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)

COPYRIGHT PROTECTED DOCUMENT

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)

7.2.4 Organization unit

In those jurisdictions where the issuing authority is further broken down by Issuing Authority Professional Branch, this Organization shall be sub-categorized by Organization Unit for those jurisdictions that maintain multiple professional authority branches. For instance, in many jurisdictions, pharmacists, physicians, dentists may each be managed through a separate government body or department.

ou=Optional

7.2.5 Structural roles

At each of the levels in the hierarchy, there may exist both Standard Structural Roles, and Locally-Defined Structural Roles. Structural Role concepts are described further in Clause 9 of this International Standard.

7.2.6 Multiple instantiations of individuals

A person within the system may be represented more than once, where that person has multiple healthcare identities in the context of professional credentials, or in the context of associations with multiple healthcare organizations, or other such cases where multiple representations may be appropriate. The separations and information representations for these persons represented by multiple healthcare identities are supported through the object classes and directory information tree (see Figure 1), but the object classes alone do not assure that the desired separation is accomplished. The distinct Common Name structure, however, does enable such separation through instantiation of multiple instances of that individual in each health identity.

Within healthcare, there is a need to enable and represent control over the information components of the healthcare identity by the different regulating bodies. Individuals are represented with validly different contact and administrative information by different regulatory bodies. For instance, the contact information and basic communication information for each licence type and jurisdiction may have conflicting attribute content due to such issues as multiple residences. The independent instantiations of these across multiple jurisdictions in the same directory shall be preserved. An individual may exist in the directory both as a subject of care and as a provider. It is also important to separate an individual's personal and professional instantiation within the directory to assure appropriate use of data. It is recognized that this may violate the concept of having a single entry in the directory for a given person, but to appropriately represent the individual's healthcare identity, it is a correct representation reflection of the fact that a given person may have multiple healthcare identities. For instance, a physician may have practicing privileges in multiple jurisdictions, and be known to those jurisdictions under distinct identifiers, and in some cases, under distinct addresses. While the DIT described enables the representation of all health individuals, organizations and device actors, it does not require that these all be contained within the same physical or logical information space. These may be separated for optimal service performance and architectural design as necessary. A given healthcare directory may contain some, all, or none of the defined actors, and this may be instantiated using centralized and decentralized methods.

A regulated health professional need be instantiated only once in any given jurisdiction. Through the use of the HCOrganizationalRole described below, this instantiation may be represented in numerous organizational capacities through the use of the attribute RoleOccupant, which will contain the DN of the professional. Using this construct, job-specific contact information may be retrieved.

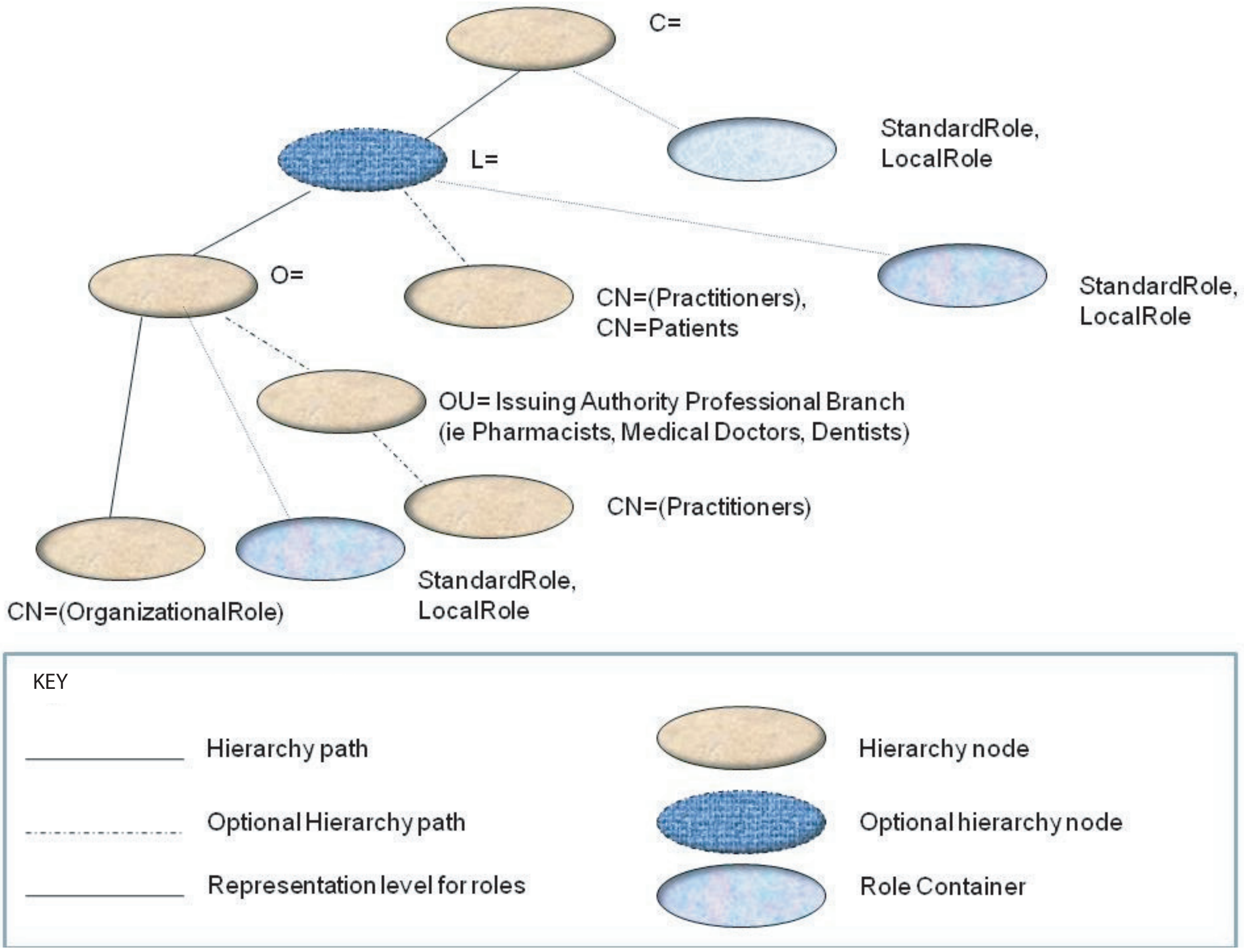

Figure 1 — Directory information tree (DIT) for healthcare

8 Healthcare schema

8.1 Healthcare persons

8.1.1 General

Multiple types of individuals are represented in the healthcare directory. The identity of each individual within the system should be represented once except where it may be appropriate to do otherwise. An example of such an exception is that a healthcare professional, when interacting with the healthcare system as a subject of care, may be represented by two object classes: one that contains profession-specific information, and another that contains subject of care-specific information. These shall all have a parent class of person, and shall be specialized accordingly so as to represent the following types of individuals: Healthcare Consumer, Healthcare Professional, and Healthcare Employee. Information attributes specific to each of the object classes shall be added as a specialization of the base object class. Support for the healthcare consumer is intended for identification and not for direct clinical care support. Healthcare professional support includes the ability to flag the practitioner with sanction indicators, credential restrictions, and other such warnings.

The object class schemas that follow include definitions for extended attributes, and include:

Attribute The name of the new attribute to be supported

OID The ISO/TC 215 assigned object identifier associated with the new attribute

Description A description of the new attribute

Syntax The LDAP supported syntax to be used in representing the attribute

Matching Rules Matching rules to be used by servers to compare attribute values against assertion values when performing Search and Compare operations

Multi-Valued An indication as to whether there is support expected for representing multiple values for the attribute

The schema extension specifications also include information as to which of the additional attributes are mandatory and which are optional. Matching rules are described in X.520|ISO/IEC 9594-6.

8.1.2 Subjects of Care (Healthcare Consumer)

Object Class HCSubjectOfCare

Superior Object Class: Person

OID: 1.0.21091.1.1.1

Object Class Type: Structural

Mandatory attributes:

Attribute	**OID**	**Description**	**Syntax**	**Matching rules**	**Multi-Valued**
HcSubjectOfCareID	1.0.21091.2.1.29	This may be an identifiable, anonymous, or pseudonymous identifier. (Issuing Authority:Type:ID)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

Using this construct, HcSubjectOfCareID can be used to represent any identifier, including, but not limited to a pseudonymous ID, citizenship number, health insurance number, medical record number, and driving licence number. A locally defined coding system may alternatively or additionally be employed.

