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

Reference number
ISO 21091:2013(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

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.

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.

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]

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

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]

3.22
key management
generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy

[ISO 7498-2]

3.23
lightweight directory access protocol
LDAP
standard access protocol for directories allowing public or controlled access to certificates and other information needed in a PKI

3.24
object identifier
OID
unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class

3.25
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

[ISO/IEC 2382-8]

3.26
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]

3.27
public key
key that is used with an asymmetric cryptographic algorithm and that can be made publicly available

[ISO/IEC 10181-1]

3.28
public key certificate
PKC
certificate that binds an identity and a public key

[RFC 3280]

3.29
public key infrastructure
PKI
structure of hardware, software, people, processes and policies that uses digital signature technology to provide relying parties with a verifiable association between the public component of an asymmetric key pair with a specific subject

3.30
relying party
recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate

[RFC 3647]

3.31
role
set of competences and/or performances associated with a task

3.32
security
combination of availability, confidentiality, integrity and accountability

[ENV 13608-1]

3.33
security policy
plan or course of action adopted for providing computer security

[ISO/IEC 2382-8]

3.34
security service
service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[ISO/IEC 7498]

3.35
security subject
active entity, generally in the form of a person, process or device, that causes information to flow among objects or changes the system state

Note 1 to entry: Technically, a process/domain pair.

3.36
subject
entity whose public key is certified in the certificate

3.37
subject of care
person scheduled to receive, receiving, or having received healthcare

3.38
third party
party other than data originator, or data recipient, required to perform a security function as part of a communication protocol

3.39
trusted third party
TTP
third party which is considered trusted for purposes of a security protocol

[ENV 13608-1]

Note 1 to entry: This term is used in many ISO/IEC standards and other documents describing mainly the services of a CA. The concept is however broader and includes services like time stamping and possibly escrowing.

4 Symbols (and abbreviated terms)

CA	Certification Authority
CN	Common Name
CRL	Certificate Revocation List

DAP	Directory Access Protocol
DIT	Directory Information Tree
DN	Distinguished Name
EDI	Electronic Data Interchange
LDAP	Lightweight Directory Access Protocol
MPI	Master Patient Index
PDA	Personal Data Assistant
PIDS	Person Identification Service
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RA	Registration Authority
RDN	Relative Distinguished Name
TTP	Trusted Third Party

5 Healthcare context

5.1 General

In order to accommodate healthcare-specific concerns, standard directory services shall be extended.

X.500 defined attributes do not completely fill the requirements to manage and distinguish health professionals, subjects of care, organizations and other health entities engaged in healthcare communications and security decisions. The increasing use of networks for the communication and management of health information expands the need for healthcare-specific directories to add support of a number of related information and security services. With increased use of internet and intranet-based health information systems, health information will need to be communicated across multiple entities and across unaffiliated entities, using both automated and human-interface based systems. Such distributed health information management and communications require a standard for communications data, healthcare professional directories, and consumer information.

Organizations are increasingly relying on enhanced information technology infrastructures to simplify and enhance user management functions through the use of LDAP and similar services to manage and access a central user repository across multiple systems within an organization. These activities include corporate and institutional directories, definition of systems and services, and definition of partner directories. Distinct from corporate models, in healthcare, such use requires enhanced schema context so as to support in the need to represent healthcare regulatory information, clinical credentials, multiple affiliations at both healthcare professional and organizational levels, unaffiliated members of the organization's healthcare community, consumers, and business partners.

There is also an increased use of directories for user authentication. By creating a single source for user management, healthcare organizations can enhance user identification, authentication, and exit process user identity removal. By providing a 'single sign-on' capability, better password security can be encouraged.

Directories may also be leveraged to communicate user attributes for authorization decisions for security infrastructure management. Associating healthcare related attributes, such as healthcare role and specialties, support enhanced associated privilege granting, privilege removal, role management,

and access control. However, while this is a powerful tool for enhanced security, the complexity of the directory and inter-directory requirements is increased.

Another security service of the healthcare directory is to support healthcare PKI efforts. Such services utilize the directory for public key storage and access, as well as PKI services support such as CRL storage and access. Both the PKI and enhanced security service support add to the complexity of the healthcare directory through additional object support requirements for servers, application components, and devices.

There are multiple types of directory implementations that may be supported by this International Standard. There is no requirement that a directory service support all options. The optionality is provided to allow for a communication domain to establish the a directory supporting the relevant healthcare organizations, persons, or devices. Provider directories may be implemented to support scheduling communications, notifications, provider-provider communications, and many other functions. Provider directories may be leveraged for implementations of credential verification supporting communication of sanction and credential status information. Service directories may support public or provider queries such as identifying a specialist within a specified geographic area. Directories supporting communications with subjects of care will require substantial access control protections, and as such should be separately managed from provider directories. Such directories may be leveraged in support of social services activities. These are just some of the applicability of healthcare directories. Additional use cases can be found in Annex A of this International Standard.

5.2 Healthcare persons

While the X.500 standards include multiple object classes to represent persons as individuals and employees, there are no standard attributes within these object classes to represent key healthcare-specific information required to support industry communications and services. The healthcare community needs to represent within the directory professional information such as credentials, healthcare identifiers, role-specific information, and healthcare-specific contact information. Contact information in healthcare is more complex than in typical business environments due to the nature of multiple affiliations discussed in the next section. Healthcare persons include:

— regulated healthcare professionals;

— non-regulated healthcare professionals;

— employees of healthcare organizations and supporting organizations;

— subjects of care.

