TECHNICAL SPECIFICATION

ISO/TS 21298

First edition
2008-12-01

Health informatics — Functional and structural roles

Informatique de santé — Rôles fonctionnel et structurel

Reference number
ISO/TS 21298:2008(E)

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 Normative references 1

3 Terms and definitions 1

4 Abbreviations 4

5 Modelling roles in an architectural context 4
5.1 Roles within the generic component model 4
5.2 Roles and policy aspects 5
5.3 Roles in privilege management 6
5.4 Structural roles 7
5.5 Functional roles 12

6 Formally modelling roles 14
6.1 Roles within the generic component model 14
6.2 Developing the role model 14
6.3 Relationships between structural and functional roles 17

7 Use cases for the use of structural and functional roles in an interregional or international context 17

Annex A (informative) **ISCO-08 Sample mapping** 19

Annex B (informative) **Sample certificate profile for regulated healthcare professional** 26

Bibliography 28

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 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 21298 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

This Technical Specification contains a specification for encoding information related to roles for health professionals and consumers. At least four areas have been identified where a model for encoding role information is needed.

a) **Privilege management and access control**: role-based access control is not possible without an effective means of recording role information for healthcare actors.

b) **Directory services**: structural roles are usefully recorded within directories of health care providers (see, for example, ISO/TS 21091).

c) **Audit trails**: functional roles are usefully recorded within audit trails for health information applications.

d) **Public key infrastructure (PKI)**: The three-part International Standard ISO 17090[9], [10] allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This Technical Specification identifies such a coded vocabulary.

In addition to these security related applications there are several other possible applications of this Technical Specification, such as:

e) **Search and retrieval**: finding and identifying the right professional for a health service.

f) **Administration**: billing of health care services.

g) **Messaging**: directing healthcare related messages by means of a specific role.

This Technical Specification is complemetary to other relevant standards that also describe and define roles for the purpose of access control. Backward compatibility with ANSI INCITS and HL7 RBAC is provided through simplification by combining the policy and role into a single construct. This Technical Specification extends the model through the separation of the role and policy. This separation allows for a richer and more flexible capability to instantiate business rules across multiple domains and jurisdictions.

Health informatics — Functional and structural roles

1 Scope

This Technical Specification defines a model for expressing functional and structural roles and populates it with a basic set of roles for international use in health applications. Roles are generally assigned to entities that are actors. This will focus on roles of persons (e.g. the roles of health professionals) and their roles in the context of the provision of care (e.g. subject of care).

Roles can be structural (e.g. licensed general practitioner, non-licensed transcriptionist) or functional (e.g. a provider who is a member of a therapeutic team, an attending physician, etc). Structural roles are relatively static, often lasting for many years. They deal with relationships between entities expressed at a level of complex concepts. Functional roles are bound to the realization of actions and are highly dynamic. They are normally expressed at a decomposed level of fine-grained concepts.

Roles addressed in this Technical Specification are not restricted to privilege management purposes, though privilege management is one of the applications of this Technical Specification as well as access control. This Technical Specification does not address specifications related to permissions. This Technical Specification treats the role and the permission as separate constructs. Further details regarding the relationship with permissions, policy and access control are provided in ISO/TS 22600-1.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 17090-2, *Health informatics — Public key infrastructure — Part 2: Certificate profile*

ISO/HL7 21731, *Health informatics — HL7 version 3 — Reference information model — Release 1*

ISO 22600-1, *Health informatics — Privilege management and access control — Part 1: Overview and policy management*

International Labour Organization: *International Standard Classification of Occupations 2008* (ISCO-08)

3 Terms and definitions

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

3.1
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]

3.2
attribute authority
AA
authority that assigns privileges by issuing attribute certificates

NOTE Adapted from X.509.

3.3
attribute certificate
data structure, digitally signed by an attribute authority, which binds some attribute values with identification about its holder

NOTE Adapted from X.509.

3.4
authority
entity that is responsible for the issuance of certificates

NOTE Two types are distinguished in this Technical Specification: certification authority which issues public-key certificates and attribute authority which issues attribute certificates.

3.5
authorization
granting of rights, which includes the granting of access based on access rights

[ISO 7498-2, definition 3.3.10]

3.6
delegation
conveyance of privilege from one entity that holds such privilege, to another entity

3.7
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

3.8
entity
any concrete or abstract thing of interest

[ISO/IEC 10746-2, definition 6.1]

NOTE While in general the word entity can be used to refer to anything, in the context of modelling it is reserved to refer to things in the universe of discourse being modelled.