There are attributes listed in this table that are strictly prohibited or restricted by some jurisdictions. It is important that each of the attributes be reviewed by the responsible person(s) to determine whether or not each attribute is required and legally permitted in the directory and which user and which role is permitted to have access to each of these attributes.

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIdentificationService	1.0.21091.2.0.2	Location of service(s) offering identification such as a subject of care identification cross reference service (PIX), e-authentication services, biometric identification, or other identity verification service	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcSigningCertificate	1.0.21091.2.0.3	Public key and certificate for the user's non-repudiation signing certificate used for health transactions	Binary	Certificate Exact Match and certificate Match	Yes
HcAttributeCertificate	1.0.21091.2.0.4	Used for credentials, power of attorney, healthcare decision maker, etc. Populated with P7 formatted certificate.	Binary	Certificate Exact Match and certificate Match	Yes
HcMPILocation	1.0.21091.2.1.2	Location of the Master Patient Index Service(s) available	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcMedicalHome	1.0.21091.2.1.4	Location of the organization or practitioner serving as the subject of care's medical home	Directory String	Case Ignore Match, Case Ignore Substrings Match	No
HcPHRLocation	1.0.21091.2.1.9	Location of the subject of care's personal health record	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcSubstituteDecision Maker	1.0.21091.2.1.3	Record entry of person(s) able to sign/act on behalf of the subject	DN	Distinguished Name Match	Yes
HcMothersMaidenName	1.0.21091.2.1.30	The subject of care's Mother's Maiden Name	Directory String	Case Ignore Match, Case Ignore Substrings Match	No
HcDateTimeofBirth	1.0.21091.2.1.31	The subject of care's Date and Time of Birth	ISO 8601 Date	Generalized Time Match Generalized Time Ordering Match	No
HcSex	1.0.21091.2.1.32	The subject of care's Administrative Sex. Populate with classifications as described in ISO/TS 22220	Directory String	Case Ignore Match, Case Ignore Substrings Match	No
HcPatientAlias	1.0.21091.2.1.33	The subject of care's Patient Alias	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcCountyCode	1.0.21091.2.1.34	The subject of care's County Code	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcReligion	1.0.21091.2.1.35	The HL-7 defined Religion. NOTE: There are jurisdictions where use of this attribute this is strictly prohibited	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcBirthPlace	1.0.21091.2.1.36	The subject of care's Birth Place	Directory String	Case Ignore Match, Case Ignore Substrings Match	No

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcPatientDeathDateand Time	1.0.21091.2.1.37	The subject of care's Patient Death Date and Time	Date	Generalized Time Match Generalized Time Ordering Match	No
HcMultipleBirth	1.0.21091.2.1.38	The subject of care's indication whether the patient was part of a multiple birth	Directory String	Case Ignore Match, Case Ignore Substrings Match	No
HcMultipleBirthOrder	1.0.21091.2.1.39	The subject of care's number representing the patient's order of birth	Directory String	Case Ignore Match, Case Ignore Substrings Match	No
preferredDelivery Method	2.5.4.28	RFC2256: preferred delivery method	1.3.6.1.4. 1.1466. 115.121.1. 14		No
St	2.5.4.8	State or Province	Directory String	caseIgnoreMatch	Yes
telexNumber	2.5.4.21	Telex Number	Telex Number		Yes
L	2.5.4.7	Locality Name	Directory String	caseIgnoreMatch	Yes
postalCode	2.5.4.17	Postal Code	Directory String	caseIgnoreMatch	Yes
Street	2.5.4.9	RFC2256: street address of this object	Directory String	caseIgnoreMatch	Yes
postalAddress	2.5.4.16	RFC2256: postal address	Postal Address	caseIgnoreList Match	Yes
facsimileTelephone Number	2.5.4.23	RFC2256: Facsimile (Fax) Telephone Number	Facsimile Telephone Number		Yes
telephoneNumber	2.5.4.20	RFC2256: Telephone Number	Telephone Number	telephoneNumber Match	Yes
teletexTerminalIdentifier	2.5.4.22	RFC2256: Teletex Terminal Identifier	1.3.6.1.4. 1.1466. 115 .121. 1.51		Yes
postOfficeBox	2.5.4.18	RFC2256: Post Office Box	Directory String	caseIgnoreMatch	Yes
destinationIndicator	2.5.4.27	RFC2256: destination indicator	Printable String	caseIgnoreMatch	Yes
userCertificate	2.5.4.36	RFC2256: X.509 user certificate use; binary	Certificate		Yes
uid	0.9.2342.19200300. 100.1.1	RFC1274: user identifier	Directory String	caseIgnoreMatch	Yes
homePostalAddress	0.9.2342.19200300. 100.1.39	RFC1274: home postal address	Postal Address	caseIgnoreList Match	Yes
preferredLanguage	2.16.840.1.113730.3.1.39	RFC2798: preferred written or spoken language for a person	Directory String	caseIgnoreMatch	No
mail	0.9.2342.19200300.100.1.3	RFC1274: RFC822 Mailbox	IA5 String	caseIgnoreIA5 Match	Yes
homePhone	0.9.2342.19200300. 100.1.20	RFC1274: home telephone number	Telephone Number	telephoneNumber Match	Yes
roomNumber	0.9.2342.19200300. 100.1.6	RFC1274: room number	Directory String	caseIgnoreMatch	Yes
x500UniqueIdentifier	2.5.4.45	RFC2256: X.500 unique identifier	Bit String	bitStringMatch	Yes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
photo	0.9.2342.19200300.100.1.7	RFC1274: photo (G3 fax)	1.3.6.1.4.1.1466.115.121.1. 23		Yes
businessCategory	2.5.4.15	RFC2256: business category	Directory String	caseIgnoreMatch	Yes
pager	0.9.2342.19200300.100.1.42	RFC1274: pager telephone number	Telephone Number	telephoneNumber Match	Yes
jpegPhoto	0.9.2342.19200300.100.1.60	RFC2798: a JPEG image	JPEG		Yes
audio	0.9.2342.19200300.100.1.55	RFC1274: audio (u-law)	Audio		Yes
userPKCS12	2.16.840.1.113730.3.1.216	RFC2798: PKCS #12 PFX PDU for exchange of personal identity information	Binary		Yes
displayName	2.16.840.1.113730.3.1.241	RFC2798: preferred name to be used when displaying entries	Directory String	caseIgnoreMatch	no
mobile	0.9.2342.19200300.100.1.41	RFC1274: mobile telephone number	Telephone Number	telephoneNumber Match	Yes
labeledURI	1.3.6.1.4.1.250.1.57	RFC2079: Uniform Resource Identifier with optional label	Directory String	caseExactMatch	Yes
carLicense	2.16.840.1.113730.3. 1.1	RFC2798: vehicle license or registration plate	Directory String	caseIgnoreMatch	Yes
givenName	2.5.4.42	RFC2256: common supertype of name attributes	Directory String	caseIgnoreMatch	Yes
userSMIMECertificate	2.16.840.1.113730.3.1.40	RFC2798: PKCS#7 SignedData used to support S/MIME	Binary		Yes
initials	2.5.4.43	RFC2256: common supertype of name attributes	Directory String	caseIgnoreMatch	Yes

Optional representation for PIDS attributes using parent class and extended attributes:

The following attributes from ISO/HL7 27931, *Data Exchange Standards — Health Level Seven Version 2.5 — An application protocol for electronic data exchange in healthcare environments*, should be populated with the referenced schema attribute using the defined ISO/HL7 27931 formatting within the relevant constraints of the referenced LDAP attribute:

HL7 PIDS Attribute	**inetOrgPerson/HcSubjectOfCare Attribute**
Patient Name	Include the XPN formatted name in cn as a second cn value
Phone Number - Home	homePhone
Phone Number - Business	telephoneNumber
Primary Language	preferredLanguage
Patient Address	homePostalAddress
Patient Account Number	Use HcSubjectOfCareID if needed
SSN Number - Patient	Use HcSubjectOfCareID if needed
Driver’s License Number – Patient	Use HcSubjectOfCareID if needed

