TECHNICAL SPECIFICATION

ISO/TS 22600-2

First edition
2006-08-01

Health informatics — Privilege management and access control —

Part 2: Formal models

Informatique de santé — Gestion de privilèges et contrôle d'accès —

Partie 2: Modèles formels

Reference number
ISO/TS 22600-2:2006(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Terms and definitions 2

3 Abbreviations 6

4 Component paradigm 6

5 Generic models 7
5.1 Framework 7
5.2 Domain model 8
5.3 Document model 10
5.4 Policy model 10
5.5 Role model 13
5.6 Authorization model — Role and privilege assignment 14
5.7 Control model 14
5.8 Delegation model 15
5.9 Access control model 17

Annex A (informative) Functional and structural roles 19

Annex B (informative) Example of structural roles in healthcare 24

Bibliography 26

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 22600-2 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

ISO/TS 22600 consists of the following parts, under the general title *Health informatics — Privilege management and access control*:

— *Part 1: Overview and policy management*

— *Part 2: Formal models*

Introduction

A common situation today is that hospitals are supported by several vendors providing different applications, who are not able to communicate authentication and authorization since each has its own way of handling these functions. To achieve an integrated scenario one has to spend a huge amount of money to get users and organizational information mapped before starting communication. Resources are required for development and maintenance of security functions that grow exponentially with the number of applications.

If, on the other hand, one looks on authorization from the health care organization's point of view, we need a flexible bridging model due to the fact that organizations change continuously. Units close down, open and merge.

The situation becomes even more complex when communications across security policy domain boundaries are necessary. The policy differences between these domains then have to be bridged through *policy agreements* between the parties.

Another complexity is found in roles when it comes to users. A user can adopt different roles related to different periods of time and even have two or more roles simultaneously. For example, a user may work as a nurse for two months and as a midwife for the next two or have both roles within the same time period.

Moreover, different responsibilities can be identified in the healthcare organization depending on the role and activities of the users. Moving from country to country or from one healthcare centre to another, different types or levels of authorization may be applied to similar types of user, both for execution of particular functions and for access to the information.

Another most important issue today is how to improve the quality of care by using IT, without infringing the privacy of the patient. To allow physicians to have more adequate information about the patient you need to have something like a ‘virtual electronic health care record’ which makes it possible to keep track of all the activities belonging to one patient regardless of where and by whom they have been documented. With such an approach we need to have a generic model or specific agreement between the parties for authorization.

Besides the needs for support of a diversity of roles and responsibilities, which are typical in any type of large organization, additional critical aspects can be identified such as ethical and legal aspects in the healthcare scenario due to the particular type of information that is managed.

The need for restrictive authorization is already high today but is going to dramatically increase over the next two years. The reason is the increase of exchange of information between applications in order to fulfil the physicians’ demands on having access to more and more patient-related information to ensure the quality and efficiency of patient treatment.

The situation, with respect to health care and its communication and application security services has changed during the last decade. Reasons are, for example:

— moving from mainframe based proprietary legacy systems to distributed systems running in local environments;

— more data are stored in information systems and are therefore also more valuable to the users;

— patients are more ambulant and in need of their medical information at different locations.

From this it follows that advanced security is required in communication and use of health information due to the sensitivity of person-related information and its corresponding personal and social impact. Those security services concern both communication and application security. Regarding communication security services, such as authentication, integrity, confidentiality, availability, accountability (including traceability and non-repudiation), control of access to entities as well as notary's services, it is authentication that is of crucial importance for most of the other services. This is also true for application security such as access control to data and functions of applications running at the aforementioned entity, integrity, confidentiality, availability, accountability, audibility and the notary's services.

The implementation of this Technical Specification will be very complex since the involved parties will already have systems in operation and will not be willing to update their system immediately to newer versions or new systems. It is therefore very important that a policy agreement is written between the parties, which states that they intend to progress towards this standard when any change in the systems is intended.

The policy agreement shall also contain defined differences in the security systems and agreed solutions on how to overcome the differences. For example, the authentication service, rights and duties of a requesting party at the responding site have to be managed according to the agreed policy written down in the agreement. For that reason, information and service requester, as well as information and service provider on the one hand, and information and services requested and provided on the other hand, have to be grouped and classified properly. Based on that classification, claimant mechanisms, target sensitivity mechanisms and policy specification and management mechanisms, can be implemented. Once all parties have underwritten the policy agreement the communication and information exchange can start with the existing systems if the parties do not see any risks. If there are risks which are of such importance that they have to be eliminated before the information exchange starts they shall also be recorded in the policy agreement together with an action plan for how these risks shall be removed. The policy agreement shall also contain a time plan for this work and an agreement on how it shall be financed.

The documentation process is very important and provides the platform for the policy agreement.

- Part 1: Overview and policy management, describes the scenarios and the critical parameters in cross border information exchange. It also gives examples of necessary documentation methods as the basis for the policy agreement.

- Part 2: Formal models, describes and explains, in a more detailed manner, the architectures and underlying models for the privileges and privilege management, which are necessary for secure information sharing plus examples of policy agreement templates.

Privilege management and access control address security services required for communication and distributed use of health information. This document introduces principles and specifies services needed for managing privileges and access control. Cryptographic protocols are out of the scope of this document.

This part of ISO/TS 22600 is strongly related to other corresponding International Standards such as ISO/TS 17090 and ISO/TS 21091. It is also related to work in progress on a future Technical Specification, ISO/TS 21298.

This part of ISO/TS 22600 is meant to be read in conjunction with its complete set of associated standards.

The distributed architecture of shared care information systems is increasingly based on networks. Due to their user friendliness, the use of standardized user interfaces, tools and protocols, and therefore their platform independence, the number of really open information systems based on corporate networks, virtual private networks has been rapidly growing during the last couple of years.

ISO/TS 22600 shall define privilege management and access control services required for communication and use of distributed health information over domain and security borders. The document introduces principles and specifies services needed for managing privileges and access control. It specifies the necessary component based concepts and is intended to support their technical implementation. It will not specify the use of these concepts in particular clinical process pathways.

Health informatics — Privilege management and access control —

Part 2: Formal models

1 Scope

This part of ISO/TS 22600 is intended to support the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners. It is also intended to support inquiries from both individuals and application systems.

ISO/TS 22600 defines methods for managing authorization and access control to data and/or functions. It accommodates policy bridging. It is based on a conceptual model where local authorization servers and cross-border directory and policy repository services can assist access control in various applications (software components). The policy repository provides information on rules for access to various application functions based on roles and other attributes. The directory service enables identification of the individual user. The granted access will be based on four aspects:

— the authenticated identification of the user;

— the rules for access connected with a specific information object;

— the rules regarding authorization attributes linked to the user provided by the authorization manager;

— the functions of the specific application.

This part of ISO/TS 22600 should be used in a perspective ranging from a local situation to a regional or national one. One of the key points in these perspectives is to have organizational criteria combined with authorization profiles agreed upon from both the requesting and delivering side in a written policy agreement.

This part of ISO/TS 22600 supports collaboration between several authorization managers that may operate over organizational and policy borders.

The collaboration is defined in a policy agreement, signed by all involved organizations, and constitutes the basic platform for the operation.

A documentation format is proposed, as a platform for the policy agreement, which makes it possible to obtain comparable documentation from all parties involved in the information exchange of information.

