SLOVENSKI STANDARD
oSIST prEN ISO 21298:2015

01-januar-2015

Zdravstvena informatika - Funkcionalne in strukturne vloge (ISO/DIS 21298:2014)

Health informatics - Functional and structural roles (ISO/DIS 21298:2014)

Informatique de santé - Rôles fonctionnels et structurels (ISO/DIS 21298:2014)

Ta slovenski standard je istoveten z: **prEN ISO 21298:2014**

ICS:

35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

oSIST prEN ISO 21298:2015 **en,fr,de**

DRAFT INTERNATIONAL STANDARD
ISO/DIS 21298

ISO/TC **215** Secretariat: **ANSI**

Voting begins on:
2014-08-26

Voting terminates on:
2014-11-26

Health informatics — Functional and structural roles

Informatique de santé — Rôles fonctionnels et structurels
[Revision of edition (ISO)]

ICS: 35.240.80

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/DIS 21298:2014(E)

Contents

Page

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 whom 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 was prepared by Technical Committee ISO/TC 215, *Health informatics*, Working Group 4: Security .

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

Introduction

This document 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 21091 Health informatics – Directory services for security, communications, and identification of professionals and subjects of care).

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

d) **Public key infrastructure (PKI)**: The three part ISO standard 17090 Health Informatics – Public Key Infrastructure (PKI) allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This International Standard identifies such a coded vocabulary.

e) **Purpose of Use**: A role specification determines for what purposes health care information can be used. Purposes of use are tied to specific roles in many cases (see for example ISO/TS 21091 Health informatics – Classification of purposes for processing personal health information).

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

f) **Clinical care provision**: finding and identifying the right professional for a health service,

g) **Support of care**: billing of health care services,

h) **Communication management**: directing healthcare related messages by means of a specific role, and

i) **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. Backward compatibility with ANSI INCITS (InterNational Committee for Information Technology Standards) and HL7 RBAC (Role-Based Access Control) is provided through simplification by combining policy and role into a single construct. This document 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.

Health informatics — Functional and structural roles

1 Scope

This International Standard 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, 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 realisation of actions and are highly dynamic. They are normally expressed at a decomposed level of fine-grained concepts.

The role concepts defined in this standard are referenced and reused in many international standards created, e.g., by ISO, CEN, HL7 International. Examples are ISO 22600 “Health informatics – Privilege management and access control”, HL7 International “HL7 Healthcare privacy and security classification system (HCS)”, HL7 International “HL7 Security and privacy ontology”, HL7 International “The HL7 RBAC Healthcare Permission Catalog” or HL7 International “HL7 Composite security and privacy domain analysis model DSTU”.Roles addressed in this International Standard are not restricted to privilege management purposes, though privilege management and access control is one of the applications of this International Standard. This standard 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

The following normative documents contain, through reference in this text, provisions of this International Standard. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

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

ISO/FDIS 17090-1:2013 Health informatics – Public Key Infrastructure

ISO/FDIS 22600:2013 Health informatics – Privilege Management and Access Control

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 2382-8:1998]

3.2
attribute authority (AA)
authority which assigns privileges by issuing attribute certificates
[ISO/IEC 9594-8:1995]

3.3
attribute certificate
data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification about its holder
[ISO/IEC 9594-8:1995]

3.4
authority
entity, which is responsible for the issuance of certificates.

Note 1 to entry: Two types are distinguished in this Specification: certification authority which issues public-key certificates and attribute authority which issues attribute certificates [ISO/FDIS 22600:2013]

3.5
authorisation
granting of privileges, which includes the granting of privileges to access data and functions

NOTE: derived from ISO 7498-2:1989: the granting of rights, which includes the granting of access based on access rights

3.6
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 may create the relying parties' keys [ISO 9594-8:1995]. 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 authorisation only that it is trusted. Certificate issuer may be a better term but CA is used very broadly.

3.7
delegation
conveyance of privilege from one entity that holds such privilege, to another entity

3.8
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

3.9
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. [ISO/IEC 10746-2:1996]

3.10
functional role
role which is bound to an act. Functional roles can be assigned to be performed during an act.

Note 1 to entry: Functional roles have been specified in this International Standard.

Note 2 to entry: Functional roles correspond to the ISO/HL7 21731 RIM participation.

Note 3 to entry: See also structural role

3.11
healthcare organisation
officially registered organisation that has a main activity related to healthcare services or health promotion [ISO/FDIS 17090-1:2013]

Example 1 to entry: Hospitals, Internet healthcare website providers, and healthcare research institutions.

Note 1 to entry: The organisation is recognised to be legally liable for its activities but need not be registered for its specific role in health.

3.12
identification
performance of tests to enable a data processing system to recognize entities [ISO/IEC 2382-08:1998]

3.13
non-regulated health professional
person employed by a healthcare organization, but who is not a regulated health professional [ISO/FDIS 17090-1:2013]

Example 1 to entry: massage therapist, music therapist, etc.

Note 1 to entry: The fact that the employee is not authorized by a body independent of the employer in his professional capacity does, of course, not imply that the employee is not professional in conducting his services.

3.14
organisation employee
person employed by a healthcare organisation or a supporting organisation

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

3.15
policy
set of legal, political, organisational, functional and technical obligations for communication and cooperation [ISO/FDIS 22600:2013]

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

3.17
principal
human users and objects that need to operate under their own rights [OMG Security Services Specification: 2001]

3.18
privilege
capacity assigned to an entity by an authority according to the entity's attribute [ISO/FDIS 22600:2013]

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

3.19
privilege asserter
privilege holder using their attribute certificate or public-key certificate to assert privilege [ISO 22600:2013]