INTERNATIONAL STANDARD

ISO 21298

First edition
2017-02

Corrected version
2017-04

Health informatics — Functional and structural roles

Informatique de santé — Rôles fonctionnels et structurels

Reference number
ISO 21298:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This first edition of ISO 21298 cancels and replaces ISO/TS 21298:2008, which has been technically revised.

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This corrected version incorporates the following correction:

— replacement of Figure 2.

Introduction

This document contains a specification for encoding information related to roles for health professionals and consumers. At least five 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 healthcare providers (see for example, ISO 21091).

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

d) **Public key infrastructure (PKI)**: The ISO 17090 series allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This document identifies such a coded vocabulary.

e) **Purpose of use**: A role specification determines for what purposes healthcare information can be used. Purposes of use are tied to specific roles in many cases (see for example, ISO 21091).

In addition to these security-related applications, there are several other possible applications of this standard, such as follows.

- **Clinical care provision**: finding and identifying the right professional for a health service.
- **Support of care**: billing of healthcare services.
- **Communication management**: directing healthcare-related messages by means of a specific role.
- **Health service management and quality assurance**: defining the purpose of use for specific data.

This document is complementary to other relevant standards that also describe and define roles for the purpose of access control. It extends the model through the separation of role and policy. This separation allows for a richer and more flexible capability to instantiate business rules across multiple domains and jurisdictions. Backward compatibility with ANSI International Committee for Information Technology Standards (INCITS) and HL7 RBAC (Role-Based Access Control) is provided through simplification by combining policy and role into a single construct.

The role concepts defined in this document are referenced and reused in many international standards created, for example, by ISO, CEN, HL7 International. Examples are ISO 22600, Reference [9], Reference [10] and Reference [11].

The European Commission and the EU Parliament have established a Professional Qualifications Directive (2005/36/EC) defining medical specialties (see http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02005L0036-20140117&from=EN).

Annex A provides ISOCO-08 sample mapping while Annex B provides sample certificate profile for regulated healthcare professionals.

INTERNATIONAL STANDARD **ISO 21298:2017(E)**

Health informatics — Functional and structural roles

1 Scope

This document 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, etc.) or functional (e.g. a provider who is a member of a therapeutic team, an attending physician, prescriber, 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 document are not restricted to privilege management purposes, though privilege management and access control is one of the applications of this document. This document does not address specifications related to permissions. This document treats the role and the permission as separate constructs. Further details regarding the relationship with permissions, policy, and access control are provided in ISO 22600.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

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

[SOURCE: ISO/IEC 2382-8:2015, 2126294]

3.2
attribute certificate authority
AA
authority which assigns privileges by issuing *attribute certificates* (3.3)

[SOURCE: ISO/IEC 9594-8:2014, 3.5.2, modified]

3.3
attribute certificate
data structure, digitally signed by an Attribute Authority, that binds some attribute values with *identification* (3.12) about its holder

[SOURCE: ISO/IEC 9594-8:2014, 3.5.1]

3.4
authorization
granting of privileges, which includes the granting of privileges to access data and functions

Note 1 to entry: Derived from ISO 7498-2: the granting of rights, which includes the granting of access based on access rights.

[SOURCE: ISO 22600-1:2014, 3.6]

3.5
certification authority
CA
certificate issuer; an authority trusted by one or more relying parties to create, assign and manage certificates

Note 1 to entry: Optionally, the certification authority can create the relying parties' keys [ISO 9594-8]. The CA issues certificates by signing certificate data with its private signing key.

Note 2 to entry: Authority in the CA term does not imply any government authorization, only that it is trusted. Certificate issuer can be a better term but CA is used very broadly.

[SOURCE: ISO 22600-1:2014, 3.8]

3.6
delegation
conveyance of privilege from one *entity* (3.8) that holds such privilege, to another entity

[SOURCE: ISO 22600-1:2014, 3.10]

3.7
delegation path
ordered sequence of certificates which, together with authentication of a *privilege asserter's* (3.19) identity, can be processed to verify the authenticity of a privilege asserter's privilege

[SOURCE: ISO 22600-2:2014, 3.15]

3.8
entity
any concrete or abstract thing of interest

Note 1 to entry: 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
functional role
role (3.21) which is bound to an act

Note 1 to entry: Functional roles can be assigned to be performed during an act.

Note 2 to entry: Functional roles have been specified in this document.

Note 3 to entry: Functional roles correspond to the ISO/HL7 21731 RIM participation.

Note 4 to entry: See also *structural role* (3.26).

