TECHNICAL SPECIFICATION

ISO/TS 21091

First edition
2005-12-15

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

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

Reference number
ISO/TS 21091:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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

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

Introduction

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

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

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

1 Scope

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

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

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

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

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

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[ISO/IEC 2382-8]

3.2
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2]

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

[X.509]

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

[X.509]

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

NOTE See also data origin authentication and peer entity authentication.

[ISO 7498-2]

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

[ISO 7498-2]

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

[ISO 7498-2]

3.8
certificate
public key certificate

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

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

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

[ISO/IEC 9594-8]

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

3.12
certificate revocation
act of removing any reliable link between a certificate and its related owner (or security subject owner) because the certificate is not trusted any more even though the time and date are within the certificate validity period

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

3.14
certificate verification
verifying that a certificate is authentic

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

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

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

[ISO 7498-2]

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

[ISO 7498-2]

3.18
digital signature
data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

[ISO 7498-2]

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

[ISO/IEC 2382-8]

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

[ENV 13608-1]

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

[ISO 7498-2]

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

[ISO 7498-2]

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

[ISO 7498-2]

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

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

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

3.27
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

[ISO/IEC 2382-8]

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

[ISO 10181-1]

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

[ISO 10181-1]

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

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

[IETF/RFC 3280]

3.31
public key infrastructure
PKI
structure of hardware, software, people, processes and policies that uses digital signature technology to provide relying parties with a verifiable association between the public component of an asymmetric key pair with a specific subject

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

[IETF/RFC 3647]

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

3.34
security
combination of availability, confidentiality, integrity and accountability

[ENV 13608-1]

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

[ISO/IEC 2382-8]

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

[ISO 7498-2]

3.37
subject
entity whose public key is certified in the certificate

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

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

[ENV 13608-1]

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

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

4 Symbols (and abbreviated terms)

CA Certification Authority

CRL Certificate Revocation List

DAP Directory Access Protocol

DIT Directory Information Tree

LDAP Lightweight Directory Access Protocol

MPI Master Patient Index

PDA Personal Data Assistant

PIDS Person Identification Service

PKC Public Key Certificate

PKI Public Key Infrastructure

RA Registration Authority

TTP Trusted Third Party

5 Health care context

5.1 General

In order to accommodate health care-specific concerns, the health care directories must be extended. The increasing use of networks for the communication and management of health information expands the need for health care-specific directories and support of a number of related information and security services. With increased use of internet- and intranet-based health information systems, health information will need to be communicated across multiple entities and across unaffiliated entities, using both automated and human-interface based systems. Such distributed health information management and communications require a standard for communications data, health care professional directories and consumer information.

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

There is also an increased use of directories for user authentication and security infrastructure management. By creating a single source for user management, health care organizations can enhance user identification and authentication security, exit process privilege removal, role management and access control. By providing a "single sign-on" capability, better password security can be encouraged. However, while this is a powerful tool for enhanced security, the complexity of the directory and inter-directory requirements is increased.

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

5.2 Health care persons

While the X.500 standards include multiple object classes to represent persons as individuals and employees, there are no standard attributes within these object classes to represent key health care-specific information required to support industry communications and services. The health care community needs to represent, within the directory, professional information such as credentials, health care identifiers, role-specific information and health care-specific contact information. Contact information in health care is more complex than in typical business environments due to the nature of multiple affiliations discussed in 5.3. Health care persons include:

— regulated health care professionals;

— non-regulated health care professionals;

— employees of health care organizations and supporting organizations;

— health care consumers.

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

5.3 Multiple affiliations

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

5.4 Health care organizations

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

— regulatory identifiers;

— class of service provided;

— service locations;

— contact information for key information management functions.

Health care organizations include:

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

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

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

5.5 Hardware/software

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

5.6 Health care security services

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

6 Directory security management framework

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

— ISO 22600-2[3];

— ISO/IEC TR 13335-1[7];

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

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

7 Interoperability

7.1 Requirements

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

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

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

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

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

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

7.2 Name space/tree structure

7.2.1 General

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

7.2.2 Country

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

c = Required

7.2.3 Locality

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

l = Optional

7.2.4 Organization

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

o = Issuing authority, health care professional organizations

7.2.5 Organization unit

The Issuing authority shall be sub-categorized by organization unit for those jurisdictions that maintain multiple professional authority branches. For instance, in many countries pharmacists, physicians, dentists may each be managed through a separate government body or department.

ou = Issuing authority professional branch

7.2.6 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 9.2.5.

7.2.7 Multiple instantiations of individuals

The identity of each individual within the system should be represented once, except where an individual has multiple professional credentials, or has associations with multiple healthcare organizations, or other cases where multiple representations may be appropriate. The separations and information representations are supported through the object classes and directory information tree, 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 health care, there is a need to enable and represent independent 'ownership' 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 license 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 must be preserved.

An individual may exist in the directory both as a patient and as a provider. It is also important to separate an individual's personal and professional instantiation within the directory to assure appropriate privacy management. 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 health care 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.