This part of ISO/TS 22600 excludes platform-specific and implementation details. It does not specify technical communication security services and protocols that have been established in other standards, e.g. ENV 13608. It also excludes authentication techniques.

This part of ISO/TS 22600 introduces the underlying paradigm of formal high level models for architectural components based on ISO/IEC 10746. In that context, the Domain Model, the Document Model, the Policy Model, the Role Model, the Authorization Model, the Delegation Model, the Control Model and the Access Control Model are introduced.

The specifications are provided using the meta-languages Unified Modelling Language (UML) and Extensible Markup Language (XML). Additional diagrams are used for explaining the principles. The attributes used have been referenced to the HL7 Reference Information Model and the HL7 datatype definitions.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[ISO/IEC 2382-8, definition 08.04.01]

2.2
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2, definition 3.3.3]

2.3
attribute authority
AA
authority that assigns privileges by issuing attribute certificates

2.4
attribute certificate
data structure, digitally signed by an attribute authority, which binds some attribute values with identification about its holder

2.5
authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

NOTE See also data origin authentication and peer entity authentication.

2.6
authority
entity that is responsible for the issuance of certificates

NOTE Two types are defined in this part of ISO/TS 22600: certification authority that issues public-key certificates and attribute authority that issues attribute certificates.

2.7
authorization
process of granting rights, which includes the granting of access rights

2.8
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2, definition 3.3.17]

2.9
certificate validation
process of ensuring that a certificate was valid at a given time, including possibly the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e. were not expired or revoked) at that given time

2.10
certification authority
CA
authority trusted by one or more relying parties to create and assign certificates

[ISO/IEC 9594-8, definition 3.3.17]

NOTE 1 Optionally the certification authority may create the relying parties' keys.

NOTE 2 Authority in the CA term does not imply any government authorization only that it is trusted. Certificate issuer may be a better term but CA is used very broadly.

2.11
certification path
ordered sequence of certificates of objects in the DIT which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path

2.12
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO 7498-2, definition 3.3.16]

2.13
credential
prerequisite for the entitlement of, or the eligibility for, a role

2.14
delegation
conveyance of privilege from one entity that holds such privilege, to another entity

2.15
delegation path
ordered sequence of certificates which, together with authentication of a privilege asserter's identity, can be processed to verify the authenticity of a privilege asserter's privilege

2.16
environmental variables
aspects of policy required for an authorization decision, which are not contained within static structures, but are available through some local means to a privilege verifier (e.g. time of day or current account balance)

2.17
identification
performance of tests to enable a data processing system to recognize entities

2.18
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[ENV 13608-1]

2.19
integrity
property that information is not altered in any way, deliberately or accidentally

2.20
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2, definition 3.3.32]

2.21
non-repudiation
service that provides proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party

2.22
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

2.23
policy agreement
written agreement where all involved parties commit themselves to a specified set of policies

2.24
principal
actor able to realize specific scenarios (user, organization, system, device, application, component, object)

2.25
private key
key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)

[ISO/IEC 10181-1, definition 3.3.10]

2.26
privilege
capacity assigned to an entity by an authority according to the entity's attribute

2.27
privilege asserter
privilege holder using their attribute certificate or public-key certificate to assert privilege

2.28
privilege management infrastructure
PMI
infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a Public Key Infrastructure

2.29
privilege policy
policy that outlines conditions for privilege verifiers to provide/perform sensitive services to/for qualified privilege asserters

NOTE Privilege policy relates attributes associated with the service as well as attributes associated with privilege asserters.

2.30
privilege verifier
entity verifying certificates against a privilege policy

2.31
public key
key that is used with an asymmetric cryptographic algorithm and that can be made publicly available

[ISO/IEC 10181-1, definition 3.3.11]

2.32

public key certificate

PKC

certificate that binds an identity and a public key

NOTE The identity may be used to support identity-based access control decisions after the client proves that they have access to the private key that corresponds to the public key contained in the PKC.

2.33

role

set of competences and/or performances which is associated with a task

2.34

role assignment certificate

certificate that contains the role attribute, assigning one or more roles to the certificate holder

2.35

role certificate

certificate that assigns privileges to a role rather than directly to individuals

NOTE Individuals assigned to that role, through an attribute certificate or public-key certificate with a subject directory attributes extension containing that assignment, are indirectly assigned the privileges contained in the role certificate.

2.36

role specification certificate

certificate that contains the assignment of privileges to a role

2.37

sensitivity

characteristic of a resource that implies its value or importance

2.38

security

combination of availability, confidentiality, integrity and accountability

[ENV 13608-1]

2.39

security policy

plan or course of action adopted for providing computer security

2.40

security service

service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[ISO 7498-2, definition 3.3.51]

2.41

source of authority

SOA

attribute authority (2.3) that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges

2.42

target

resource being accessed by a claimant

NOTE Its sensitivity is modelled in this document as a collection of attributes, represented as either ASN.1 attributes or XML elements.

2.43
trust
quality by which an entity can be said to “trust” a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects

NOTE This trust may apply only for some specific function. The key role of trust in this framework is to describe the relationship between an authenticating entity and an authority; an entity should be certain that it can trust the authority to create only valid and reliable certificates.

3 Abbreviations

AA	Attribute Authority
PKC	Public Key Certificate
UML	Unified Modelling Language
XML	eXtensible Markup Language

4 Component paradigm

The framework for a future-proof health information system architecture is based on the generic component model developed in the mid-nineties (e.g. references [1], [2], [3]). Basis of that architecture are a reference information model (RIM) and agreed vocabularies enabling interoperability. Referenced to them, domain-specific constraint models will be specified which represent domain-specific knowledge concepts, considering both structural and functional knowledge. The corresponding components have to be established according to all views of the reference model in ISO 10746-1 on open distributed processing (RM-ODP), i.e. enterprise view, information view, computational view, engineering view and technology view. A view focuses consideration on one aspect abstracting from all others. The different domain concepts and their view representation is not the task of programmers but of domain experts. For that reason, they will use appropriate expression means such as specific graphical representation (e.g. UML diagrams) or sometimes even verbal templates expressed in XML.

The components can be aggregated to higher level of composition. Contrary to the ISO definition of primitives and composition, in the generic component model at least four levels of composition/decomposition have been defined (see Figure 1).

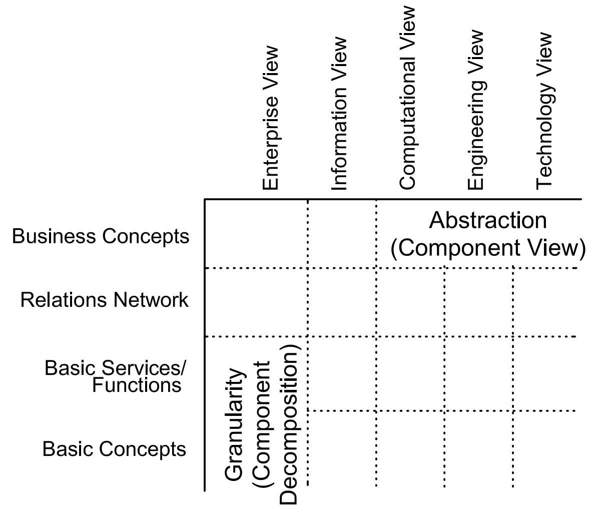


Figure 1 — Generic component model

The aggregation is performed according to content- or process-related knowledge expressed by logics/algorithms/operations or rules/workflows/procedures/relationships. So, the aggregation of the building blocks “constraint models” is controlled by the aforementioned mechanisms or by the communicating or co-operating principal’s behaviour. The specification is completely provided at meta-level. Different vocabularies as well as tooling environment and functionality are harmonized by meta-languages like XML Metadata Interchange (XMI)[4].

