layers structure of the CEN architecture of health care information systems

- *The Applications* layer consists of a set of components responsible for interacting with the users, providing a specialised support to the various activities carried out in the various sectors of the health care organisation.
- *The Middleware* layer provides a set of services which support the whole system with respect to the management of those common data and procedures of paramount relevance for the whole organisation..
- *The Bitways* layer represents the technological platform, providing facilities enabling the various modules of the information system to interact through common mechanisms, hiding the diverse technologies adopted for their implementation and the mutual location over the (distributed) environment.

Through its services for the definition and management of the information common to the whole organisation, the middleware represents both the key element for ensuring the openness and modularity of the information system, and an operational infrastructure suitable for the integration of legacy systems and for the development of new modules.

By extending the scope of its services, also specific business procedures (e.g. admitting patients, making requests for services, managing complete healthcare records, etc.) may become common facilities of the information system, directly exploitable by the various applications with major benefits in terms of overall consistency and reduction of development/maintenance costs.

2 AUTHORISATION VS. SECURITY

The term 'security' is frequently used to generically refer to all aspects relating to the identification, authorisation and validation of one agent (either individual or software process) in the information system. Approaching them all together in one unique term (or component of the information system) is risky with respect to the final results. An incremental methodological approach -as recommended by the Open Distributed Processing (ODP) and HISA- based on different levels of abstraction is therefore beneficial for simplifying the whole matter.

We can first of all identify a set of requirements related to how the individual users carry on their daily activities. Such aspects formalise the rules according to which each user is authorised to perform certain tasks (e.g. registering a diagnosis), as well as to access / manipulate certain data, both clinical and administrative (e.g. the results of some laboratory tests for one patient, the salary of other employees, etc.). Such issues are completely independent from any technological or implementation aspect of the system; they just relate to the organisation and to the laws and procedures which are in force in that place or country. The identification of a clear and common set of terms of reference on how to formalise and manage such aspects represents thus a fundamental pre-requisite for any implementation initiative. This set of requirements and the formalisation of a comprehensive, technological independent, framework for their description and management can be more properly referred to with the term '*Authorisation*'.

A *different* (but complementary) set of requirements relates to the secure authentication of the agents (i.e. individuals and software processes) performing the tasks, to the reliable communication of information between two agents and to the archiving of information according to legal and ethical requirements. This set of aspects will be referred to with the term '*Security*'.

In the three-layer model of the HISA architecture, different classes of services (and of components) are responsible for the Authorisation and for the Security aspects. The formalisation of the model and the management of the information related to the authorisation rules and criteria is under the responsibility of the healthcare-specific services of the middleware. The mechanisms, tools and technologies according to which the security requirements are implemented are under the responsibility of the 'bitways' layer of the architecture. Obviously, generic services are employed by the middleware and by the applications to operate according to the security requirements imposed in the specific organisation.

It may be stressed that, while a generic model and a common set of services can be identified for the management of the authorisation aspects throughout all information systems, it is very difficult to define a unique and standard set of security technologies to be implemented in all healthcare information systems of all European countries due to the diversities in the rules, budget, cultural characteristics of the various organisations,. Moreover, the rapid evolution of the techniques should be taken in account. An open environment, therefore, should conform to the following fundamental rules:

- To provide a common framework and a common set of services for allowing all applications and components to retrieve the authorisation aspects of the organisation and to operate accordingly;
- To foresee a set of 'sockets' in the physical implementation, allowing to simply plug-in additional components and services responsible for providing specific security features.

3 AUTHORISATION ASPECTS IN HISA AND IN THE DHE

3.1 CURRENT FEATURES OF HISA

Besides the need for supporting the diversification of roles and responsibilities, additional critical aspects can be identified in the healthcare scenario due to the particular type of information which is managed, implying also ethical and legal aspects. Moreover, moving from country to country or from one healthcare centre to another, different levels of authorisation may be applied to similar types of users.

The Authorisation Common Services in the middleware layer of HISA aim at supporting this specific need, by providing:

- a comprehensive and consistent repository where those responsible in the organisation may define the rules according to which the users may execute the functions provided by the system;
- a standard mechanism according to which the rest of the system may check whether one user is allowed to perform the activities they are requesting.