3.9
identification
performance of tests to enable a data processing system to recognise entities

[ISO/IEC 2382-8, definition 08.04.12 (as **identitiy authentication**, **identity validation**)]

3.10
non-regulated health professional
person employed by a healthcare organization, but who is not a health professional

[ISO/IEC 17090-1, definition 3.1.5]

EXAMPLES Receptionist or secretary who organizes appointments, or a business manager who is responsible for validating patient health insurance.

NOTE The fact that the employee is not authorized by a body independent of the employer in his professional capacity does not, of course, imply that the employee is not professional in conducting his services.

3.11
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

3.12
policy agreement
written agreement in which all involved parties commit themselves to a specified set of policies

3.13
principal
actor able to realize specific scenarios (user, organization, system, device, application, component, object)

3.14
privilege
capacity assigned to an entity by an authority according to the entity's attribute

NOTE Per OASIS Extensible Access Control Markup Language (XACML) V2.0, privilege, permissions, authorization, entitlement and rights are replaced by the term “rule”.

3.15
regulated health professional
person who is authorized by a nationally recognized body to be qualified to perform certain health services

[ISO/IEC 17090-1, definition 3.1.8]

EXAMPLES Physicians, registered nurses and pharmacists.

NOTE 1 The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognised bodies include local or regional governmental agencies, independent professional associations and other formally and nationally recognised organizations. They may be exclusive or non-exclusive in their territory.

NOTE 2 A nationally recognized body in this definition does not imply one nationally controlled system of professional registration but, in order to facilitate international communication, it would be preferable for one nationwide directory of recognised health professional registration bodies to exist.

3.16
role
set of competences and/or performances that are associated with a task

3.17
role assignment certificate
certificate that contains the role attribute, assigning one or more roles to the certificate holder

3.18
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.

3.19
role specification certificate
certificate that contains the assignment of privileges to a role

4 Abbreviations

AA Attribute Authority

XML eXtensible Markup Language

ILO International Labour Organization

PKI Public Key Infrastructure

PMI Privilege Management Infrastructure

UML Unified Modelling Language

5 Modelling roles in an architectural context

5.1 Roles within the generic component model

For embedding components meeting functional requirements and services needed in a system, the components of that system have to be managed in its architectural context. Therefore, requirements analysis, design, and deployment of those components shall be developed and managed based on a reference architecture following a unified process.

With the generic component model such reference architecture in conformance with essential standards for distributed, component-based, service-oriented and semantically interoperable information systems has been developed in the mid-nineties (see, e.g. References [1], [2], [3]) and used in the context of several ISO/TC 215 and CEN/TC 251 specifications. The model specifies a component-based and service oriented architecture for any domain. While this Technical Specification goes beyond security and privacy issues, functional and structural roles are also used to manage privileges and access control. In this restricted context, functional and structural roles have been specified and modelled in ISO/TS 22600-2. This Technical Specification extends scope, services, and deployment of functional and structural roles, nevertheless being based on the architectural approach for semantically interoperable eHealth/pHealth (personal health) information systems.

A system architecture defines the system's components, their functions and interrelationships. A system architecture is modelled in three dimensions:

— components for meeting specific domains' requirements;

— the decomposition and, after detailing the underlying concepts, the composition of those components following corresponding aggregation concepts/rule (e.g. component collaboration, workflow, algorithm); granularity levels are at least business concepts, relations networks, basic services/functions and basic concepts;

— the different views on that component according to ISO 10746-2[8] from the enterprise view (business case, use case, requirements) through the information view and the computational view representing the platform independent logic of the system/component as well as the engineering view and technology view both dealing with platform-specific implementation aspects.

Figure 1 presents the generic component model providing the aforementioned reference architecture.