5 Generic models

5.1 Framework

Privilege management and authorization may be based on roles that individual actors or groups of individual actors play. Actors interacting with system components are called principals, which can be a human user, a system, a device, an application, a component or even an object.

In order to obtain the above described structure and functionality there are a number of models, mechanisms, processes, objects, etc. needed, which must be considered.

Regarding privilege management and access control management, two basic class types must be dealt with:

- entities:
  - documents;
  - principals;
  - policies;
  - roles;
- acts:
  - policy management;
  - principal management;
  - privilege management;
  - authentication;
  - authorization;
  - access control management;
  - audit.

The following models will be considered in more detail:

- domain model;
- document model;
- policy model;
- role model;
- authorization model;

- control model;
- delegation model;
- access control model.

All specifications in this framework will be kept open, platform-independent, portable and scalable. Therefore, the models provided are described at meta-model level and at the model level keeping the instance level out of consideration. For expressing systems in such a way, specific languages and meta-languages are used such as UML and XML including means for transfer from one vocabulary to another one.

This specification is defined using UML constructs, UML specifications, UML profiles and all different diagrams. Regarding XML, several specifications within the XML standard set will be used.

All models being used establish specific kinds of constraints forming constraint models. This concerns all conceivable services or views on systems. A model is a simplified view at the reality according to special concepts. The language to be used for graphical models is UML and MOF. The language for verbal models is the XML standard set.

It is expected that many documents will be expressed using XML. The structure for such a document is defined in a document type definition (DTD) or an XML schema instance. A privilege policy may act directly on the XML elements (e.g. by comparing attributes in an authorization certificate to elements in the document).

5.2 Domain model

To keep (complex) information systems that support shared care manageable and operating, principal-related components of the system are grouped by common organizational, logical and technical properties into domains. Following OMG's (Object Management Group) definition, this could be done for common policies (policy domains), for common environments (environment domains) or common technology (technology domains). Any kind of interoperability internal to a domain is called an intradomain communication and co-operation, whereas interoperability between domains is called an interdomain communication and co-operation. For example, communication could be realized between departments of a hospital internally to the domain hospital (intradomain communication), but externally to the domain of a special department (interdomain communication). Regarding security requirements, security policy domains are of special interest.

A domain is characterized by a domain identifier, a domain name, a domain authority, a domain qualifier. The provided data type definition resembles the HL7 Version 3 Data type Definition[5].

Table 1 — Security policy domain attributes

Attribute	Type	Remarks
domain_identifier	SET <OID>	SET of ISO ObjectIdentifier
domain_name	BAG <EN>	Bag of EntityName
domain_authority_ID	OID	ISO ObjectIdentifier
domain_authority_name	ST	String
domain_qualifier	CS	CodedSimpleValue

Security policy domain class inherits attributes from domain class, plus the attributes: policy identifier and policy name.

A policy describes the legal framework including rules and regulations, the organizational and administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties and penalties defined as well as the technological solution implemented for collecting, recording, processing and communicating data in information systems. For describing policies, methods such as policy templates or formal policy modelling might be deployed.

Domains are specified generically in this part of ISO/TS 22600, and their definition in practice can be flexible. A domain might consist of sub-domains (which will inherit and might specialize policies from the parent domain). The smallest-scale domain might be an individual workplace or a specific component within an information system. Domains can be extended into super-domains, by chaining a set of distinct domains and forming a common larger-scale domain for communication and co-operation.

This co-operation between domains requires the definition of a common set of policies that applies to all of the collaborating domains. It must be derived from all of the relevant domain-specific policies across all of those domains. These common policies are derived (negotiated) through a process known as policy bridging (see Figure 2). The eventual agreed policies need to be documented and signed by all of the domain authorities (see ISO/TS 22600-1:2006, Annex A). Ideally this whole process will be capable of electronic representation and negotiation, to permit real-time electronic collaboration to take place within a (pre-agreed) permitted and regulated framework. The policy negotiation or verification would then take place at every service interaction.

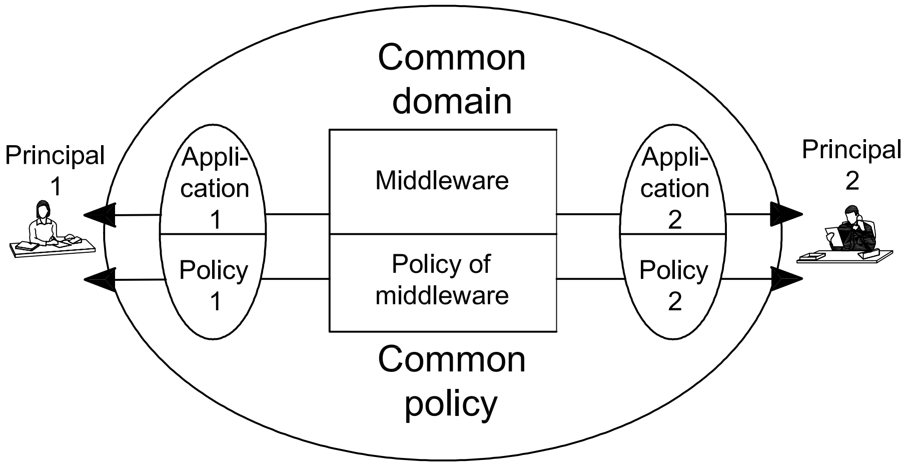


Figure 2 — Policy bridging

This collaboration will introduce the need for components between the principals. Middleware concepts are being introduced increasingly into the new(er) healthcare information systems. Middleware components can enable interoperability through direct invocation (middleware communication services) or chained invocation (including middleware application services). The latter is characterized by different models of delegation (see 5.8).

Such an architecture can be represented by chains of different domains as shown in Figure 3.

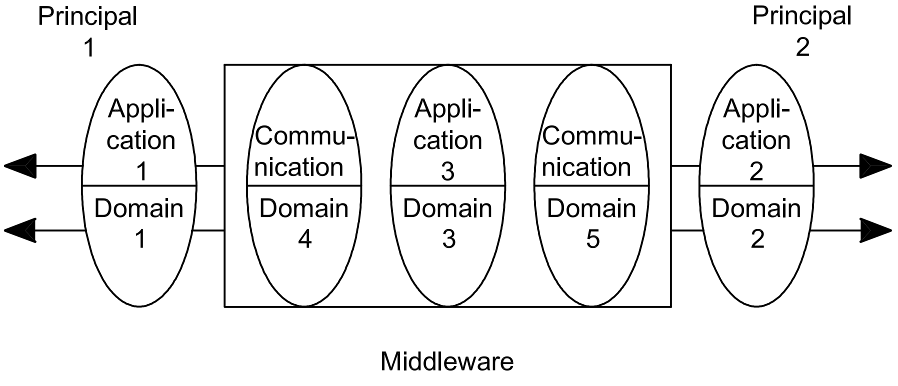


Figure 3 — Domain concept with middleware services

From the security point of view, a domain that ensures intradomain communication according to its own policy, is commonly considered to have need of protection only at its boundary, to external domains with their specific policies (or even the policy-free domain of the Internet). This is done by, e.g. firewalls, proxy servers, etc. Regarding the external environment, a domain is therefore often considered closed. The internal domain is mistakenly assumed to be secure, often neglecting internal threats and attacks which are among the majority of all security attacks.