The inclusion of the subjects of care supports potential uses such as personal health records, patient portals, or other such healthcare-specific endeavours in which large numbers of patients require online identification and authentication services. Supporting inclusion of the subjects of care requires a balance of core directory information, subject of care identifying information, and confidentiality in compliance with underlying policy, for example compliance with permitted purposes of use. Implementations of directories supporting such capabilities for the subjects of care should be separately managed from provider directories.

5.3 Multiple affiliations

Healthcare persons, in many environments, may be affiliated with multiple organizations. These persons may serve different functions under each of the organizations with which they are affiliated. Many healthcare professionals operate independently, but are allowed practicing privileges within one or many organizations. Similarly, supporting services may be provided to multiple healthcare organizations. Within an organization, an individual may operate under differing roles depending upon the care setting or other factors. Healthcare consumers typically seek services from numerous healthcare professionals and organizations. In order to minimize inaccuracies associated with duplicate management of information, the healthcare schema shall allow for links to primary management sources in support of multiple affiliations.

Another important factor is that healthcare staff are also healthcare consumers, and their professional identities should be distinct from their healthcare consumer identity. From the perspective of appropriate use, it is important that healthcare staff and their associated professional identities be separate from their personal identities as the purposes of use are different in the different roles or contexts.

5.4 Healthcare organizations

While X.500 provides object classes for organizations, there are insufficient attributes within these constructs to represent healthcare-specific information needed to support the healthcare directory requirements. Healthcare-specific information includes:

— regulatory identifiers;

— class of service provided;

— service locations;

— contact information for key information management functions.

Healthcare organizations include:

— regulated healthcare organizations (i.e. hospitals, pharmacies, clinics, mobile units, skilled nursing facilities, specialty units);

— payers, supporting organizations (i.e. suppliers, transcription services, coding services, claims processing services);

— regulatory/monitoring agencies (i.e. professional colleges, disease control, drug control, public health)

5.5 Hardware/software

While X.500 provides object classes for servers and applications, healthcare devices and software are subject to regulation and validation requirements and therefore should include additional attributes to properly represent healthcare directory requirements. PDAs and other devices may also have specific associations with other entities within the healthcare directory. The representation of hardware and software in the directory is limited to the identification and communication parameters of these, and association of these with individuals and organizations. The directory may be used for asset identification but should not be relied upon for asset management.

5.6 Healthcare security services

Healthcare certification authorities, attribute authorities and registration authorities need to be represented within the directory, and need to be able to publish relevant key management information. Support for healthcare role management within the directory shall be able to represent healthcare-specific components. This includes the representation of job function, job-specific contact information and certificates (both professional and attribute certificates) associated with a healthcare person. This does not include direct support for the representation of functional roles.

6 Directory security management framework

Healthcare needs to be supported by a framework of strong security management policies so as to assure the integrity of communications data and the authentication infrastructure. There are already such strong practice principles defined in international standards. While the following standards are not directory specific, they should be adhered to for the protection of directory infrastructures:

— ISO/IEC 27000;

— ISO/IEC 27001;

— ISO 27799;

— ISO/IEC 27005;

— COBIT specification produced by the Information Systems Audit and Control Foundation.

7 Interoperability

7.1 Requirements

Healthcare directories shall be able to contact and/or exchange relative information from directories of various trading partners. Techniques include chaining, replication, referrals and unilateral or bi-lateral trust between the directories. Some of these techniques will be sensitive to schema inconsistencies depending upon the application or service. The following hierarchy requirements apply to the interoperability models:

a) shall be able to physically separate the healthcare client base/community into a controlled, high-service environment;

b) shall be able to provide replication and load-balancing management;

c) shall be able to limit the search tree to a specific geographical or logical area in order to provide efficient access performance (i.e. 80/20 rule);

d) shall be able to organize DIT to facilitate access control management to protect confidential information stored in the directory (e.g. subject of care certificates shall not be publicly accessible) through branch-point references;

e) shall be able to organize the DIT to enable distributed access to healthcare jurisdictions.

7.2 Name space/tree structure

In order to address these requirements in a consistent manner, and in order to adhere to existing healthcare regulatory jurisdictions, the following high-level name space and tree structure should be available.

7.2.1 Country

In all cases, the country of the healthcare professional jurisdiction shall be available and shall be the top of the tree. In the case where an organization operates in multiple countries, there shall be a view available that subjugates the organization to the healthcare regulatory jurisdiction.

c=Required

7.2.2 Locality

In those jurisdictions where Locality represents a regulatory jurisdiction (i.e. each state in the case of the US), Locality shall be used to delineate the region of healthcare regulatory jurisdiction.

l=Optional

7.2.3 Organization

Organization shall be used to indicate the healthcare regulatory jurisdiction issuing authority under which the healthcare professionals in the directory are authorized. Organization may also be used to represent healthcare professional organizations and institutions, healthcare provider organizations, and research organizations.

o=Required (issuing authority, healthcare professional organizations)