Each component may be described in terms of a set of controlled functionalities, whose invocation and manipulation by external agents is subject to specific authorisations. For each component, a set of authorisation profiles are defined, usually reflecting the jobs and responsibilities in the organisational area where the system is operating. Each profile may operate with a set of functionalities, according to one set of conditions such as:

- the working ways, which define whether the profile is allowed to access that element by adding new data or reading, updating, or deleting existing data;
- the time frame, which permits the specification of the temporal limits of the authorisation, through a start and end time every day;
- the workstations, which specify a list of workstations or nodes of the information system from which the agent is allowed to interact with the object.

Data being maintained through these services is schematised in Figure 2.

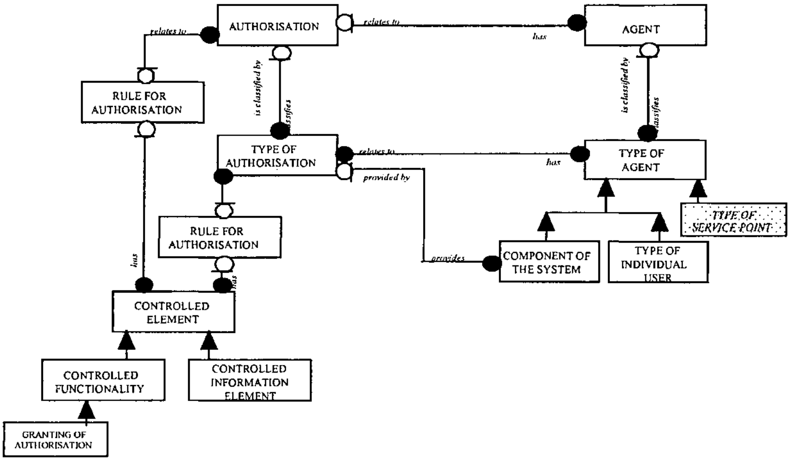

Figure 2: The Data model of the middleware Authorisation Common services

An *Agent* is an individual user or a software component authorised to interact with the information system, while the *Controlled element* represents an element for which authorisation mechanisms are defined. The general procedures according to which the agents may operate are formalised through the '*Type of Authorisation*' and the '*Rules for Authorisation*'. Each agent inherits the authorisations defined for his/her class (i.e. type of agent). Should some particular cases occur (e.g. vacancy, temporary substitution, etc.) individual authorisations overriding the generic values may be formalised. The HISA implementation "Distributed Healthcare Environment"(DHE) fully implements such model.

3.2 ENVISAGEABLE EXTENSIONS TO THE STANDARD

The need for a homogeneous set of components, supporting the specific need for authorisation has dramatically increased during the last decade. The development has changed from proprietary legacy systems, usually running on mainframes to distributed applications running in local environments. A common situation today is that a hospital is supported by different vendors providing different applications not able to fully communicate one with each other.

If on the other hand we look on authorisations from the health care organisation point of view we need to have a flexible model due to the fact that organisations change constantly and that a user could adopt different roles. The combination of user and role is time related which means that when working nightshift, the user may have one authorisation profile but when working dayshift another one is used.

Another most important issue today is how to improve the quality of care by using IT without interfering with respect of the patient privacy. To let the physicians have more adequate information on the patient you need to have something like a "virtual electronic health care record", able to keep track of all the activities belonging to one patient regardless of where and by whom they have been performed. With such approach we need to have a kind of generic model for authorisation in order to specify a unique global authorisation that can be executed on different organisations. The authorisation model, which already exist in the specification of HISA, needs to be extended to have a more accurate control, adapted to its purpose.

Based on the conceptual model for security and authorisation described in HISA three components, integrated in the DHE, are planned or under construction. These should be seen as middleware components with open interfaces as shown in figure 3.

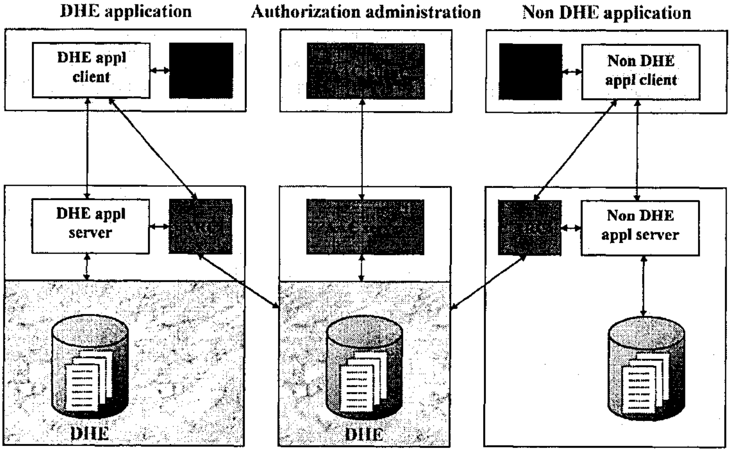

Figure 3: The authorisation components

- *Authorisation Administration Component* (AAC) is a client-server module for the authorisations administration.
- *Authorisation Runtime Component* (ARC) provides a client or a server component with the users authorisations in a standard structured record.
- *Login and Session Component* (LSC) provides the ability of sharing a common session between different applications for different environment.