Regarding the specific requirements and conditions of healthcare, the underlying security model must consider the whole spectre of security services and mechanisms, which can be accomplished by secure micro domains.

5.3 Document model

Processes, entities, roles, etc. must be documented and signed expressing the particular relations between entities and processes. The combination of processes and relations leads to multiple signatures (e.g. in the case of delegation).

This part of ISO/TS 22600 uses the cryptographic message syntax to support multiple signatures on a document. Each signature is computed over the document content and optionally a set of signed attributes specific to the particular signature. These attributes may include time stamps, signature purpose and other information.

5.4 Policy model

A security policy is the complex of legal, ethical, social, organizational, psychological, functional and technical implications for assuring trustworthiness of health information systems. A policy is the formulation of the concept of requirements and conditions for trustworthy creation, storage, processing and use of sensitive information. A policy can be expressed:

- verbally unstructured;
- structured using schemata or templates;
- formally modelled.

For interoperability reasons, a policy must be formulated and encoded in a way that enables its correct interpretation and practice. Therefore, policies have to be constrained regarding syntax, semantics, vocabulary and operation of policy documents, also called policy statements or policy agreements (agreements between the partners involved).

To reliably refer to a specific policy, the policy instance must be uniquely named and identified via a unique policy ID. The same is true for all the policy elements such as domain, targets, operations and their policies, which also have to be named and uniquely identified. In summary, a policy is characterized by a policy identifier, a policy name, a policy authority, a domain identifier, a domain name, a target list, target identifier, target name, target object, operations allowed and related policies.

For readability reasons, domain-related attributes have been included in Table 2 even if policy inherits from domain. The provided data type definition resembles the HL7 Version 3 Data type Definition.

Health information systems such as the EHR should at minimum have a policy for patients to control access to their health information, a policy with common access rules by the organization, policies defined by laws and regulations, and one policy per structural role as well as one policy per functional role.

Every creation, access or modification to an EHR component must be covered by one or more policies. The reference model of the EHR extract includes a policy ID attribute within the record component class to permit references to such policies to be made at any level of granularity within the EHR hierarchy. The policies that apply specifically to an EHR may be included within the EHR extract, eventually including any bridged policies.

As any other component, also policy components can be composed or decomposed according to the generic component model. Using H7 Version 3 data type definitions, the policy class can be specialized into basic policy, meta policy and composite policy (see Figure 4), which have been verbally explained in detail in Table 3 and Table 4 respectively. See reference [6].

Table 2 — Basic security policy attributes

Attribute	Type	Remarks
policy_identifier	SET <II>	Set of InstanceIdentifier
policy_name	CS	CodedSimpleValue
policy_authority_ID	OID	ISO ObjectIdentifier
policy_authority-name	ST	String
domain_identifier	SET <OID>	Set of ISO ObjectIdentifier
domain_name	BAG <EN>	Bag of EntityName
target_list	LIST <INT>	List of INT
target_ID	SET <II>	Set of InstanceIdentifier
target_name	EN	EntityName
target_object	II	InstanceIdentifier
operation_code	CE	CodedWithEqivalents
policies	CD	ConceptDescription

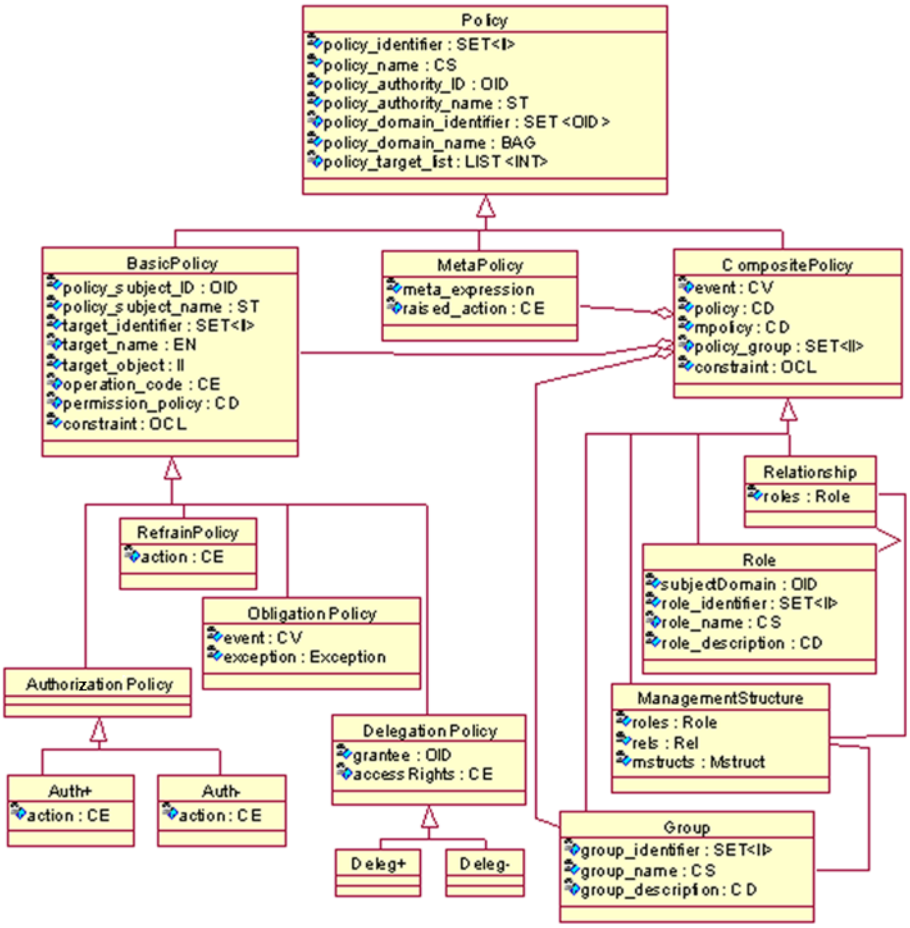


Figure 4 — Policy base-class diagram

The specializations of the composite policy abstract class are interrelated in a complex way, which has been indicated in outlines as simple association.

Table 3 — Basic policy types

Basic policy type	Purpose	Content
Authorization policies	define permitted actions	subject (except in roles), target, action
Obligation policies	are event-triggered and define actions to be performed by manager agents	subject (except in roles), action, event
Refrain policies	define actions the subjects must refrain from performing	subject (except in roles), action
Delegation policies	define what authorizations can be delegated to whom	

Table 4 — Composite policy types

Composite policy type	Purpose
Groups	define a scope for related policies to which a set of constraints can apply
Roles	define a group of policies (authorization, obligation and refrain policies) (for details on roles see 5.5 plus Annex A)
Relationships	define a group of policies pertaining to the interactions between a set of roles

Another way for policy decomposition has been provided by the OMG's security services specification distinguishing between the following policies:

- invocation access policy implementing access control policy for objects;
- invocation audit policy controlling event type and criteria for audit;
- secure invocation policy specifying security policies associated with security associations and message protection.