3.10
healthcare organization
officially registered organization that has a main activity related to healthcare services or health promotion

EXAMPLE Hospitals, Internet healthcare website providers, and healthcare research institutions.

Note 1 to entry: The organization is recognized to be legally liable for its activities but need not be registered for its specific *role* (3.21) in health.

[SOURCE: ISO 17090-1:2013, 3.1.4]

3.11
healthcare professional
healthcare personnel having a healthcare professional entitlement recognized in a given jurisdiction

Note 1 to entry: The healthcare professional entitlement entitles a healthcare professional to provide healthcare independent of a *role* (3.21) in a *healthcare organization* (3.10).

EXAMPLE GP, medical consultant, therapist, dentist, etc.

3.12
identification
performance of tests to enable a data processing system to recognize entities

3.13
non-regulated healthcare personnel
person employed by a *healthcare organization* (3.10), but who is not a regulated health professional

EXAMPLE Massage therapist, music therapist, etc.

[SOURCE: ISO 17090-1:2013, 3.1.5, modified]

3.14
organization employee
person employed by a *healthcare organization* (3.10) or a *supporting organization* (3.27)

EXAMPLE Medical records transcriptionists, healthcare insurance claims adjudicators, and pharmaceutical order entry clerks.

3.15
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

[SOURCE: ISO 22600-1:2014, 3.13]

3.16
policy agreement
written agreement where all involved parties commit themselves to a specified set of policies

[SOURCE: ISO 22600-1:2014, 3.14]

3.17
principal
human users and objects that need to operate under their own rights

[SOURCE: OMG Security Services Specification: 2001]

3.18
privilege
capacity assigned to an *entity* (3.8) by an authority according to the entity’s attribute

Note 1 to entry: Per OASIS Extensible Access Control Markup Language (XACML) V2.0, privilege, permissions, authorization, entitlement and rights are replaced by the term ‘rule’.

[SOURCE: ISO 22600-1:2014, 3.17]

3.19
privilege asserter
privilege holder using their *attribute certificate* (3.3) or public-key certificate to assert *privilege* (3.18)

[SOURCE: ISO 22600-2:2014, 3.27]

3.20
privilege verifier
entity (3.8) verifying certificates against a privilege policy

[SOURCE: ISO 22600-2:2014, 3.30]

3.21
role
set of competencies and/or performances that are associated with a task

[SOURCE: ISO 22600-2:2014, 3.33]

3.22
role assignment certificate
certificate that contains the role attribute, assigning one or more *roles* (3.21) to the certificate holder

[SOURCE: ISO 22600-2:2014, 3.34]

3.23
role certificate
certificate that assigns *privileges* (3.18) to a *role* (3.21) rather than directly to individuals

Note 1 to entry: Individuals assigned to a role, through an *attribute certificate* (3.3) or public-key certificate with a subject directory attributes extension containing that assignment, are indirectly assigned the privileges contained in the role certificate.

3.24
role specification certificate
certificate that contains the assignment of *privileges* (3.18) to a *role* (3.21)

[SOURCE: ISO 22600-2:2014, 3.35]

3.25
sponsored healthcare provider
health services provider who is not a regulated professional in the jurisdiction of his/her practice, but who is active in his/her healthcare community and sponsored by a regulated *healthcare organization* (3.10)

EXAMPLE Drug and alcohol education officer who is working with a particular ethnic group, or a healthcare aid worker in a developing country.

[SOURCE: ISO 17090-1:2013, 3.1.10]

3.26
structural role
role (3.21) specifying relations between entities in the sense of competence, often reflecting organizational or structural relations (hierarchies).

Note 1 to entry: Structural roles have been specified in this document.

Note 2 to entry: Structural roles correspond to the ISO/HL7 21731 RIM role.

Note 3 to entry: See also *functional role* (3.9).

3.27
supporting organization
officially registered organization which is providing services to a *healthcare organization* (3.10), but which is not providing healthcare services

EXAMPLE Healthcare financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods.

[SOURCE: ISO 17090-1:2013, 3.1.11]

3.28
supporting organization employee
person employed by a *supporting organization* (3.27)

4 Abbreviated terms

AA	Attribute Authority
CA	Certification Authority
GCM	Generic Component Model
HL7	Health Level 7
ILO	International Labour Organization
NIST	National Institute for Standards
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
RBAC	Role-Based Access Control
UML	Unified Modeling Language
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

5 Modeling 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 have to be developed and managed based on a reference architecture following a unified process.