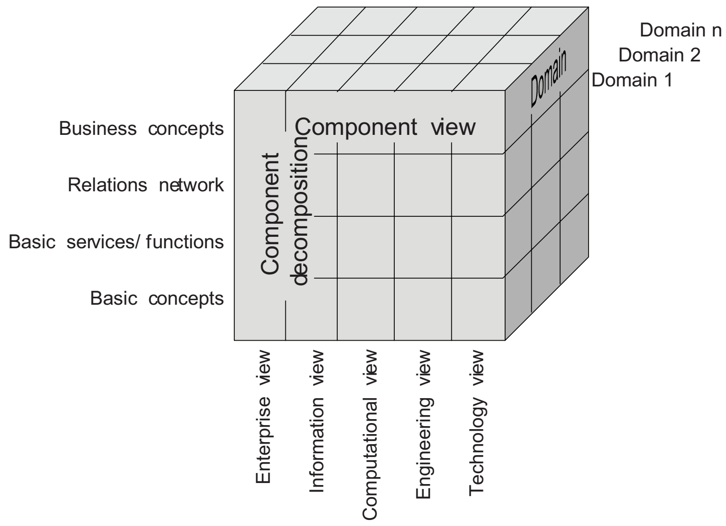

Figure 1 — Generic component model

The development of components, their concept representation and their aggregation are based on constraint modelling. Concepts and rules can be represented using meta-languages such as UML and UML derivates or the XML languages set.

5.2 Roles and policy aspects

Roles are components reflecting specific aspects of a system. They have to be managed according to all dimensions of the GCM. As policies are properties and functions in another system/component dimension, policies have to be embedded in the component specification through corresponding constraints. Interrelated classes and associations can be simplistically modelled by component attributes and operational constraints. This is done, for example, in some simplistic RBAC specifications, ignoring the policy-driven correct approach. Associating, for example, a functional role class with the related policy class defining context and other constraints to access target objects, the resulting component can summarise those constraints in a permission bound to this role and expressed as permission attribute.

For managing relationships between the entities, structural (organizational) and functional roles can be defined. Roles might be assigned to any entity as an actor in a communication or cooperation interrelationship (e.g. person, organization, system, device, application, component, etc.). Because entities are actors in use cases, roles have a relationship to actors and therefore to actions. Functional and structural roles are associated with and defined by policies.

A policy may describe the legal framework including rules and regulations, the organizational and administrative framework, functionalities, claims and objectives, the entities involved, agreements, rights, duties, and penalties defined as well as the technological solution implemented for collecting, recording, processing and communicating data in information systems.

Policies can be specified and implemented in different ways, including:

- in a policy agreement as specified in ISO/TS 22600-1;
- as an attribute;
- as an implicit policy as part of another component;
- as a separate policy element to be combined with another component or used directly;
- as a rule policy combined with another policy;
- as structured expressions (e.g. using XACML).

A policy may be applied as a set of rules describing the design and operation of a system. Health information systems such as the Electronic Health Record (EHR), for instance, should have a patient policy, enterprise policy, policies defined by laws and regulations, and one policy per structural role as well as one policy per functional role. Further details regarding policy specification and the relationship to privilege management and access control are provided in ISO/TS 22600-1.

Roles can be instantiated through numerous mechanisms, including directory entries, database variables and certificates, among others. Role assignment certificates may be attribute certificates or public-key certificates. Specific privileges are assigned to a role rather than to an individual through role specification certificates. The indirect assignment enables the privileges assigned to a role to be updated, without impacting the certificates that assign roles to individuals. Role specification certificates must be attribute certificates, and not public-key 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 are all possible:

a) any number of roles can be defined by any attribute authority;

b) the role itself and the members of a role can be defined and administered separately, by different attribute authorities;

c) a privilege may be delegated;

d) roles may be assigned any suitable lifetime.

Further discussion regarding assignment of multiplicity of structural and functional roles is addressed in the discussion of structural and functional roles below. Further details regarding the expression of roles through digital certificates are provided in ISO 17090-2. Further details regarding the representation of roles as a directory entry are provided in ISO/TS 21091.

Functional and structural roles are associated with and defined by policies.

Health information systems such as the Electronic Health Record (EHR), for instance, should have a patient policy, an enterprise policy, policies defined by laws and regulations, and one policy per structural role as well as one policy per functional role. Further details regarding policy specification and the relationship to privilege management and access control are provided in ISO/TS 22600-1.

5.3 Roles in privilege management

Privileges can be assigned to an individual by a role assignment, or directly. A role can be expressed in public key certificates, attribute certificates or in a directory entry as described in ISO 17090-2 and ISO/TS 21091. 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, not privileges assigned to the role. If the role assignment certificate is an attribute certificate, the **role** attribute is contained in the **attributes** component of the attribute certificate.

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 make a pass/fail authorization decision. 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 done within the PMI in a role specification certificate or outside the PMI (e.g. locally configured). If the role privileges are 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 Technical Specification. A role specification certificate cannot be delegated to any other entity. The issuer of the role assignment certificate may be independent of the issuer of the role specification certificate and these