Regarding requirements for different object types:

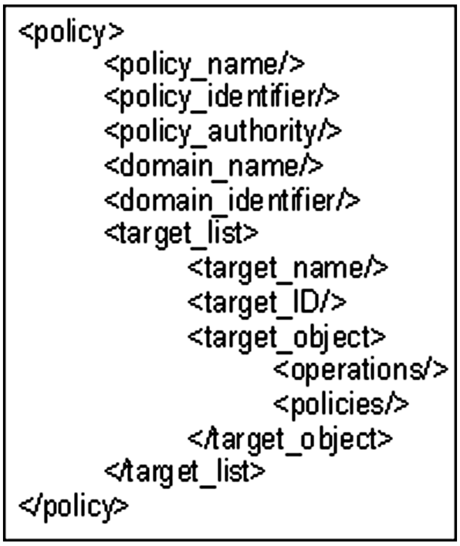
- invocation delegation policy;
- application access policy;
- application audit policy;
- non-repudiation policy

have been defined.

One common way to express constraints is the specification of user defined schemata such as XML schemata. This schema should be standardized for the interoperability purposes mentioned above.

Figure 5 presents a simple XML instance for a security policy statement.

Policies must be managed and stored in standardized trustworthy policy repositories.



```
<policy>
        <policy_name/>
        <policy_identifier/>
        <policy_authority/>
        <domain_name/>
        <domain_identifier/>
        <target_list>
                <target_name/>
                <target_ID/>
                <target_object>
                        <operations/>
                        <policies/>
                </target_object>
        </target_list>
</policy>
```

Figure 5 — Policy template example

5.5 Role model

For managing relationships between the entities mediated by an activity, two different roles must be defined: organizational roles at the entity's side and functional roles at the act's side.

To facilitate the deployment of ISO/TS 22600, functional and structural roles are presented in Annex A.

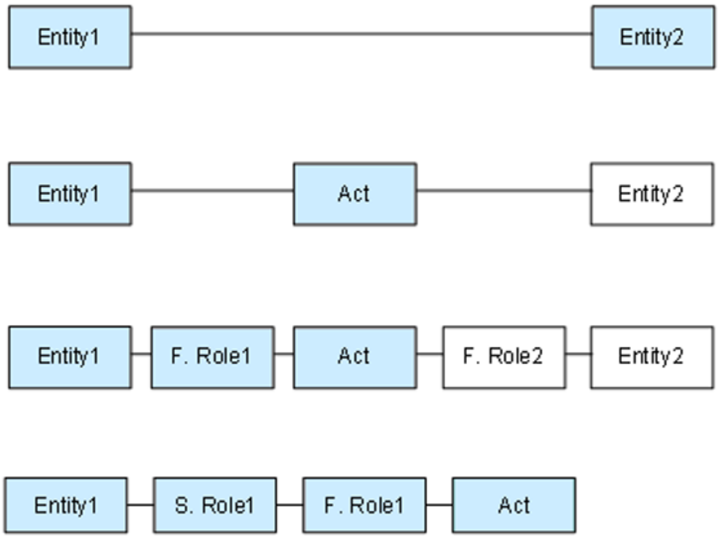


Figure 6 — The generic role concept

5.6 Authorization model — Role and privilege assignment

Credentialling, privileging and authorization are performed by connecting roles to policies.

Roles provide a means of indirectly assigning privileges to individuals. Individuals are issued role assignment certificates assigning one or more roles to them by role attributes. Privileges are assigned to a role by role specification certificates, rather than to individuals. The indirect assignment enables the privileges assigned to a role to be updated without impacting the certificates that assign roles to individuals. Role assignment certificates may be attribute certificates or public-key certificates. Role specification certificates cannot be public-key certificates, but must be attribute certificates. If role specification certificates are not used, the assignment of privileges to a role may be done through other means (e.g. may be locally configured at a privilege verifier).

The following scenarios are all possible:

- any number of roles can be defined by any attribute authority (AA);
- the role itself and the members of a role can be defined and administered separately, by different AAs; this implies that roles may be local within a domain, e.g. on an organizational, regional or national level;
- role membership, just as any other privilege, may be delegated;
- roles and membership may be assigned any suitable lifetime.

If the role assignment certificate is an attribute certificate, the **role** attribute is contained in the **attributes** component of the attribute certificate. If the role assignment certificate is a public-key certificate, the **role** attribute is contained in the **subjectDirectoryAttributes** extension. In the latter case, any additional privileges contained in the public-key certificate are privileges that are directly assigned to the certificate subject. Thus, a privilege asserter may present a role assignment certificate to the privilege verifier demonstrating only that the privilege asserter has a particular role (e.g., “manager”, or “purchaser”). The privilege verifier may know *a priori*, or may have to discover by some other means, the privileges associated with the asserted role in order to accept/reject/modify a request. The role specification certificate can be used for this purpose.

A privilege verifier must have an understanding of the privileges specified for the role. The assignment of those privileges to the role may be made within the privilege management infrastructure (PMI) by a role specification certificate or outside the PMI (e.g. locally configured). For role privileges asserted in a role specification certificate, mechanisms for linking that certificate with the relevant role assignment certificate for the privilege asserter are provided in this part of ISO/TS 22600. The issuer of the role assignment certificate may be different from the issuer of the role specification certificate and these certificates are administered (e.g. creation, expiration, revocation) entirely separately. The same certificate (attribute certificate or public-key certificate) can contain role assignment certificate as well as contain assignment of other privileges directly to the same individual. However, a role specification certificate must be a separate certificate.

NOTE The use of roles within an authorization framework can increase the complexity of path processing, because such functionality essentially defines another delegation path which must be followed. The delegation path for the role assignment certificate may involve different AAs and may be independent of the AA that issued the role specification certificate.

The general privilege management model consists of three entities: the object, the privilege asserter and the privilege verifier. Request may be authorized, denied or modified.

5.7 Control model

Access control is the process which determines whether a claimant’s privileges permit him/her/it to access a service provided by a target component. In this context, access is broader than acquiring some data. It might refer to any service offered by a target component (e.g. deletion, computation, transfer).

The control model illustrates how control is exerted over access to a sensitive object operation. There are four components in the model: the claimant, the verifier, the target and the control policy (see Figure 7).

The claimant has privilege attributes, contained in an attribute certificate. The target has sensitivity attributes, which may be contained in a security label, attribute certificate or in a local database. The techniques described here enable the verifier, who may be the owner of the target or an independent authority, to control access to the target by the claimant, in accordance with the control policy and optionally taking other environmental variables or components into account (e.g. local time).