Two additional components are also provided:

- *Authorisation eXchange Component* (AXC) provides facilities for import/export authorisations data to / from some other system in a standardised XML format.
- *Dynamic Authorisation Rules Component* (DARC) generates automatically authorisation depending on certain rules and regulations.

The need for restrictive authorisation is going to dramatically increase over the next couple of years as the physicians demand more and more patient related information. From the European market point of view there is already today a defined need for such functionality, especially from the Nordic countries but also for the European market in general. Therefor we consider these components most valuable for the European Health Care Sectors.

4 Security issues

In the physical implementation of the DHE, several security features are implemented, as it is briefly schematised in the following.

- *Encryption/decryption* modules based on private and public keys may be activated on both the client and the server side.
- *Digital signature* may be added when validating or entering health data. A function can validate the authenticity of the signature.
- *Certification* of the user activities is provided for auditing and/or legal purposes as a log of all interactions occurred which is signed and encrypted by the user.

Those features could collaborate together with the authorisations in an extension of HISA based on the following security principles:

- *The secure extranet principle* specifies that the treatment of a user request cannot be affected by any other system than those handling the request. It implies that the systems implied have to be securely authenticated and are the only that can access the key to exploit the information.
- *The systematic computation of the authorisation rules* certifies that *any* request addressed to *any* of its services is validated according to the actual authorisation rules before being processed.
- *The a posteriori proof* is able to provide the necessary information to verify that the above principles have been respected within the execution of any of the received requests.

Those principles can be implemented within the standard architecture as in figure 4.

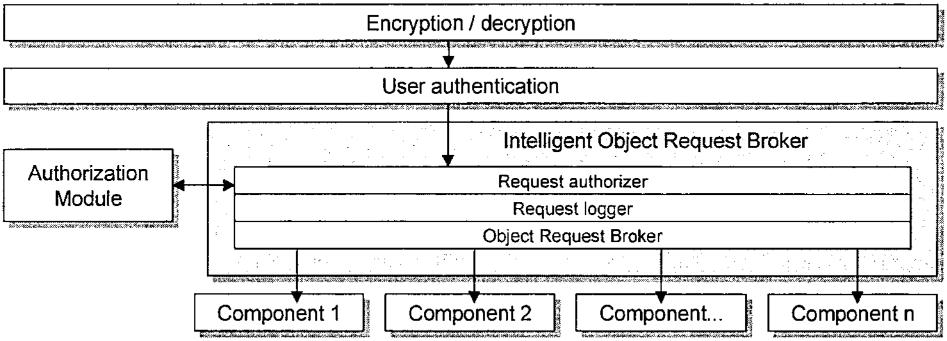

Figure 4: The security architecture

In this approach the broker guaranties to each component that any request it receives is authorised and logged in accordance to the organisation security rules. The information carried by the extranet is encrypted and the user is clearly authenticated. Only the request authoriser, logger and /or the authorisation modules have to be customised according to the rules of a specific organisation.

In such architecture, the universality of the middleware's components is easier to reach. The framework for the collaboration between these new components and the existing ones is clearly defined in order to reduce their interdependency and the service duplication. The three proposed services can be considered as generic components as their behaviour is independent of a specific business area such as health care.

REFERENCES

[1] CEN/TC251 ENV 12967-1 'Health care Information Systems Architecture'

[2] CEN/TC251 ENV12265 'Electronic Health care Record Architecture'

[3] The DHE middleware: - Information view, Functional view and API's – SPRI 1998

[4] S. Spahni - J.R. Scherrer - D. Sauquet - P.A. Sottile. 'Consensual trends for optimising the constitution of middleware', SYNAPSES project, Telematics Application Programme of the Commission of the European Communities, project No. HC1046 published in SIGCOMM Computer Communication Review, vol–28, no 5, 1998, pp 76-90.