SLOVENSKI STANDARD
SIST EN ISO 21091:2013

01-april-2013

Zdravstvena informatika - Imeniške storitve za ponudnike zdravstvenega varstva, zdravstvene delavce in paciente (ISO 21091:2013)

Health informatics - Directory services for healthcare providers, subjects of care and other entities (ISO 21091:2013)

Medizinische Informatik - Verzeichnisdienste für Sicherheit, Kommunikation und Identifikation von Heilberuflern und Patienten (ISO 21091:2013)

Informatique de santé - Services d'annuaires pour la sécurité, les communications et l'identification des patients et des professionnels (ISO 21091:2013)

Ta slovenski standard je istoveten z: **EN ISO 21091:2013**

ICS:

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

SIST EN ISO 21091:2013 **en**

iTeh STANDARD PREVIEW

(standards.iteh.ai)

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 21091

February 2013

ICS 35.240.80

English Version

Health informatics - Directory services for healthcare providers, subjects of care and other entities (ISO 21091:2013)

Informatique de santé - Services d'annuaires pour les fournisseurs de soins de santé, les sujets de soins et autres entités (ISO 21091:2013)

Medizinische Informatik - Verzeichnisdienste für Anbieter, zu Behandelnde und andere Entitäten im Gesundheitswesen (ISO 21091:2013)

This European Standard was approved by CEN on 2 February 2013.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO 21091:2013: E

EN ISO 21091:2013 (E)

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Foreword

This document (EN ISO 21091:2013) has been prepared by Technical Committee ISO/TC 215 "Health informatics" in collaboration with Technical Committee CEN/TC 251 "Health informatics" the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2013, and conflicting national standards shall be withdrawn at the latest by August 2013.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 21091:2013 has been approved by CEN as EN ISO 21091:2013 without any modification.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

INTERNATIONAL STANDARD

ISO
21091

First edition
2013-02-15

Health informatics — Directory services for healthcare providers, subjects of care and other entities

Informatique de santé — Services d'annuaires pour les fournisseurs de soins de santé, les sujets de soins et autres entités

© ISO 2013

ISO 21091:2013(E)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

COPYRIGHT PROTECTED DOCUMENT

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 21091:2013
https://standards.iteh.ai/catalog/standards/sist/0cfe5c69-fcd4-438d-ad5d-
8675c67574c5/sist-en-iso-21091-2013

ISO 21091:2013(E)

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.

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 21091 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This first edition cancels and replaces ISO/TS 21091:2005, which has been technically revised.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Introduction

Health informatics directory services for healthcare providers, subjects of care and other entities are intended to support the communication and security requirements of healthcare professionals in the conduct of clinical and administrative functions. Healthcare requires extensive encipherment and access control requirements for the disclosure and transport of all confidential health information. In support of the healthcare public key infrastructure, healthcare will make available a registry of certificates including business and professional information necessary to conduct healthcare transactions. This information necessarily includes identification of individual roles within the healthcare system as can only be identified by the respective healthcare organizations. As such, the registration and management functions are to be extensible, and potentially distributed throughout the healthcare community. Support for these additional healthcare requirements for security is also to be offered through the directory service.

The directory is becoming an increasingly popular method of providing a means for single sign-on capabilities to support authentication. This goal has resulted in the inclusion of authentication and identity attributes to authenticate the identity of a healthcare person or entity.

The directory also supports the communication of additional attributes that can be used to support authorization decisions. This goal has driven directory schema extensions to include organization employee management information, healthcare-specific contact information, and healthcare identifiers. This International Standard addresses the healthcare-specific requirements of the directory, and defines, as appropriate, standard specifications for inclusion of this information in the healthcare directory.

Besides technical security measures that are discussed in other ISO standards, communication of healthcare data requires a reliable accountable "chain of trust." In order to maintain this chain of trust within a public key infrastructure, users (relying parties) need to be able to obtain current correct certificates and certificate status information through secure directory management.

The healthcare directory will support standard lightweight directory access protocol (LDAP) client searches, interface engines for message transformation, and service oriented architecture (SOA) implementations to enable the service in any environment. Specific implementation guidance, search criteria and support are outside the scope of this International Standard.

While specific security measures and access control specifications are out of scope of this International Standard, due to the sensitive nature of health related and privacy information that may be supported through the directory services, significant controls need to be enabled at branch, object classes, and attribute levels. Processes and procedures should be in place to ensure information integrity represented within the health directory, and responsibility for the content of the directory should be clearly allocated through policy and process. It is anticipated that appropriate access controls managing who can read, write or modify all items in the healthcare directory will be applied. This may be accomplished by assigning individuals within the directory to the HCOrganizationalRole and assigning appropriate privileges (e.g. read, modify, delete) to that role in directory management configuration.

iTeh STANDARD PREVIEW

(standards.iteh.ai)

ISO 21091:2013(E)

Health informatics — Directory services for healthcare providers, subjects of care and other entities

1   Scope

This International Standard defines minimal specifications for directory services for healthcare. It can be used to enable communications between organizations, devices, servers, application components, systems, technical actors, and devices.

This International Standard provides the common directory information and services needed to support the secure exchange of healthcare information over public networks where directory information and services are used for these purposes. It addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction, and international healthcare communications. While several options are supported by this International Standard, a given service will not need to include all of the options.

In addition to the support of security services, such as access control and confidentiality, this International Standard provides specification for other aspects of communication, such as addresses and protocols of communication entities.

This International Standard also supports directory services aiming to support identification of health professionals and organizations and the subjects of care.

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/HL7 27931:2009, *Data Exchange Standards — Health Level Seven Version 2.5 — An application protocol for electronic data exchange in healthcare environments*

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]

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

[X.509]

ISO 21091:2013(E)

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

[X.509]

3.4
authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

[ISO 7498-2]

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

[ISO 7498-2]

3.6
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2]

3.7
certificate
public key certificate

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.8
certificate distribution
act of publishing certificates and transferring certificates to security subjects

3.9
certificate issuer
authority trusted by one or more relying parties to create and assign certificates

Note 1 to entry: Optionally the certification authority may create the relying parties' keys.

[ISO/IEC 9594-8]

3.10
certificate management
procedures relating to certificates, i.e. certificate generation, certificate distribution, certificate archiving and revocation

3.11
certificate revocation
act of removing any reliable link between a certificate and its related owner (or security subject owner) because the certificate is not trusted any more, even though it is unexpired

3.12
certificate revocation list
CRL
published list of the suspended and revoked certificates (digitally signed by the CA)

3.13
certificate verification
verifying that a *certificate* (3.7) is authentic

3.14
certification authority
CA
authority trusted by one or more relying parties to create and assign certificates and which may, optionally, create the relying parties' keys

Note 1 to entry: Adapted from ISO/IEC 9594-8.

Note 2 to entry: Authority in the CA term does not imply any government authorization, but only denotes that it is trusted.

Note 3 to entry: "Certificate issuer" may be a better term, but CA is very widely used.

3.15
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO 7498-2]

3.16
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

3.17
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[ISO 7498-2]

3.18
identification
performance of tests to enable a data processing system to recognize entities

[ISO/IEC 2382-8]

3.19
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[ENV 13608-1]

3.20
integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

3.21
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2]

3