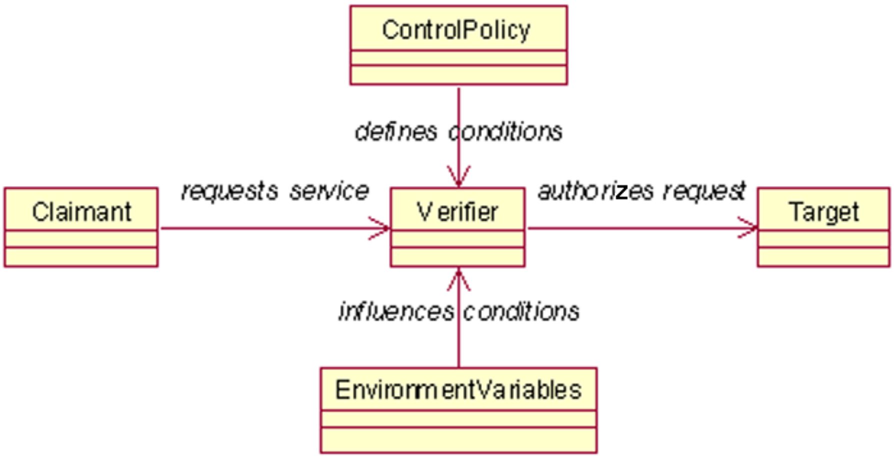


Figure 7 — Control model

The claimant's privileges are typically encapsulated in its attribute certificate. This may be presented to the verifier in the service request (push strategy), or it can be distributed by some other means, such as via a directory (pull strategy). The control policy must be protected for integrity and authenticity and, for this purpose, it may sometimes be combined with the claimant's privilege in an attribute certificate. Normally, however, it will be declared separately.

The claimant may be an entity identified by a public key certificate, or an executable object identified by the digest.

5.8 Delegation model

In addition to the control model, there is a need for a delegation model. There are three components of the delegation model: the verifier, the source of authority, and the claimant (see Figure 8).

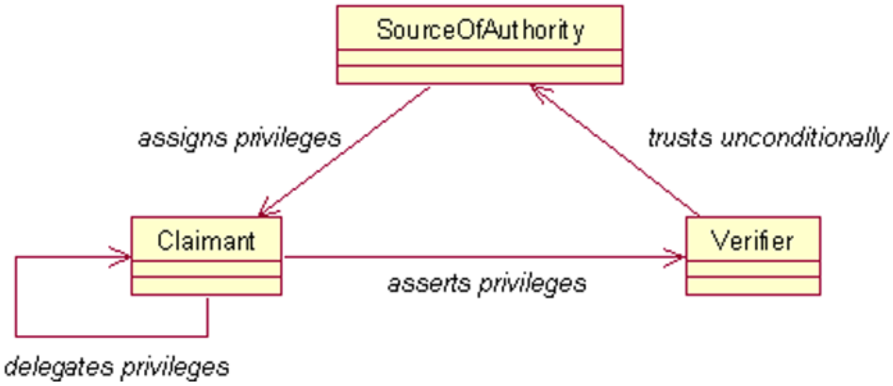


Figure 8 — Delegation model

The verifier endows an entity known as the source of authority with global privilege within the context a delegation occurs. The source of authority is an attribute authority. It delegates privilege to claimants by issuing attribute certificates. The claimant asserts its delegated privilege by demonstrating its identity. This can be done by proving its knowledge of a private key whose public counterpart is contained in a public key certificate referenced by an attribute certificate which includes the claimed privilege.

Optionally, the claimant may delegate its privilege to another claimant. The verifier must confirm that all entities in the delegation path possess sufficient privilege to access the target requested by the direct claimant.

The source of authority may also process a request from an entity to delegate its privilege by issuing an attribute certificate to another entity. However, this process is outside the scope of this part of ISO/TS 22600.

The claimant and the verifier may be entities in different security domains. In such cases, the source of authority may be located in the verifier's domain, and a continuous section of the delegation path, which includes the direct claimant, shall be in the other security domain.

The delegation path is distinct from the certificate validation path used to validate the public key certificates of the entities involved in the delegation process. However, the quality of authenticity offered by the public key certificate validation process must be commensurate with the sensitivity of the target being protected.

Specifying interoperability between distributed objects or components, the object management group has defined an alternative delegation model within its CORBA security services specification. In an object system, a client calls on an object to perform an operation, but this object will often not complete the operation itself, so it will call on other objects to do so. This will usually result in a chain of calls on other objects. (For further details see www.omg.org.)

In privilege delegation, the initiating principal's access control information (i.e., its security attributes) may be delegated to further objects in the chain to give the recipient the rights to act on its behalf under specified circumstances.

Another authorization scheme is reference restriction where the rights to use an object under specified circumstances are passed as part of the object reference to the recipient. Reference restriction is not included in this specification.

The following terms are used in describing OMG's delegation options:

— **Initiator** — the first client in a call chain.

— **Final target** — the final recipient in a call chain.

— **Intermediate** — an object in a call chain which is neither the initiator nor the final target.

— **Immediate invoker** — an object or client from which an object receives a call.

Communication of health information is frequently connected with a supplier chain performing this activity (e.g. involvement of secretaries, clerks, service departments, but also any other principals). This delegation model must be used for any such chaining of services. See Table 5.

Table 5 — Delegation schemes (OMG)

Intermediate performs	Target	Constraints
1. one method on one object		
2. several methods on one object		
3. any method on:	a. one object b. some object(s) c. any object	none target restrictions no target restrictions
	using no privileges	
	a subset of the initiator’s privileges	simple delegation
	both the initiator’s and its own privileges	composite delegation
	received privileges and its own privileges	combined or traced delegation, depending on whether privileges are combined or concatenated
	during some validity period	part of time constraints
	for a specified number of invocations	part of time constraints

5.9 Access control model

The use of roles can greatly simplify security administration. Additionally, administration constraints may need to be enforced. For example, the separation of duties may be introduced as a widely used authorization constraint.

Basic elements for access control management are principals, roles, permissions, operations and objects. The access control management is characterized by the following components:

- definition of roles and role constraints;
- user-role assignment;
- role-permission assignment;
- assignment of constraints for activation of user assigned roles.

Harmonizing the role models specified in 5.5 and Annex A, and advanced access control models such as the NIST standard role-based access Control, Figure 9 has been developed presenting an adapted role-based access control schema.

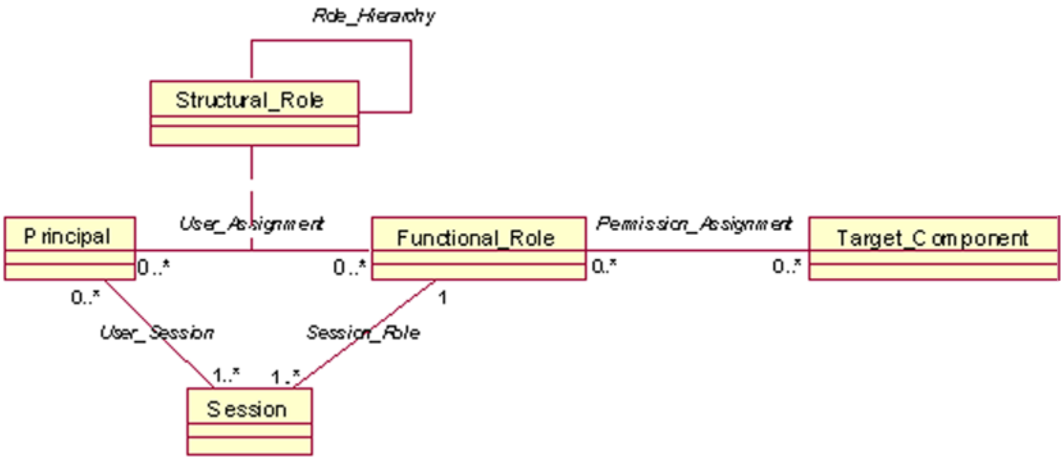


Figure 9 — Role-based access control schema

The RBAC schema defines the assignment of permissions dedicated to a functional role which has been assigned to a principal within a certain session. The functional role might be qualified by a set of structural roles assigned to the same principal.

