TECHNICAL SPECIFICATION

ISO/TS 21091

First edition
2005-12-15

Health informatics — Directory services for security, communications and identification of professionals and patients

Informatique de santé — Services d'annuaires pour la sécurité, les communications et l'identification des patients et des professionnels

Reference number
ISO/TS 21091:2005(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.

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order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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 21091 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

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

The directory is becoming an increasingly popular method of providing a means for single sign-on capabilities. This goal has driven directory schema extensions to include organization employee management information, health care-specific contact information and health care identifiers. This Technical Specification will review the health care specific requirements of the directory, and define, as appropriate, standard specifications for inclusion of this information in the health care directory.

Health informatics — Directory services for security, communications and identification of professionals and patients

1 Scope

This Technical Specification defines minimal specifications for directory services for health care using the X.500 framework. This Technical Specification provides the common directory information and services needed to support the secure exchange of health care information over public networks. This Technical Specification addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction, and international health care communications. Besides technical security measures that are discussed in other ISO standards, communication of health care data requires a reliable accountable "chain of trust." In order to maintain this chain of trust within a public key infrastructure, users (relying parties) must be able to obtain current correct certificates and certificate status information through secure directory management.

In addition to the support of security services such as access control and confidentiality, a standard shall provide specification for other aspects of communication, such as addresses and protocols of communication entities.

This Technical Specification also supports directory services aiming to support identification of health professionals and organizations and the patients/consumers. The latter services include aspects sometimes referred to as master patient indices.

The health care directory will only support standard LDAP Client searches. Specific implementation guidance, search criteria and support are out of scope of this document.

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.

ITU-T Recommendation X.500:2001 | ISO/IEC 9594-1:2001, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services – Part 1*

ITU-T Recommendation X.501:2001 | ISO/IEC 9594-2:2001, *Information technology – Open Systems Interconnection – The Directory: Models – Part 2*

ITU-T Recommendation X.511:2001 | ISO/IEC 9594-3:2001, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition – Part 3*

ITU-T Recommendation X.520:2001 | ISO/IEC 9594-6:2001, *Information technology – Open Systems Interconnection – The Directory: Selected Attribute Types – Part 6*

ITU-T Recommendation X.521:2001 | ISO/IEC 9594-7:2001, *Information technology – Open Systems Interconnection – The Directory: Selected Object Classes – Part 7*

IETF/RFC 3771:2004, *The Lightweight Directory Access Protocol (LDAP) Intermediate Response Message*

IETF/RFC 3377:2002, *Lightweight Directory Access Protocol (v3): Technical Specification*

IETF/RFC 3698:2004, *Lightweight Directory Access Protocol (LDAP): Additional Matching Rules*

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
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2]

3.3
attribute authority
AA
authority that assigns privileges by issuing attribute certificates

[X.509]

3.4
attribute certificate
data structure, digitally signed by an attribute authority, that binds some attribute values with identification about its holder

[X.509]

3.5
authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

NOTE See also data origin authentication and peer entity authentication.

[ISO 7498-2]

3.6
authorization
granting of rights, including the granting of access based on access rights

[ISO 7498-2]

3.7
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2]

3.8
certificate
public key certificate

3.9
certificate distribution
act of publishing certificates and transferring certificates to security subjects

3.10
certificate issuer
authority trusted by one or more relying parties to create and assign certificates

NOTE Optionally the certification authority may create the relying parties' keys.

[ISO/IEC 9594-8]

3.11
certificate management
procedures relating to certificates such as: certificate generation, certificate distribution, certificate archiving and revocation

3.12
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 the time and date are within the certificate validity period

3.13
certificate revocation list
CRL
published list of the suspended and revoked certificates (digitally signed by the CA)

3.14
certificate verification
verifying that a certificate is authentic

3.15
certification authority
CA
entity that issues certificates by signing certificate data with its private signing key

NOTE Authority in the certification authority term does not imply any government authorization, only that it is trusted. Certificate issuer may be a better term but CA is used very broadly.

3.16
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO 7498-2]

3.17
data integrity
property that data have not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

3.18
digital signature
data appended to, or a cryptographic transformation (see cryptography) 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]

3.19
identification
performance of tests to enable a data processing system to recognize entities

[ISO/IEC 2382-8]

3.20
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[ENV 13608-1]

3.21
integrity
proof that the message content has not altered, deliberately or accidentally in any way, during transmission

[ISO 7498-2]

3.22
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2]

3.23
key management
generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy

[ISO 7498-2]

3.24
lightweight directory access protocol
LDAP
standard access protocol for directories allowing public or controlled access to certificates and other information needed in a PKI

3.25
object identifier
OID
unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class

3.26
patient/consumer
person who is the receiver of health related services and who is a person in a health information system

3.27
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]

3.28
private key
key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)

[ISO 10181-1]

3.29
public key
key that is used with an asymmetric cryptographic algorithm and that can be made publicly available

[ISO 10181-1]

3.30
public key certificate
public key certificates (PKCs) [X.509] that bind an identity and a public key

NOTE The identity can be used to support identity-based access control decisions after the client proves that they have access to the private key that corresponds to the public key contained in the PKC.