8.1.3 Healthcare Professional

Object Class: HCProfessional

Superior Object Class: InetOrgPerson

OID: 1.0.21091.1.2

Object Class Type: Structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIdentifier	1.0.21091.2.0.1	The healthcare identifier. Where this is a regulated healthcare professional, this shall minimally contain an entry indicating the identifier assigned by the regulating authority (Issuing Authority:Type:ID:Status)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcProfession	1.0.21091.2.2.1	Text representation of the user profession (Issuing Authority: Code System: Code)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcRegistrationStatus	1.0.21091.2.2.40	Condition flag indicating the status of the regulatory credential restrictions, or other sanction indicators	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIdentificationService	1.0.21091.2.0.2	Location of service(s) offering biometric or other identification verification service	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcSigningCertificate	1.0.21091.2.0.3	Public key and certificate for the user's non-repudiation signing certificate used for health transactions	Binary	Certificate Exact Match and certificate Match	Yes
HcAttributeCertificate	1.0.21091.2.0.4	Used for credentials, certifications, education degrees, etc. Populated with P7 formatted Certificate.	Binary	Certificate Exact Match and certificate Match	Yes
HcRole	1.0.21091.2.0.5	(Issuing Authority: Code System: Code) Populate with ISO/TS 21298 defined roles. May also be populated with other roles specified by jurisdiction or organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcSpecialisation	1.0.21091.2.0.6	(Issuing Authority: Code System: Code) Populate with ISO/TS 21298 defined medical specialties. May also be populated with other specialties specified by jurisdiction or organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcPrincipalPractice Location	1.0.21091.2.2.3	Use DN of the organization	DN	Distinguished Name Match	No
HcPracticeLocation	1.0.21091.2.2.4	Use DN of the organization	DN	Distinguished Name Match	Yes

8.1.4 Employees

Object Class:	HCEmployee
Superior Object Class:	InetOrgPerson
OID:	1.0.21091.1.3
Object Class Type:	Structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIdentifier	1.0.21091.2.0.1	The healthcare identifier. The issuing authority may be the employer (Issuing Authority: ID)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIdentificationService	1.0.21091.2.0.2	Location of service(s) offering biometric or other identification verification service	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcSigningCertificate	1.0.21091.2.0.3	Public key and certificate for the user's non-repudiation signing certificate used for health transactions	Binary	Certificate Exact Match and certificate Match	Yes
HcAttributeCertificate	1.0.21091.2.0.4	Used for credentials, certifications, education degrees, etc. Populated with P7 formatted certificate.	Binary	Certificate Exact Match and certificate Match	Yes
HcRole	1.0.21091.2.0.5	(Issuing Authority: Code System: Code) Populate with ISO/TS 21298 defined roles. May also be populated with other roles specified by jurisdiction or organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcOrganization	1.0.21091.2.3.1	Used to indicate organization DN of organization	DN	Distinguished Name Match	Yes

For employees that are non-regulated healthcare professionals, there will be an instantiation for each healthcare organization for which that individual is employed. Regulated health professionals will be represented through the HCOrganizationalRole described in 8.3.1.

8.2 Organization identities

Organizations shall be represented by an object class containing organization-specific information. This information shall include all variables required for the conduct of healthcare administrative and clinical functions. The following types of organizations shall be represented within the directory:

a) Regulated Healthcare Organization;

b) Payers;

c) Supporting Organizations and Regulatory Agencies.

Each organization type shall be further specialized as needed to accommodate healthcare-specific requirements for these trading partners. For instance, a payer may be specialized so as to include a national payer identification number. Employers may include a national employer identification number. Small physician practices shall be considered a Regulated Healthcare Organization so as to appropriately accommodate all relevant office staff. Agencies are represented as a Supporting Organization. Organization is described in Annex B.

8.2.1 Regulated Healthcare Organization

Object Class: HCRegulatedOrganization

Superior Object Class: Organization

OID: 1.0.21091.1.4

Object Class Type: structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIdentifier	1.0.21091.2.0.1	The healthcare identifier. The issuing authority may be the employer (Issuing Authority: ID)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcSigningCertificate	1.0.21091.2.0.3	Public key and certificate for the user's non-repudiation signing certificate used for health transactions	Binary	Certificate Exact Match and certificate Match	Yes
HcAttributeCertificate	1.0.21091.2.0.4	Used for credentials, certifications, etc. Populated with P7 formatted certificate.	Binary	Certificate Exact Match and certificate Match	Yes
HcSpecialisation	1.0.21091.2.0.6	(Issuing Authority: Code System: Code) Populate with ISO/TS 21298 defined medical specialties. May also be populated with other specialties specified by jurisdiction or organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
EdiAdministrative Contact	1.0.21091.2.0.7	The entry for the individual responsible for EDI administration	DN	Distinguished Name Match	Yes
ClinicalInformation Contact	1.0.21091.2.0.8	The entry for the individual to contact with clinical issues	DN	Distinguished Name Match	Yes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcOrganization Certificates	1.0.21091.2.0.9	Used for storing healthcare organization certificates	Binary	Certificate Exact Match and certificate Match	Yes
HcClosureDate	1.0.21091.2.0.10	Date of closure of the organization or date when the organization changed name/affiliation	Date	Generalized Time Match Generalized Time Ordering Match	No
HcSuccessorName	1.0.21091.2.0.11	DN of Successor Entry	DN	Distinguished Name Match	Yes
HcRegisteredName	1.0.21091.2.4.1	The legal name of the entity as registered with the healthcare regulating authority	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcRegisteredAddr	1.0.21091.2.4.2	The address as registered with the regulatory authority. This shall be structured the same as PostalAddress	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcServiceLocations	1.0.21091.2.4.3	Healthcare organizations where healthcare services are rendered	DN	Distinguished Name Match	Yes
HcOperatingHours	1.0.21091.2.4.4	Hours of operation of the organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcSigningCertificate	1.0.21091.2.0.3	Public key and certificate for the user's non-repudiation signing certificate used for health transactions	Binary	Certificate Exact Match and certificate Match	Yes

8.2.2 Payer Organizations

Object Class: HCPayer

Superior Object Class: Organization

OID: 1.0.21091.1.5

Object Class Type: Structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIdentifier	1.0.21091.2.0.1	The healthcare Identifier. The issuing authority may be the employer (Issuing Authority: ID)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcSigningCertificate	1.0.21091.2.0.3	Public key and certificate for the user's non-repudiation signing certificate used for health transactions	Binary	Certificate Exact Match and certificate Match	Yes
HcAttributeCertificate	1.0.21091.2.0.4	Used for credentials, certifications, etc. Populated with P7 formatted certificate.	Binary	Certificate Exact Match and certificate Match	Yes
EdiAdministrative Contact	1.0.21091.2.0.7	The entry for the individual responsible for EDI administration	DN	Distinguished Name Match	Yes
ClinicalInformation Contact	1.0.21091.2.0.8	The entry for the individual to contact with clinical issues.	DN	Distinguished Name Match	Yes
HcOrganization Certificates	1.0.21091.2.0.9	Used for storing healthcare organization certificates. These certificates would be used for secure communications with the organization or organization departments rather than specific individuals within the organization	Binary	Certificate Exact Match and certificate Match	Yes
HcClosureDate	1.0.21091.2.0.10	Date of closure of the organization or date when the organization changed name/affiliation	Date	Generalized Time Match Generalized Time Ordering Match	No
HcSuccessorName	1.0.21091.2.0.11	DN of successor entry	DN	Distinguished Name Match	Yes
HcPayerProductID	1.0.21091.2.5.1	Name of Assigning Authority:payers plan:ID	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcOperatingHours	1.0.21091.2.4.4	Hours of operation of the organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

8.2.3 Supporting Organizations (including agencies)

Object Class: HCSupportingOrganization

Superior Object Class: Organization

OID: 1.0.21091.1.6

Object Class Type: Structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIdentifier	1.0.21091.2.0.1	The healthcare Identifier. The issuing authority may be the employer (Issuing Authority: ID)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcSigningCertificate	1.0.21091.2.0.3	Public key and certificate for the user's non-repudiation signing certificate used for health transactions	Binary	Certificate Exact Match and certificate Match	Yes
HcAttributeCertificate	1.0.21091.2.0.4	Used for credentials, certifications, etc. Populated with P7 formatted certificate	Binary	Certificate Exact Match and certificate Match	Yes
EdiAdministrative Contact	1.0.21091.2.0.7	The entry for the individual responsible for EDI administration	DN	Distinguished Name Match	Yes
ClinicalInformation Contact	1.0.21091.2.0.8	The entry for the individual to contact with Clinical issues	DN	Distinguished Name Match	Yes
HcOrganization Certificates	1.0.21091.2.0.9	Used for storing healthcare organization certificates	Binary	Certificate Exact Match and certificate Match	Yes
HcClosureDate	1.0.21091.2.0.10	Date of closure of the organization or date when the organization changed name/affiliation	Date	Generalized Time Match Generalized Time Ordering Match	No
HcSuccessorName	1.0.21091.2.0.11	DN of Successor Entry	DN	Distinguished Name Match	Yes
HcOperatingHours	1.0.21091.2.4.4	Hours of operation of the organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

8.3 Roles, Job Function and Group

8.3.1 Organizational Role Individual

This is the organization-defined job function of an individual employee or contractor. An individual may occupy one or many job functions within an organization. For instance, a physician may work both as a clinician and as an administrator within a hospital. Each of these job functions may have different contact information. It is appropriate to enable clinical communications to be directed to a different location from administrative communications in this example. In order to enable a single identity to occupy multiple job functions at one or many organizations, the schema shall include an object class with no UID, containing an attribute, Role Occupant, of type DN. Note that this schema object is different from Role and is titled as such in order to maintain consistency with the object class which represents this concept, OrganizationalRole. OrganizationalRole and GroupOfNames are described in Annex B.