Each model component is defined by the subcomponents:

— a set of basic element sets;

— a set of RBAC relations involving those element sets (containing subsets of Cartesian products denoting valid assignments);

— a set of mapping functions that yield instances of members from one element set for a given instance from another element set.

Annex A
(informative)

Functional and structural roles

A.1 Health care related roles

For managing relationships between the entities, roles may be assigned to any principal. Principals are the actors in healthcare, therefore, roles are associated with actors and with acts.

In general, two types of role can be distinguished: structural roles and functional roles. Structural roles reflect the structural aspects of relationships between entities. Structural roles describe prerequisites, feasibilities or competences for acts. Functional roles reflect functional aspects of relationships between entities. Functional roles are bound to the realization/performance of acts.

Considering both structural roles and functional roles in the same context, structural roles provide the prerequisites/competences for entities to perform interactions (an act) within their specific functional roles. Qualifications, skills, etc., influence both the assignment of the structural roles and the performance of activities according to their functional roles (Figure A.1).

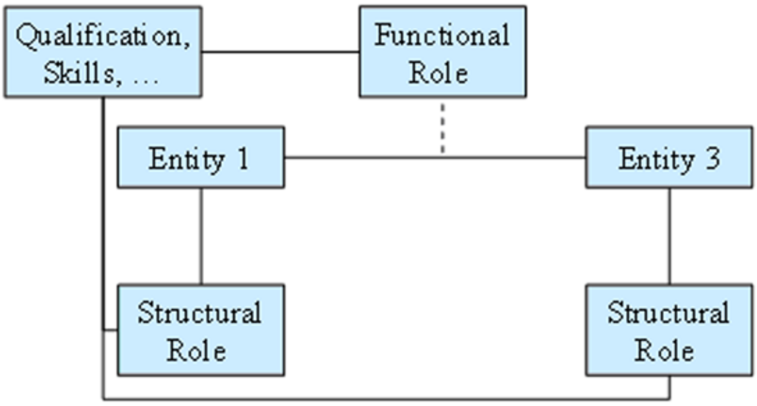


Figure A.1 — Generic role concept

Possible examples for structural roles of healthcare professionals are:

- medical director;
- director of clinic;
- head of the department;
- senior physician;
- resident physician;
- physician;
- medical assistant;

- trainee;
- head nurse;
- nurse;
- medical student.

Possible examples for functional roles of healthcare professionals are:

- caring doctor (responsible doctor);
- member of diagnostic team;
- member of therapeutic team;
- consulting doctor;
- admitting doctor;
- family doctor;
- function-specific nurse.

A.2 Functional role model

Regarding the healthcare business process, functional roles can be defined in levels of authorization and access right in the following generic way re-using slightly changed definitions established in the Australian HealthNet Project, cross-referenced against other works:

- subject of care (normally the patient);
- subject of care agent (parent, guardian, carer or other legal representative);
- responsible (personal) healthcare professional (the healthcare professional with the closest relationship to the patient, often his GP);
- privileged healthcare professional:
  - nominated by the subject of care;
  - nominated by the healthcare facility of care (there is a nomination by regulation, practice, etc.);
- healthcare professional (involved in providing direct care to the patient);
- health-related professional (indirectly involved in patient care, teaching, research, etc.);
- administrator (and any other parties supporting service provision to the patient).

This list fixes the set functional roles applied to manage the creation, access, processing and communication of health information.

Additionally, functional roles can be grouped according to the relation to the information created, recorded, entered, processed, stored, and communicated:

- composer;
- committer;
- certifier;
- authorizer;
- subject of information;
- information provider.

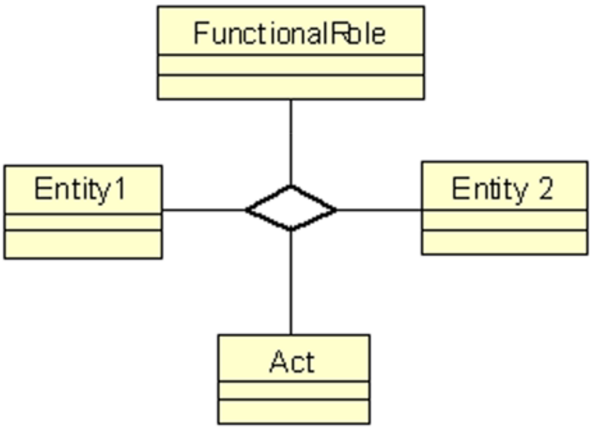


Figure A.2 — Functional role model

Expressing this in UML the many-to-many relationships between entities and acts can be transformed according to Figure A.3.

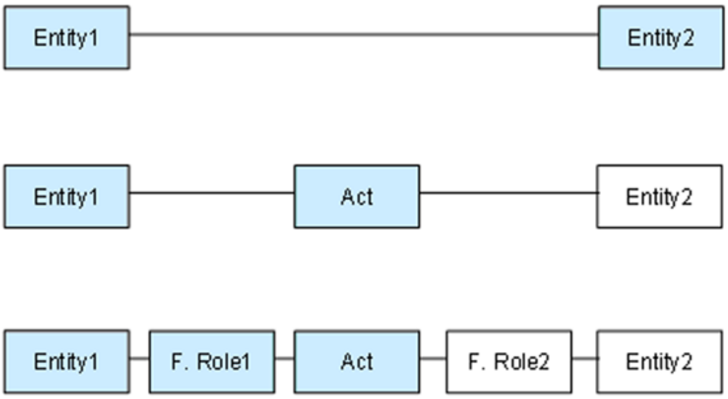


Figure A.3 — Development of the functional role model

A.3 Structural role model

An entity-entity relationship may concern a contracting act resulting in a contract between entities playing specific functional roles (see below). The contract could define the structural role of being, e.g. a head physician. Another example may concern an entity-entity relationship for education resulting in a special qualification as well as a certificate certifying this qualification as a structural role.

These structural role constraints cause another entity-entity relationship to influence the functional role played by the entities involved in an activity. The establishment of a structural role is provided within an act between entities according to specific act-related functional roles as shown in Figure A.4.

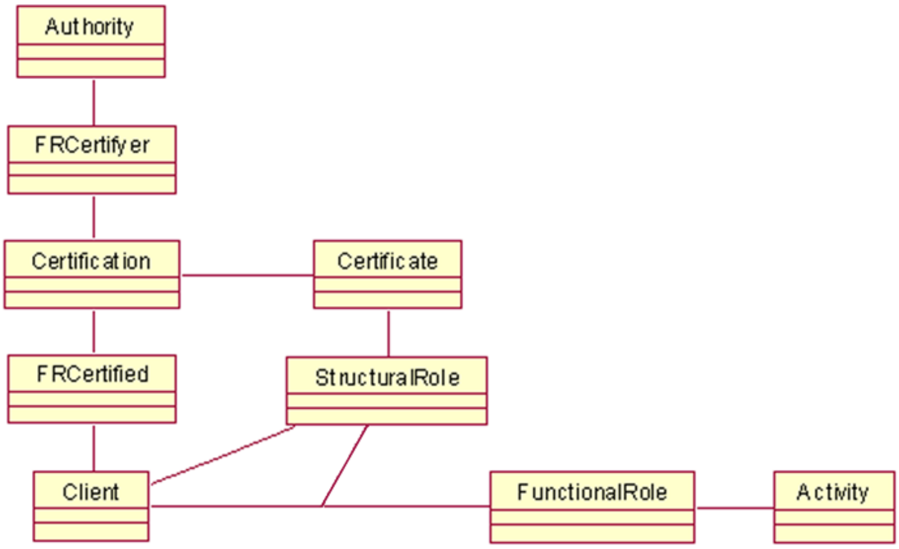


Figure A.4 — Establishment of a structural role within an act according to specific functional roles

Considering both structural roles and functional roles in the same context, structural roles provide the prerequisites/competences for entities to perform interactions (an act) within their specific functional roles. Qualifications, skills, etc., are influencing both the assignment of the structural roles and the performance of activities according to their functional roles.