With the Generic Component Model (GCM), 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-1990s (e.g. ISO/IEC 9594-8, ISO/IEC 10746-2, and ISO/IEC 2382-8) and used in the context of several ISO TC 215 and CEN TC 251, as well as HL7 specifications. The model specifies a component-based and service-oriented architecture for any domain. While this document 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 22600. This document 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[7][8].

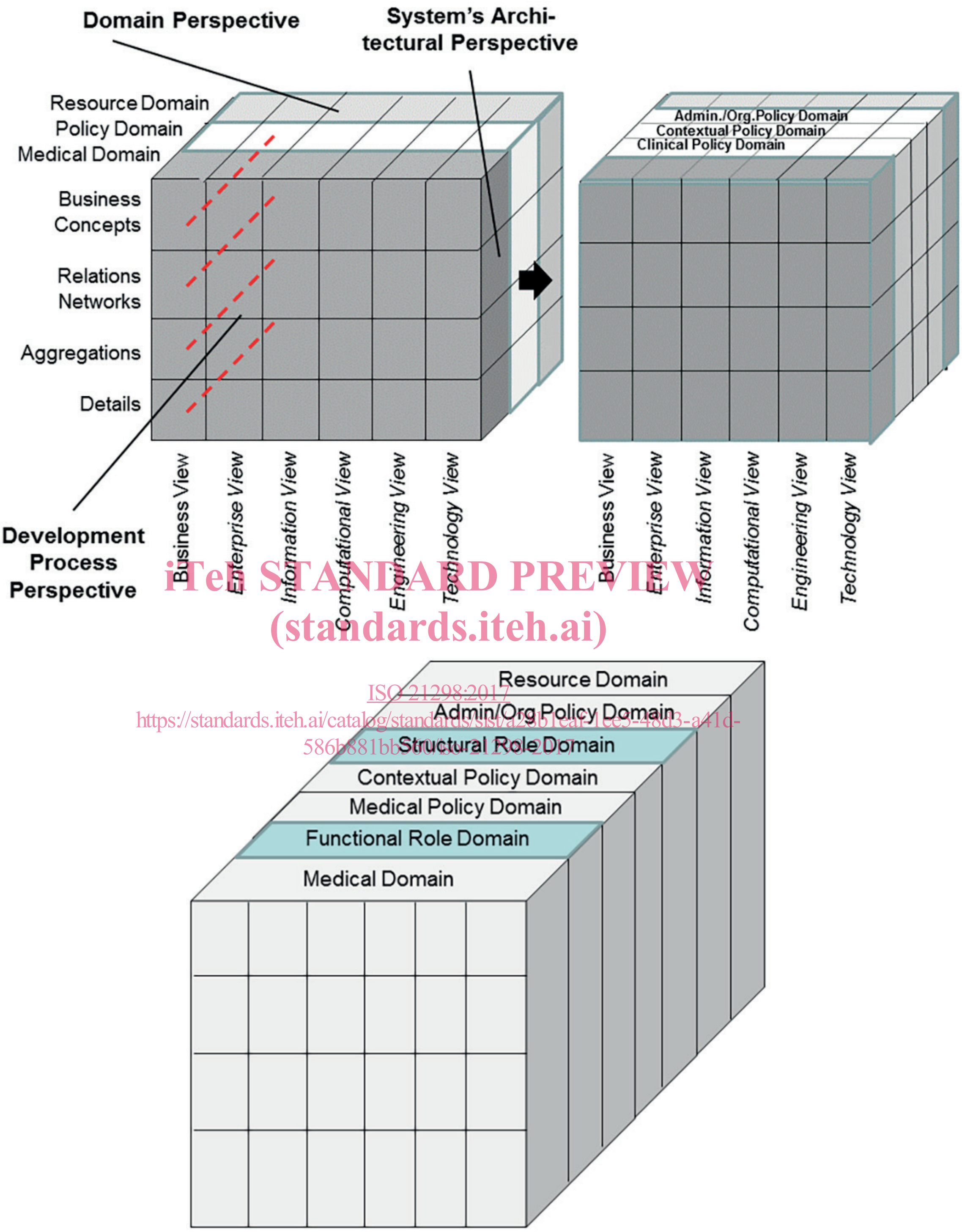
A system architecture defines the system's components, their functions and interrelationships. A system architecture is modelled in three dimensions.

— 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 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, adding a real-world business viewpoint to the ISO 10746 viewpoints.



NOTE Modelled after Reference [8] (modified).

Figure 1 — Representation of the role concepts defined in this standard using the Generic Component Model

The principles established in this document are also applicable to domains other than healthcare. In that case, that domain and its related policy domain have to be entered in Figure 1c.