Object Class:	HCOrganizationalRole
Superior Object Class:	OrganizationalRole
OID:	1.0.21091.1.7
Object Class Type:	Structural

Mandatory attributes:

No additional mandatory attributes are specified.

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcAttributeCertificate	1.0.21091.2.0.4	Used for credentials, certifications, education degrees, etc. Populated with P7 formatted certificate.	Binary	Certificate Exact Match and certificate Match	Yes
HcRole	1.0.21091.2.0.5	(Issuing Authority: Code System: Code) Job-specific Role. Populate with ISO/TS 21298 defined roles. May also be populated with other roles specified by jurisdiction or organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
mail	0.9.2342.19200300.100.1.3	Email address for communications under this role	IA5String	case Ignore IA5String or caseExactIA5String	Yes
HcResponsibleParty	1.0.21091.2.7.1	DN of person or HCOrganizationalRole responsible for this entry (medical staffing, legal review, contract staff, employee)	DN	Distinguished Name Match	Yes

8.3.2 Healthcare Standard Role

Role is a special type of Group intended to represent the multiple types of roles in healthcare. These shall be restricted to standard defined roles. Members of these Roles shall be identified by the DN of the Organizational Role Individual. These roles will be used as a basis for access control definition by applications referring to the directory services for SSL certificate-based authentication. These roles will also be referenced by clinical applications which may restrict some functions based upon user role.

Object Class	HCStandardRole
Superior Object Class:	GroupOfNames
OID:	1.0.21091.1.8
Object Class Type:	Structural

Mandatory attributes:

No additional mandatory attributes defined.

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcRole	1.0.21091.2.0.5	(Issuing Authority: Code System: Code) Populate with ISO/TS 21298 defined roles. May also be populated with other roles specified by jurisdiction or organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcRoleValidTime	1.0.21091.2.0.12	Times in GMT format that the user may act under this role	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcRoleLocation Restriction	1.0.21091.2.0.13	Location restrictions from where the role is valid (i.e. from the Emergency Department only, from IP address, etc.)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

8.3.3 Local Roles

This is used to service organization-defined groups not defined in standards. Most access control requirements should be based upon standard roles. In cases where roles are insufficient to meet the access control requirements, however, groups shall be available to accommodate such special needs.

Object Class:	HCLocalRole
Superior Object Class:	GroupOfNames
OID:	1.0.21091.1.9
Object Class Type:	Structural

Mandatory attributes:

No additional mandatory attributes defined.

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcRole	1.0.21091.2.0.5	(Issuing Authority: Code System: Code) Populate with ISO/TS 21298 defined roles. May also be populated with other roles specified by jurisdiction or organization	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcRoleValidTime	1.0.21091.2.0.12	Times in GMT format that the user may act under this role	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcRoleLocation Restriction	1.0.21091.2.0.13	Location restrictions from where the role is valid (i.e. from the Emergency Department only, from IP address, etc.)	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

8.3.4 Coded References

Healthcare utilizes a number of coded reference files. The directory technology is capable of facilitating communication of this information used by health information management applications. The coded reference information itself is stored as a concatenated value of the code and the associated description in the HcReferenceDescription attribute. The following attributes constitute a new healthcare-specific Object Class:

Object Class:	HCCodedReference
Superior Object Class:	Top
OID:	1.0.21091.1.10
Object Class Type:	Auxiliary

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcIssuingAuthority	1.0.21091.2.10.1	Authority responsible for coding scheme	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcReferenceEffective Date	1.0.21091.2.10.2	Date on which the reference vocabulary is/was effective	Date	Generalized Time Match Generalized Time Ordering Match	No
HcReference Description	1.0.21091.2.10.3	concatenated value:Reference code:Description	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcVocabularyOID	1.0.21091.2.10.4	OID of the healthcare vocabulary used	Object Identifier	Object Identifier Match	No
HcReferenceDateOf Issue	1.0.21091.2.10.5	Date on which the reference vocabulary was issued	Date	Generalized Time Match Generalized Time Ordering Match	No
HcReferenceInvalid Date	1.0.21091.2.10.6	Date on which the reference vocabulary is/was invalid	Date	Generalized Time Match Generalized Time Ordering Match	No
HcReferenceVersion	1.0.21091.2.10.7	Version number of the coded reference	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes

8.3.5 Devices

Device support shall be as described by DICOM Supplement 67: Configuration Management or relevant ISO device specifications with the following additional support for property management:

8.3.6 Addressable Device Property Management

Object Class: HCDevice

Superior Object Class: Top

OID: 1.0.21091.1.11

Object Class Type: Auxiliary

Mandatory attributes:

None of these attributes are mandatory.

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
HcDeviceIssuedTo	1.0.21091.2.11.1	DN of the individual to whom the device has been issued	DN	Distinguished Name Match	No
HcDeviceDateOfIssue	1.0.21091.2.11.2	Date on which the device was issued to the recipient	Date	Generalized Time Match Generalized Time Ordering Match	No
HcDeviceDateRecalled	1.0.21091.2.11.3	Date on which the device was recalled	Date	Generalized Time Match Generalized Time Ordering Match	No
HcDeviceDateRetrieved	1.0.21091.2.11.4	Date on which the device was retrieved	Date	Generalized Time Match Generalized Time Ordering Match	No
HcDeviceCertificate	1.0.21091.2.11.5	Device certificates issued	Binary	Certificate Exact Match and certificate Match	Yes
HcDeviceTracking Number	1.0.21091.2.11.6	(Issuer:Number) Tracking number assigned to the device	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcDevicePhone	1.0.21091.2.11.7	Phone number assigned to the device (i.e. PDA)	Telephone Number	telephone Number-Match and telephone Substrings Number Match	Yes

9 Distinguished Name

9.1 General

The Distinguished Name (of an entry) is the name of an entry which is formed from the sequence of the RDNs of the entry and each of its superior entries. The Relative Distinguished Name (RDN) is a set of one or more attribute type and value pairs, each of which matches a distinct distinguished attribute value of the entry.

A common mistake is to assume that every search of the directory is based on the attributes used in the distinguished name. However, the distinguished name is only a unique identifier for the directory, and you cannot search against it. Instead, you search for entries based on the attribute type-value pairs stored on the entry itself.

9.2 Relative Distinguished Name

9.2.1 General

The Relative Distinguished Name (RDN) is often UID or Common Name. Since it is desirable to represent multiple concepts within this directory, it is important to establish a common unique naming convention within the healthcare domain. This unique RDN shall be composed of a concatenation of Issuing Authority Name and Identifier, using a ':' (colon) as a separator in accordance with WC3 for name spaces such that:

ID=issuing_authority_name:ID

For Health Professionals, the issuing authority is considered to be the regulating body with the authority to manage the health professional's practicing credentials. This enables each country or governing jurisdiction to have a distinguished name for the issuing authority representing the country, state/province, and clinical jurisdiction (i.e. physicians, dentists, pharmacists) as the authority identifier, within which it is anticipated that the authority will maintain a unique identifying system. For chaining, should a separator be needed, the chain shall use '.' as a separator.

9.2.2 Healthcare professionals

9.2.2.1 Directory Identifier

For healthcare professionals, the directory Identifier shall be able to account for the professional with:

— multiple regulated professions;

— multiple practice locations.