A.4 Generic role specification

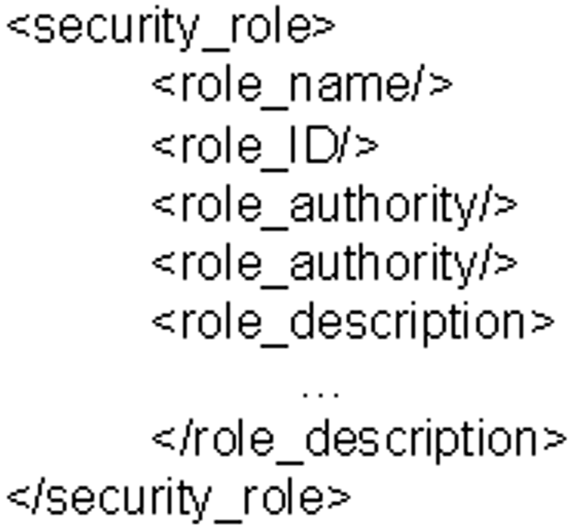
The role class is characterized by attributes summarized in Table A.1.

Table A.1 — Role attributes

Attribute	Type	Remarks
role_identifier	SET <II>	Set of InstanceIndentifier
role_name	CS	CodedSimpleValue
authority_identifier_ID	OID	ISO ObjectIdentifier
authority_identifier_name	ST	String
role_description	CD	ConceptDescription

Additionally, administration constraints may need to be enforced. For example, the separation of duties may be introduced as a widely used authorization constraint.

Figure A.5 describes a role using XML.



```
<security_role>
        <role_name/>
        <role_ID/>
        <role_authority/>
        <role_authority/>
        <role_description>
                ...
        </role_description>
</security_role>
```

Figure A.5 — Role specification

Annex B
(informative)

Example of structural roles in healthcare

Table B.1 — ASTM E-1986 licensed healthcare personnel that warrant differing levels of access control

Current standard list of licensed healthcare providers	Recommended enhanced list of licensed healthcare providers
Physician (MD/allopath, osteopath, chiropractic, naturopath, homeopath)	Physician (with sub-categories:) Chiropractor (was "chiropractic") Homeopath MD/Allopath Naturopath Osteopath Pathologist (new recommended role) Psychiatrist (new recommended role) Radiologist (new recommended role)
Physician assistant (PA)	Physician assistant (PA)
Advanced PRACTICE REGISTERED Nurse (NP, NM, CAN, CNS)	Nurse (with sub-categories:) Clinical NURSE Specialist (CNS) (was "CNS") Clinical registered nurse anesthetist (CRNA) (was "CAN") Licensed VOCATIONAL Nurse (LVN)/licensed practical nurse (LPN) [was "licensed vocational nurse (LVN)"] Nurse midwife (NM) (was "midwives" and "NM") Nurse practitioner (NP) (was "NP") Registered nurse (RN)
Midwives	See nurse
Registered nurse (RN)	See nurse
Licensed vocational nurse (LVN)	See nurse
Pharmacist (DP)	Pharmacist (with sub-categories) Pharmacist, apothecary (new recommended role) Pharmacist, clinical (new recommended role)
Non-western medicine providers	Non-western Medicine Providers (with sub-categories:) Acupuncturist (new recommended role) Massage Therapist (new recommended role)

Table B.1 (*continued*)

Current standard list of licensed healthcare providers	Recommended enhanced list of licensed healthcare providers
Ancillary service providers	Recommend deletion of “ancillary service providers” and replacement with detailed provider roles: Audiologist (new recommended role) Dentist (new recommended role) Dietitian (new recommended role) Psychologist (new recommended role) Speech pathologist (new recommended role) Veterinarian (DVM) (new recommended role)
Occupational therapy	Therapist (with sub-categories:) Audio Therapist (new recommended role) Educational Therapist (new recommended role) Kinesiotherapist (new recommended role) Musical Therapist (new recommended role) Occupational Therapist (was “Occupational Therapy”) Physical Therapist (was “Physical Therapy”) Recreational Therapist (new recommended role) Respiratory Therapist (was “Respiratory Therapy”) Speech Therapist (was “Speech Therapy”) Vocational Therapist (new recommended role)
Physical therapy	See therapist
Speech therapy	See therapist
Respiratory therapy	See therapist
Technician	Technician (with sub-categories:) Cardiology technician (new recommended role) Laboratory technician (new recommended role) Pharmacy technician (new recommended role) Prosthetic technician Radiology technician (new recommended role)
CAST technicians	Recommend deletion. See technician
Prosthetic technicians	See technician
(none)	Technologist (with sub-category) (new recommended role) Laboratory technologist (new recommended role)

Bibliography

[1] BLOBEL, B., *Assessment of Middleware Concepts Using a Generic Component Model*, Proceedings of the Conference “Toward An Electronic Health Record Europe ’97”, pp. 221-228. 20-23 October 1997, London

[2] BLOBEL, B., *Application of the Component Paradigm for Analysis and Design of Advanced Health System Architectures*. International Journal of Medical Informatics **60** (3), pp. 281-301, 2000

[3] BLOBEL, B., *Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems*, Series “Studies in Health Technology and Informatics” **89**, IOS Press, Amsterdam, 2002

[4] World Wide Web Consortium: Metadata Interchange Format (XMI): www.w3.org

[5] Health Level Seven, Inc.: www.hl7.org

[6] DAMIANOU, N., DULAY, N., LUPU, E. and SLOMAN, M., *Ponder: A Language for Specifying Security and Management Policies for Distributed Systems*, The Language Specification, Version 2.3. Imperial College Research Report DoC 2000/1. 20 October, 2000

[7] ISO/IEC 2382-8:1998, *Information technology — Vocabulary — Part 8: Security*

[8] ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[9] ISO/IEC 8824-1:2002, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

[10] ISO/IEC 9594-8:2001, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

[11] ISO/IEC 9798-3:1998, *Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques*

[12] ISO/IEC 10181-1:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*

[13] ISO/IEC TR 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[14] ISO/IEC TR 14516:2002, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*

[15] ISO/IEC 15945:2002, *Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*

[16] ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

[17] ENV 13729:2000, *Health informatics — Secure user identification — Strong authentication using microprocessor cards*

[18] ENV 13608-1:2000, *Health informatics — Security for healthcare communication — Part 1: Concepts and terminology*

[19] ENV 13606-3:2000, *Health informatics — Electronic healthcare record communication — Part 3: Distribution rules*

[20] ISO/IEC 10746-1, *Information technology — Open Distributed Processing — Reference model: Overview*

[21] ISO/TS 21298, *Health informatics — Functional and structural roles*

ICS 35.240.80

Price based on 27 pages