[IETF/RFC 3280]

3.31
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

3.32
relying party
recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate

[IETF/RFC 3647]

3.33
role
set of competencies and/or performances that are associated with a task

3.34
security
combination of availability, confidentiality, integrity and accountability

[ENV 13608-1]

3.35
security policy
plan or course of action adopted for providing computer security

[ISO/IEC 2382-8]

3.36
security service
service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[ISO 7498-2]

3.37
subject
entity whose public key is certified in the certificate

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 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.

3.40
X.509
ITU-T Standard X.509 for certificates and their corresponding authentication framework

4 Symbols (and abbreviated terms)

CA Certification Authority

CRL Certificate Revocation List

DAP Directory Access Protocol

DIT Directory Information Tree

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

TTP Trusted Third Party

5 Health care context

5.1 General

In order to accommodate health care-specific concerns, the health care directories must be extended. The increasing use of networks for the communication and management of health information expands the need for health care-specific directories and 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, health care professional directories and consumer information.

Organizations are increasingly reliant on enhanced information technology infrastructures to simplify and enhance user management functions through the use of LDAP in order 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 health care, such use requires enhanced schema context so as to support the need to represent health care regulatory information, clinical credentials, multiple affiliations at both health care professional and organizational levels, unaffiliated members of the organization's health care community, consumers and business partners.

There is also an increased use of directories for user authentication and security infrastructure management. By creating a single source for user management, health care organizations can enhance user identification and authentication security, exit process privilege removal, role management and access control. By providing a "single sign-on" capability, better password security can be encouraged. 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 health care directory is to support health care PKI efforts. Such services utilizes 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 health care directory through additional object support requirements for servers, application components and devices.

5.2 Health care 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 health care-specific information required to support industry communications and services. The health care community needs to represent, within the directory, professional information such as credentials, health care identifiers, role-specific information and health care-specific contact information. Contact information in health care is more complex than in typical business environments due to the nature of multiple affiliations discussed in 5.3. Health care persons include:

- regulated health care professionals;
- non-regulated health care professionals;
- employees of health care organizations and supporting organizations;
- health care consumers.

The inclusion of the health care consumer requires a balance of core directory information, MPI Information and confidentiality.

5.3 Multiple affiliations

Health care 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 health care professionals operate independently, but are allowed practicing privileges within one or many organizations. Similarly, supporting services may be provided to multiple health care organizations. Within an organization an individual may operate under differing roles depending upon the care setting or other factors. Health care consumers typically seek services from numerous health care professionals and organizations. In order to minimize inaccuracies associated with duplicate management of information, the health care schema must allow for links to primary management sources in support of multiple affiliations. Health care staff are also health care consumers, and their professional identities should be distinct from their health care consumer identity.

5.4 Health care organizations

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

— regulatory identifiers;

— class of service provided;

— service locations;

— contact information for key information management functions.

Health care organizations include:

— regulated health care 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. disease control, drug control, public health).

5.5 Hardware/software

While X.500 provides object classes for servers and applications, health care devices and software are subject to regulation and validation requirements, and therefore should include additional attributes to properly represent health care directory requirements. PDAs and other devices may also have specific associations with other entities within the health care 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 Health care security services

Health care 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 health care role management within the directory must be able to represent health care specific components. This includes the representation of job function, job-specific contact information and certificates (both professional and attribute certificates) associated with a health care person. This does not include direct support for the representation of functional roles.

6 Directory security management framework

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

— ISO 22600-2[3];

— ISO/IEC TR 13335-1[7];

— COBIT (Control Objectives for Information and Related Technologies) specification produced by the Information Systems Audit and Control Foundation.

While specific security measures and access control specifications are outside the scope of this Technical Specification, due to the sensitive nature of health related and privacy information that may be supported through the directory services, significant controls must be enabled at branch, object classes and attribute levels. Processes and procedures must be in place to assure accountability and information integrity represented within the health directory. We anticipate that appropriate access controls managing who can read, write or modify all items in the health care directory.

7 Interoperability

7.1 Requirements

Health care directories must 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 considerations apply to the interoperability models.

a) Must be able to physically separate the health care client base/community into a controlled, high-service environment.

b) Must be able to provide replication and load-balancing management.

c) Must 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) Must be able to organize DIT to facilitate access control management to protect sensitive information stored in the directory (e.g. patient certificates must not be publicly accessible) through branch-point references.

e) Must be able to organize the DIT to enable distributed access to health care jurisdictions.

7.2 Name space/tree structure

7.2.1 General

In order to address these requirements in a consistent manner, and in order to adhere to existing health care regulatory jurisdictions, the high-level name space and tree structure described in 7.2.2 to 7.2.7 should be available.

7.2.2 Country

In all cases, the country of the health care 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 health care regulatory jurisdiction.

c = Required

7.2.3 Locality

In those countries where locality represents a regulatory jurisdiction (i.e. each state in the case of the USA), locality shall be used to delineate the region of health care regulatory jurisdiction.

l = Optional