9.2.2.2 UID

In order to account for the multiple regulated professions and practice locations that may be associated with a healthcare professional, the UID shall be composed of:

UID = Issuing Authority Identifier : National/Regional Professional Identifier

It is recognized that this may result in multiple instantiations of the same individual in the health directory, but because the health identity is an integral component of the user interaction in the delivery of healthcare, it is appropriate to represent the individual as acting under a specific regulatory body and in accordance with the governing laws of that body at any point in time.

9.2.2.3 Common Name

The Common Name (CN) should preserve the legal name of individual or organization. In order to assure that the uniqueness of Common Name, and the ease of use for individual look-up, the Common Name for Health Professionals shall be composed of:

'Surname, Given Names, UID'

where UID is composed as described in 9.2.2.2.

In the case of multiple surnames, the Common Name should list first the chosen surname. If there are differences in the representation of name in the individual's government issued identifications, the name used shall be the same as that listed by a medical regulatory authority.

There shall be no titles used in the representation of Common Name (i.e. MD, DVM). However, suffixes such as Jr. Sr. II, etc. that distinguish like-named individuals within a family shall be preserved.

9.2.2.4 Use of Multi-valued Common Name

Additional Common Name values may be used to represent the preferred name or usual name of the individual represented.

9.2.3 Health Consumers

9.2.3.1 Representation

Health Consumers may be represented by a number of identifying systems including an anonymous identity. These identifiers may include regional identifier, cross-referencing index identifiers and regional managed systems. The individual may be represented in numerous directory object instantiations. Searching criteria for the consumer shall include the list of PIDS identifying attributes.

9.2.3.2 UID

In order to account for the multiple organizations and entities needing to represent the consumer within their own realm and location, the UID shall be composed of:

UID = Issuing Authority Identifier:National/Regional/Organization/Patient/Person Identifier

It is recognized that this may result in multiple instantiations of the same individual in the health directory, but because the health identity is an integral component of the user interaction in the receipt of healthcare, it is appropriate to represent the individual as acting under a specific identity issuing body. This will necessarily require supporting Patient Identifier Locating Services, and as such, the object class shall contain those variables supporting such search capability. In the case of an anonymous consumer, these variables and identifiers may be reversible or non-reversible pseudonyms and coded values. In order to distinguish a home address, a domicile identifier ID Number may be used either as part of the Common Name or as an optional variable in the HCConsumer Object Class.

9.2.3.3 Common Name

The Common Name should preserve the legal name of an individual or organization. In order to ensure the uniqueness of Common Name, and the ease of use for individual look-up, the Common Name for Health Consumers shall be composed of:

'Surname, Given Names, UID'

where UID is composed as described in 9.2.3.2.

In the case of multiple Surnames, the Common Name should list first the chosen surname. However, suffixes such as Jr. Sr. II, etc. that distinguish like-named individuals within a family shall be preserved.

9.2.3.4 Use of Multi-valued Common Name

Additional Common Name values may be used to represent the preferred name or Usual Name of the individual represented.

9.2.4 Organization

9.2.4.1 UID

The Organization UID shall be composed of:

UID = Issuing Authority Identifier:National/Regional Identifier

It is recognized that this may result in multiple instantiations of the same organization in the health directory, but because the health identity is an integral component of the user interaction in the receipt of healthcare, it is appropriate to represent the organization as acting under a specific identity issuing body.

9.2.4.2 Common Name

The Common Name should preserve the current legal name of organization.

9.2.4.3 Preservation of Legal Organization Name

In the case of transfer of business affiliations, name change, and other successor instances, the successor shall be indicated by the DN of the new entity entry with the current organization legal name. In the case of business closure, the date of closure shall be represented by the HcClosureDate.

9.2.5 Roles/Jobs

9.2.5.1 General

Since one UID may have several jobs or affiliations within the healthcare community, we shall consider this type of object class to be keyed on Common Name (CN), thereby using CN for the RDN of any object class within this concept. The RDN for Role will be Common Name (CN). This name shall be constructed based upon standard structural roles in the case of HCStandardRole:

9.2.5.2 HCOrganizationalRole

The use of the object class HC is intended as a representation of a special structural role expressing relationships and job title. This is not intended to support privilege management, rather it is intended for job-specific contact information and attributes. Naming for this will be:

CN.job_function@organization**_domain_name**

where CN is the CN of the individual, and organization_domain_name is the domain name of the organization, using object class OrganizationalRole. Job_function is based upon organizational structure and positions and is not considered a candidate for international standardization, though this does not preclude the use of standards-based names. Job-specific attribute certificates may be populated in this object class.

9.2.5.3 HCstandardRole

This is a healthcare standards-based structural role which can be used for directory-based management of privileged groups. Naming for this will be:

standardRole@organization_domain_name

where standardRole is the standard name of the structural role, and organization_domain_name is the domain name of the organization for those standards-based roles local to the organization, or

standardRole@Locality

where standardRole is the standard name of the structural role if applicable to the Locality (i.e. state).

9.2.5.4 HClocalRole

This is a non-standards-based specialization of GroupOfNames used for new, non-standard, regionally, or locally defined roles. Naming for this shall be:

localRole@organization_domain_name

where localRole is the name of the structural role, and organization_domain_name is the domain name of the organization for those non-standards-based roles local to the organization, or

localRole@Locality

where localRole is the standard name of the structural role if applicable to the Locality (i.e. state).

Annex A
(informative)

Healthcare directory scenarios

A.1 General

This annex presents a series of high-level healthcare cases or “scenarios” representing core business and technical requirements for directory services that will support a broad cross-section of the healthcare industry.

General requirements are presented first, speaking to basic privacy and security principles and fundamental needs of the healthcare industry. The document then details each scenario as follows:

a) a description of the scenario, or healthcare situation requiring healthcare directory services;

b) resulting business and technical requirements that a directory service should provide.

A.2 Scenario explanation

The scenarios described in A.3 show how directory services can be used in healthcare. Each scenario is intended to describe potential uses of a healthcare directory service to provide clinical, administrative, and security support to secure electronic health information sharing. With the dispersed nature of healthcare across the world, together with the range of different persons and organizations that will need to actively co-operate to provide seamless healthcare, it is essential that any directory service be able to operate across and support different healthcare settings, including hospital and community based care, public and private sectors.

A.3 Services exemplified in healthcare scenarios

Service	Scenario number															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Professional focused clinical care support		X	X	X	X	X	X	X				X	X	X	X	X
Health information management and administrative support	X	X	X			X	X				X	X	X			
Health information security support	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X
Consumer health support		X			X			X				X	X			X
Personal contact/healthcare information	X	X	X	X	X	X		X			X	X	X	X	X	X
System contact/healthcare information	X	X					X					X	X			
Organization contact/healthcare information			X	X		X		X			X	X	X			
Retrieval of public keys for encipherment	X	X	X	X	X	X	X	X			X	X	X			
Signature verification			X	X	X	X	X					X	X		X	
CRL checking			X	X	X	X	X	X			X	X	X	X	X	X
Authentication								X				X	X	X		X
Biometric reference								X								
Certification/publishing support									X	X	X					

Scenarios

1. Claims processing
2. Laboratory orders/results
3. Electronic prescriptions
4. Broadcast clinical practice guidelines
5. Broadcast disease state management
6. Patient referral
7. Longitudinal patient history
8. Routine disease state management
9. CA certification process support
10. Attribute certification process support
11. Credentialing process support
12. Patient care in another country
13. Medical referral from another country
14. Remote access to clinical application
15. Privilege delegation
16. Mobile user authentication

A.4 Scenario descriptions

A.4.1 Claims processing

A.4.1.1 Scenario description

This scenario provides an example of using directory services to support secure communications for administrative functions. The healthcare professional billing system processes a batch of claims generating a claim file in accordance with the appropriate EDI specification. The system conducts a directory look-up to identify the communication information of the recipient system and the public key of the recipient. The message is enciphered to the recipient and sent for processing. The system generates an error report for supplemental follow-up. The claims processing system looks up the contact information of the EdiAdministrativeContact for the healthcare professional institution from the directory retrieving the contact and public certificate information into the email system. An enciphered email message is sent to the healthcare professional contact group requesting clarification and back-up documentation from the healthcare professional. The healthcare professional attaches the appropriate documentation containing subject of care information and sends an enciphered email to the response to the payer, looking up the payer contact information and encipherment certificate from the directory.

A.4.1.2 Directory services used

This scenario used the directory for personal and system contact information, email to group, and retrieval of public keys for encipherment.

A.4.2 Laboratory orders and results handling

A.4.2.1 Scenario description

This scenario provides an example of using directory services to support secure communications for clinical communications from a healthcare professional to an organization. The healthcare professional consults with the subject of care to determine where the patient will present for laboratory testing, and sends an encrypted email for medical order for laboratory services to the indicated healthcare organization, looking up the public key of the laboratory contact and communication information from the directory. The healthcare professional signs the request using his/her private key. The laboratory conducts the requested tests on the subject of care and emails the result to the requesting healthcare organization, again using the directory to look up the appropriate contact information and public key for encryption. The result is signed by the laboratory staff and/or system as appropriate. The healthcare professional sends a signed, encrypted email containing the test results to the subject of care identifying the contact information and encryption key from the directory.

A.4.2.2 Directory services used

This scenario used the directory for personal, organization, and system contact information and retrieval of public keys for encryption.

A.4.3 Electronic prescription

A.4.3.1 Scenario description

This scenario provides an example of using directory services to support secure communications and signature verifications for clinical functions. A physician writes a prescription signing with his/her signature key. The CRL is checked for revocation prior to applying the certificate to avoid potential professional embarrassment. The signed, encrypted prescription is sent to the pharmacy and the contact information and encryption certificate information for the organization are obtained via LDAP look-up. The pharmacist authenticates to the local environment enabling local system to provide the user with the deciphered message, verifies the signature and data content against public key via LDAP look-up. The signing certificate is checked for revocation against the directory and is checked to assure that is was issued by a trusted CA. In the case that OCSP services are used, the identity of the OCSP service contact information is identified through the directory.

A.4.3.2 Directory services used

This scenario used the directory for personal and organization contact information, retrieval of public keys for encipherment and signature verification, and CRL checking.

A.4.4 Group broadcast of clinical practice guidelines

A.4.4.1 Scenario description

This scenario provides an example of using directory services to support targeted broadcast communications to clinicians based on professional role. An update to clinical practice guidelines on the use of a new drug therapy in combination with a traditional minor surgical procedure for treatment of pedal onychomycosis is sent out as a broadcast message to all dermatologists. The directory is used to identify the group of all dermatologists. The message is signed, and the directory is again used by the recipients to verify the authenticity of the signature and the validity status of the signer’s certificate.

A.4.4.2 Directory services used

This scenario used the directory for personal contact information, retrieval of public keys for encipherment and signature verification, organization lookup, and CRL checking.

A.4.5 Group broadcast disease state management guidelines

A.4.5.1 Scenario description

This scenario provides an example of using directory services to support secure communications of digitally signed content to the subjects of care. An update to disease state management guidelines is published. The personal health record resource identifies subjects of care affected by the guidelines, and uses the directory to identify the subject of care contact information and public key to initiate a broadcast message to those subjects of care that have requested to receive guideline updates. The email message is signed and encrypted to the subject of care. The subject of care email system then verifies the signer's certificate against the directory and validates the signature.

A.4.5.2 Directory services used

This scenario used the directory for personal contact information, retrieval of public keys for encipherment and signature verification, and CRL checking.

A.4.6 Patient referral

A.4.6.1 Scenario description

This scenario provides an example of using directory services to support secure communications using contact details from a particular role where the healthcare provider holds multiple roles within an organization. Patient referral application interacts with the directory to identify the healthcare organization and associated contact information to receive patient referral information. In this scenario, the healthcare professional identified by the directory inquiry is both an administrator and clinician at the receiving organization. In order to associate the clinical communication with the correct communication details, the health directory is queried for email where objectClass=HcOrganizationalRole, and where roleOccupant is the DN of the practitioner, and cn contains job_function@organization. Alternatively, a 2-pass inquiry may be conducted, first retrieving all of the job functions for the practitioner at the organization, and second requesting the contact information for that job function. Communications information and encryption certificate are identified via LDAP query, and the application sends signed notification and care instructions to the recipient of the patient referral. The receiving organization verifies the signature and certificate validity against the directory and CRL.

A.4.6.2 Directory services used

This scenario used the directory for personal contact information, organization contact information, retrieval of public keys for encipherment and signature verification, organization lookup, and CRL checking.

A.4.7 Longitudinal patient history

A.4.7.1 Scenario description

This scenario provides an example of using directory services to support secure communications pertaining to subject of care digitally signed authorizations. The subject of care presents to a clinician for primary, ambulatory, or urgent care. It is the policy of the jurisdiction to capture consent for authorization to view health information previously recorded for either its use, or authorized disclosure. The subject of care signs consent for authorization to view their medical records. Signature and data content are verified against the public key via LDAP look-up. The certificate is checked for revocation.

The longitudinal patient record application identifies the source of the MPI data from the directory and identifies from that resource record details that are available. Communications information and encryption certificates are identified via LDAP query by the application, and requests for details are sent to the ClinicalInformationContact.

Alternatively, a subject of care without digital credentials presents to the healthcare professional. It is the policy of the jurisdiction to capture consent for authorization to view health information previously recorded for either its use, or authorized disclosure.

A.4.7.2 Directory services used

This scenario used the directory for MPI location information and to verify the subject of care consent credentials against signature verification the CRL from the directory. The directory is also used for the retrieval of public keys for encipherment and communications information.

A.4.8 Routine Disease State Management communications

A.4.8.1 Scenario description

This scenario provides an example of using directory services for authentication of a personal health record and validating digitally signed clinical alerts. The subject of care subscribes to a Disease State Management program. The subject of care authenticates using user-id and password or digital certificate to the personal health record journaling application to enter routine measurements. The CRL is checked for authentication purposes. Secondary biometric verification may be provided as well to confirm the identity of the subject of care. Encrypted alerts are generated from either the automated system or from an individual conducting a case review and sent to the subject of care to remind the subject of care of pending/missed appointments or other such alerts. Communications information and encryption certificates are identified via LDAP query by the application.

A.4.8.2 Directory services used

This scenario used the directory for personal contact information, user authentication, biometric verification service referral, retrieval of public keys for encipherment and CRL checking.

A.4.9 CA certification process support

A.4.9.1 Scenario description

This scenario provides an example of using directory services to support healthcare public key infrastructure key management and revocation verification. The directory used for the healthcare certification authority contains the CA hierarchy and the CA contact information. A healthcare person is issued a certificate by the certification authority. The subject of the certificate is entered into the directory along with attributes held within the certificate, and healthcare schema information. The CA posts public key/certificate to directory for signing key, authentication key and encryption key. The CA updates the CRL stored in the directory.

A.4.9.2 Directory services used

The directory is used to store certificate holder identity and contact information. The directory is also used to store and service subscriber certificates, CA contact information and CRLs.

A.4.10 Attribute certification process support

A.4.10.1 Scenario description

This scenario provides an example of using directory services to support the association of attribute certificates and associated revocations with the healthcare person. The directory used for the healthcare attribute authority contains the AA hierarchy and the AA contact information. A healthcare person is issued an attribute certificate by the attribute authority. The subject of the certificate is updated in the directory with attributes held within the certificate. The AA posts the attribute certificate to the directory under the subscriber entry or the subscriber OrganizationalRole. The AA updates the CRL stored in the directory.

A.4.10.2 Directory services used

The directory is used to store and service subscriber certificates, AA contact information, and CRLs.

A.4.11 Credentialing process support

A.4.11.1 Scenario description

This scenario provides an example of using directory services to support access to healthcare related attributes used for verifying the healthcare provider’s credentials. A healthcare organization or regulatory body working on accreditation looks up education information and contact information from the directory. Certifications in the form of attribute certificate information may also be posted.

A.4.11.2 Directory services used

The directory is used to store and service detailed health related education credentials.

A.4.12 Patient care in another country

A.4.12.1 Scenario description

This scenario provides an example of using directory services to support communication of authorization credentials across jurisdictions for access control decisions. A subject of care falls ill while visiting another country. The subject of care contacts a local physician. That physician authenticates to the local medical institution using local certificate credentials verified against the local directory services and revocation checked against the CRL. The physician requests history information from the primary care physician in the subject of care’s country through an encrypted message, providing certificate credentials to the foreign directory. The credentials and CRL are checked against the source directory.

A.4.12.2 Directory services used

This scenario used the directory for personal contact information, retrieval of public keys for encipherment and signature verification, organization lookup, and CRL checking.

A.4.13 Medical referral from another country

A.4.13.1 Scenario description

This scenario provides an example of using directory services to support look-up of providers of a particular specialty in another jurisdiction, and to send secure communications to that provider for clinical care functions. The subject of care visiting a foreign country requests a medical referral from the primary care physician in the home country. The primary care physician authenticates to the local directory and requests specialty information from the foreign directory servicing the location of the subject of care. Once a clinician is identified, the referring physician authenticates to the messaging application using the credentials verified by the local directory. These credentials are used to generate the referral message to the designated clinician, attesting to the content of the information with his/her signing certificate. The recipient credentials are verified via CRL. The sending physician credentials are verified via CRL check.

A.4.13.2 Directory services used

This scenario used the directory for personal contact information, retrieval of public keys for encipherment and signature verification, organization lookup, and CRL checking.

A.4.14 Remote access to clinical application

A.4.14.1 Scenario description

This scenario provides an example of using directory services to user authentication and to supply associated healthcare credentials belonging to the authenticated individual for authorization decisions. An application is configured to require an SSL3 client-side authentication certificate from a trusted CA. The user presents a token-stored certificate for authentication into the application environment. Certificate mapping links the presented certificate to the user directory entry, and the user is identified. The roles of the authenticated user are identified via LDAP query. Role-based access control decisions are made based upon roles registered in the directory either through the individual as a member of the appropriate group, or through attribute certificate assertions. The revocation status of certificates is checked, and the user is permitted access in accordance with privileges specified at the relying application.

A.4.14.2 Directory services used

The directory is used to authenticate the user role information for role-based access control. It is also used for CRL checking.

A.4.15 Privilege delegation

A.4.15.1 Scenario description

This scenario provides an example of using directory services to communicate attribute certificates and revocation status for authorization decisions. A healthcare professional delegates authority to act on their behalf under certain conditions via an attribute certificate. The directory is consulted to verify the privilege path and the revocation status of the credentials.

A.4.15.2 Directory services used

The directory is used to verify the delegation credentials and revocation status via CRL.

A.4.16 Mobile user authentication

A.4.16.1 Scenario description

This scenario provides an example of using directory services to support user authentication with X.509 certificates and associated revocation checking. A user presents a software certificate for authentication to an application from a mobile environment. The revocation status of the certificate is checked. The application requires secondary password verification against the directory.

A.4.16.2 Directory services used

The directory is used for user authentication, CRL checking, and password verification.

Annex B
(informative)

Referenced object classes

B.1 inetOrgPerson

Reference: inetOrgPerson is described is RFC 2798

Object Class: inetOrgPerson

Superior Object Class: organizationalPerson

OID: 2.16.840.1.113730.3.2.2

Object Class Type: Structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
sn	2.5.4.4	Surname	Directory String	caseIgnore Match	Yes
cn	2.5.4.3	Common Name: RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
description	2.5.4.13	Descriptive Information	Directory String	caseIgnore Match	Yes
seeAlso	2.5.4.34	RFC2256: common supertype of DN attributes	Distinguished Name	distinguished NameMatch	Yes
telephoneNumber	2.5.4.20	RFC2256: Telephone Number	Telephone Number	telephone Number-Match	Yes
userPassword	2.5.4.35	RFC2256/2307: password of user	Octet String	octetString Match	Yes
title	2.5.4.12	Working title, as opposed to personnel title.	Directory String	caseIgnore Match	Yes
ou	2.5.4.11	DN of organization of primary affiliation	Directory String	caseIgnore Match	Yes
preferredDelivery Method	2.5.4.28	RFC2256: preferred delivery method	1.3.6.1.4. 1.1466. 115.121. 1.14		No
st	2.5.4.8	State or Province	Directory String	caseIgnore Match	Yes
telexNumber	2.5.4.21	Telex Number	Telex Number		Yes
l	2.5.4.7	Locality Name	Directory String	caseIgnore Match	Yes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
physicalDeliveryOffice Name	2.5.4.19	Physical Delivery Office Name	Directory String	caseIgnore Match	Yes
postalCode	2.5.4.17	Postal Code	Directory String	caseIgnore Match	Yes
internationalISDN Number	2.5.4.25	RFC2256: international ISDN number	Numeric String	numericString Match	Yes
x121Address	2.5.4.24	RFC2256: X.121 Address	Numeric String	numericString Match	Yes
registeredAddress	2.5.4.26	RFC2256: postal address	Postal Address	caseIgnoreList Match	Yes
street	2.5.4.9	RFC2256: street address of this object	Directory String	caseIgnore Match	Yes
postalAddress	2.5.4.16	RFC2256: postal address	Postal Address	caseIgnoreList Match	Yes
facsimileTelephone Number	2.5.4.23	RFC2256: Facsimile (Fax) Telephone Number	Facsimile Telephone Number		Yes
teletexTerminalIdentifier	2.5.4.22	RFC2256: Teletex Terminal Identifier	1.3.6.1.4. 1.1466. 115.121. 1.51		Yes
postOfficeBox	2.5.4.18	RFC2256: Post Office Box	Directory String	caseIgnore Match	Yes
destinationIndicator	2.5.4.27	RFC2256: destination indicator	Printable String	caseIgnore Match	Yes
userCertificate	2.5.4.36	RFC2256: X.509 user certificate use; binary	Certificate		Yes
uid	0.9.2342.19200300. 100.1.1	RFC1274: user identifier	Directory String	caseIgnore Match	Yes
homePostalAddress	0.9.2342.19200300. 100.1.39	RFC1274: home postal address	Postal Address	caseIgnoreList Match	Yes
employeeType	2.16.840.1.113730. 3.1.4	RFC2798: type of employment for a person	Directory String	caseIgnore Match	Yes
preferredLanguage	2.16.840.1.113730. 3.1.39	RFC2798: preferred written or spoken language for a person	Directory String	caseIgnore Match	No
mail	0.9.2342.19200300. 100.1.3	RFC1274: RFC822 Mailbox	IA5 String	caseIgnoreIA5 Match	Yes
homePhone	0.9.2342.19200300. 100.1.20	RFC1274: home telephone number	Telephone Number	telephone Number-Match	Yes
roomNumber	0.9.2342.19200300. 100.1.6	RFC1274: room number	Directory String	caseIgnore Match	Yes
x500UniqueIdentifier	2.5.4.45	RFC2256: X.500 unique identifier	Bit String	bitStringMatch	Yes
employeeNumber	2.16.840.1.113730. 3.1.3	RFC2798: numerically identifies an employee within an organization	Directory String	caseIgnore Match	No
photo	0.9.2342.19200300. 100.1.7	RFC1274: photo (G3 fax)	1.3.6.1.4. 1.1466. 115.121. 1.23		Yes
businessCategory	2.5.4.15	RFC2256: business category	Directory String	caseIgnore Match	Yes
pager	0.9.2342.19200300. 100.1.42	RFC1274: pager telephone number	Telephone Number	telephone Number-Match	Yes
o	2.5.4.10	Organization Name: RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes
jpegPhoto	0.9.2342.19200300. 100.1.60	RFC2798: a JPEG image	JPEG		Yes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
secretary	0.9.2342.19200300.100.1.21	RFC1274: DN of secretary	DN	distinguished NameMatch	Yes
audio	0.9.2342.19200300.100.1.55	RFC1274: audio (u-law)	Audio		Yes
userPKCS12	2.16.840.1.113730.3.1.216	RFC2798: PKCS #12 PFX PDU for exchange of personal identity information	Binary		Yes
displayName	2.16.840.1.113730.3.1.241	RFC2798: preferred name to be used when displaying entries	Directory String	caseIgnore Match	No
mobile	0.9.2342.19200300.100.1.41	RFC1274: mobile telephone number	Telephone Number	telephone Number-Match	Yes
labeledURI	1.3.6.1.4.1.250.1.57	RFC2079: Uniform Resource Identifier with optional label	Directory String	caseExact Match	Yes
carLicense	2.16.840.1.113730. 3.1.1	RFC2798: vehicle license or registration plate	Directory String	caseIgnore Match	Yes
givenName	2.5.4.42	RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes
Manager	0.9.2342.19200300.100.1.10	RFC1274: DN of manager	DN	distinguished NameMatch	Yes
userSMIMECertificate	2.16.840.1.113730. 3.1.40	RFC2798: PKCS#7 Signed-Data used to support S/MIME	Binary		Yes
initials	2.5.4.43	RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes
departmentNumber	2.16.840.1.113730. 3.1.2	RFC2798: identifies a department within an organization	Directory String	caseIgnore Match	Yes

B.2 Organization

Reference: Organization is described in X.521|ISO/IEC 9594-7

Object Class: organization

Superior Object Class: Top

OID: 2.5.6.4

Object Class Type: Structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
o	2.5.4.10	Organization Name: RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
description	2.5.4.13	Descriptive Information	Directory String	caseIgnore Match	Yes
preferredDelivery Method	2.5.4.28	RFC2256: preferred delivery method	1.3.6.1.4.1.1466.115.121.1.14		No
searchGuide	2.5.4.14	RFC2256: search guide obsoleted by enhancedSearchGuide	1.3.6.1.4.1.1466.115.121.1.25		Yes
st	2.5.4.8	RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes
businessCategory	2.5.4.15	RFC2256: business category	Directory String	caseIgnore Match	Yes
telexNumber	2.5.4.21	Telex Number	Telex Number		Yes
l	2.5.4.7	Locality Name	Directory String	caseIgnore Match	Yes
seeAlso	2.5.4.34	RFC2256: common supertype of DN attributes	Distinguished Name	distinguished NameMatch	Yes
telephoneNumber	2.5.4.20	RFC2256: Telephone Number	Telephone Number	telephone NumberMatch	Yes
physicalDeliveryOffice Name	2.5.4.19	Physical Delivery Office Name	Directory String	caseIgnore Match	Yes
postalCode	2.5.4.17	Postal Code	Directory String	caseIgnore Match	Yes
internationalISDN Number	2.5.4.25	RFC2256: international ISDN number	Numeric String	numericString Match	Yes
x121Address	2.5.4.24	RFC2256: X.121 Address	Numeric String	numericString Match	Yes
userPassword	2.5.4.35	RFC2256/2307: password of user	Octet String	octetString Match	Yes
registeredAddress	2.5.4.26	RFC2256: postal address	Postal Addresss	caseIgnoreList Match	Yes
street	2.5.4.9	RFC2256: street address of this object	Directory String	caseIgnore Match	Yes
postalAddress	2.5.4.16	RFC2256: postal address	Postal Address	caseIgnore ListMatch	Yes
facsimileTelephone-Number	2.5.4.23	RFC2256: Facsimile (Fax) Telephone Number	Facsimile Telephone Number		Yes
teletexTerminalIdentifier	2.5.4.22	RFC2256: Teletex Terminal Identifier	1.3.6.1.4.1.1466.115.121.1.51		Yes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
postOfficeBox	2.5.4.18	RFC2256: Post Office Box	Directory String	caseIgnore Match	Yes
destinationIndicator	2.5.4.27	RFC2256: destination indicator	Printable String	caseIgnore Match	Yes

B.3 OrganizationalRole

Object Class:	organizationalRole
Superior Object Class:	Top
OID:	2.5.6.8
Object Class Type:	Structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
cn	2.5.4.3	Common Name: RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
description	2.5.4.13	Descriptive Information	Directory String	caseIgnore Match	Yes
ou	2.5.4.11	DN of organization of primary affiliation	Directory String	caseIgnore Match	Yes
preferredDelivery Method	2.5.4.28	RFC2256: preferred delivery method	1.3.6.1.4. 1.1466. 115.121. 1.14		No
st	2.5.4.8	RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes
telexNumber	2.5.4.21	Telex Number	Telex Number		Yes
l	2.5.4.7	Locality Name	Directory String	caseIgnore Match	Yes
seeAlso	2.5.4.34	RFC2256: common supertype of DN attributes	Distinguished Name	distinguished NameMatch	Yes
telephoneNumber	2.5.4.20	RFC2256: Telephone Number	Telephone Number	telephone NumberMatch	Yes
physicalDeliveryOffice Name	2.5.4.19	Physical Delivery Office Name	Directory String	caseIgnore Match	Yes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
postalCode	2.5.4.17	Postal Code	Directory String	caseIgnore Match	Yes
roleOccupant	2.5.4.33	RFC2256: common supertype of DN attributes	DN	distinguished NameMatch	Yes
internationalISDN Number	2.5.4.25	RFC2256: international ISDN number	Numeric String	numericString Match	Yes
x121Address	2.5.4.24	RFC2256: X.121 Address	Numeric String	numericString Match	Yes
registeredAddress	2.5.4.26	RFC2256: postal address	Postal Addresss	caseIgnoreList Match	Yes
street	2.5.4.9	RFC2256: street address of this object	Directory String	caseIgnore Match	Yes
postalAddress	2.5.4.16	RFC2256: postal address	Postal Address	caseIgnoreList Match	Yes
facsimileTelephone Number	2.5.4.23	RFC2256: Facsimile (Fax) Telephone Number	Facsimile Telephone Number		Yes
teletexTerminalIdentifier	2.5.4.22	RFC2256: Teletex Terminal Identifier	1.3.6.1.4.1.1466.115.121.1.51		Yes
postOfficeBox	2.5.4.18	RFC2256: Post Office Box	Directory String	caseIgnore Match	Yes
destinationIndicator	2.5.4.27	RFC2256: destination indicator	Printable String	caseIgnore Match	Yes

B.4 GroupOfNames

Reference: GroupOfNames is described in X.521|ISO/IEC 9594-7

Object Class: groupOfNames

Superior Object Class: Top

OID: 2.5.6.9

Object Class Type: Structural

Mandatory attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
cn	2.5.4.3	Common Name: RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes
member	2.5.4.31	RFC2256: common supertype of DN attributes	Distinguished Name	distinguished NameMatch	Yes

Optional attributes:

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
description	2.5.4.13	Descriptive Information	Directory String	caseIgnore Match	Yes
ou	2.5.4.11	DN of organization of primary affiliation	Directory String	caseIgnore Match	Yes
businessCategory	2.5.4.15	RFC2256: business category	Directory String	caseIgnore Match	Yes
owner	2.5.4.32	RFC2256: common supertype of DN attributes	Distinguished Name	distinguished NameMatch	Yes
seeAlso	2.5.4.34	RFC2256: common supertype of DN attributes	Distinguished Name	distinguished NameMatch	Yes
o	2.5.4.10	Organization Name: RFC2256: common supertype of name attributes	Directory String	caseIgnore Match	Yes

Bibliography

[1] ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[2] ISO/TS 14265, *Health Informatics - Classification of purposes for processing personal health information*

[3] ISO 17090 (all parts), *Health informatics — Public key infrastructure*

[4] ISO/TS 21298, *Health informatics — Functional and structural roles*

[5] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*

[6] ISO/TS 22600-2, *Health informatics — Privilege management and access control — Part 2: Formal models*

[7] ISO/IEC 2382-8, *Information technology — Vocabulary — Part 8: Security*

[8] ISO/IEC 10181-1, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview — Part 1*

[9] ISO/IEC/TR 13335-1, *Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security*

[10] ISO/IEC/TR 14516, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*

[11] ISO/IEC 15945, *Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*

[12] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[13] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[14] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[15] CWA 13896, *Lightweight directory access protocol (LDAP) client profile*

[16] CWA 13943:2000, *Lightweight directory access protocol (LDAP) V3: Level of support of LDAP server*

[17] CWA 14193:2001, *Directory synchronisation and the meta-directory. An analysis of issues and techniques*

[18] CWA 13678:1999, *Guidelines for naming in the directory*

[19] DICOM Supplement 67:2003, *Configuration Management*

[20] HL7 V3 RIM, *Reference Information Model*: Health Level Seven Inc., Ann Arbor HL7 V3, *Entity Identification Service*: Health Level Seven Inc., Ann Arbor

[21] IETF/RFC 2798:2000, *Definition of the inetOrgPerson LDAP Object Class*

[22] IETF/RFC 3280:2002, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*

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

[24] IETF/RFC 3647:2003, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

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

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

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

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

[29] ITU-T Recommendation X.509:2001 | ISO/IEC 9594-8, Information technology — Open Systems Interconnection — The Directory — Public-key and attribute certificate frameworks — Part 8[2]

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

[31] ITU-T Recommendation X.520:2001 | ISO/IEC 9594-6, *Information technology — Open Systems Interconnection — The Directory: Selected attribute types — Part 6*

[32] ITU-T Recommendation X.521:2001 | ISO/IEC 9594-7, *Information technology — Open Systems Interconnection — The Directory: Selected object classes — Part 7*

[33] ENV 13608-1, *Health informatics — Security for healthcare communication — Concepts and terminology*

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

[1] ITU-T Standard X.500 is the ITU-T standard for directories and their corresponding concepts, models and services.

[2] ITU-T standard X.509 is the ITU-T standard for certificates and their corresponding authentication framework.

ICS 35.240.80

Price based on 48 pages