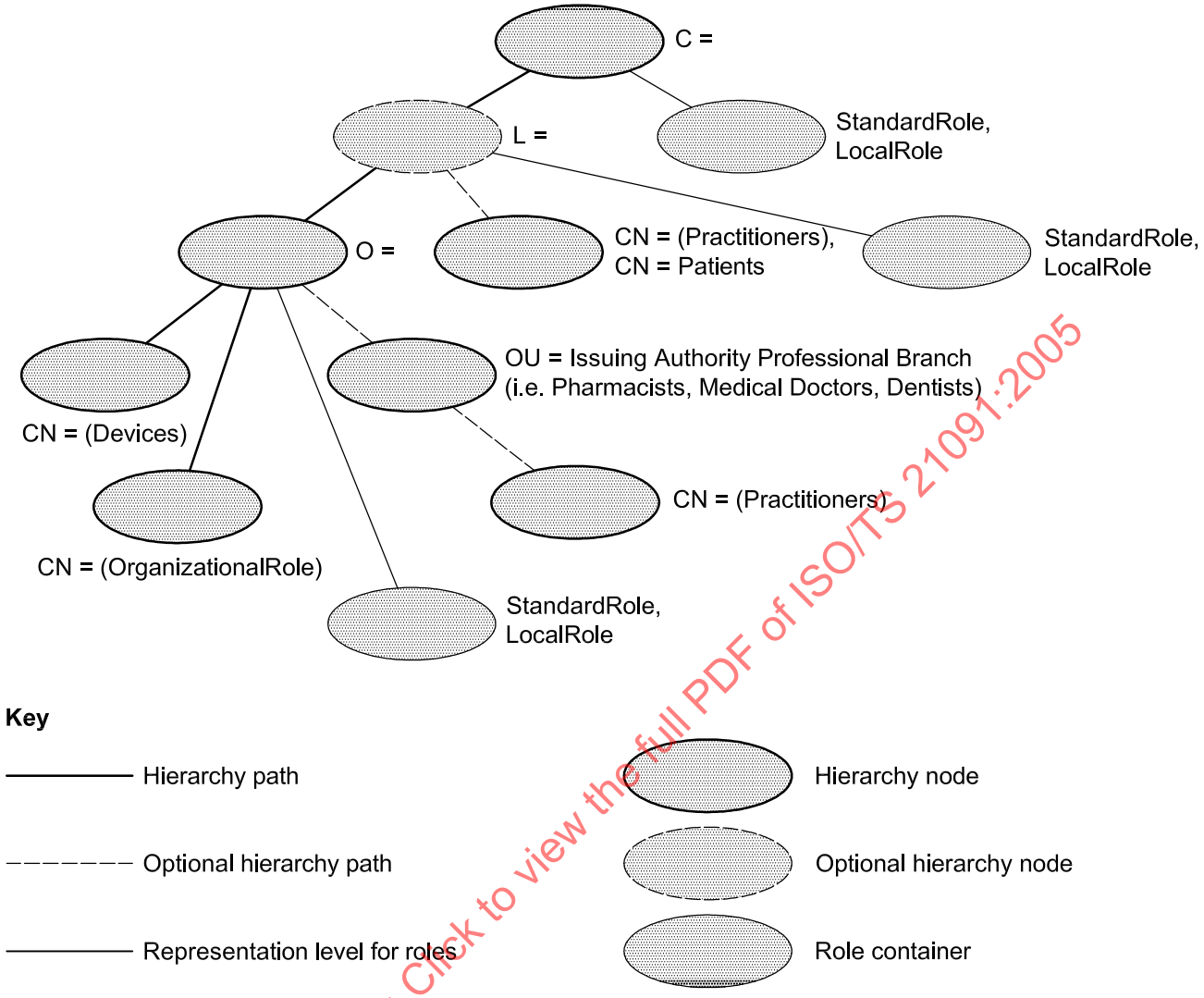

Figure 1 — Directory information tree (DIT) for health care

8 Health care schema

8.1 Health care persons

8.1.1 General

Multiple types of individuals are represented in the health care 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 health care professional, when interacting with the health care system as a patient, may be represented by two object classes: one that contains profession-specific information and another that contains patient-specific information. These shall all have a parent class of person, and shall be specialized accordingly so as to represent the following types of individual: health care consumer, health care professional and health care employee. Information attributes specific to each of the object classes shall be added as a specialization of the base object class.

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.

8.1.2 Health care consumer

Object class: HCConsumer

Superior object class: InetOrgPerson

OID: 1.0.21091.1.1

Object class type: Structural

Mandatory attributes:

Attribute	**OID**	**Description**	**Syntax**	**Matching rules**	**Multi-valued**
HcConsumerID	1.0.21091.2.1.1	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, HcConsumerID can be used to represent any identifier, including, but not limited to security number, health insurance number, medical record number, and driving license number.

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, power of attorney, health care 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 to identify patient clinical records	Directory String	Case Ignore Match, Case Ignore Substrings Match	Yes
HcSubstituteDecisionMaker	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
HL7MothersMaidenName	1.0.21091.2.1.5	The HL-7 defined mother's maiden name	Directory string	Case ignore match, Case ignore substrings match	Yes
HL7DateTimeofBirth	1.0.21091.2.1.6	The hl-7 defined date and time of birth	ISO 8601 Date	Generalized time match Generalized time ordering match	Yes
HL7Sex	1.0.21091.2.1.7	The HL-7 defined sex	Directory string	Case ignore match, Case ignore substrings match	Yes

Attribute	OID	Description	Syntax	Matching rules	Multi-valued
HL7PatientAlias	1.0.21091.2.1.8	The HL-7 defined patient alias	Directory string	Case ignore match, Case ignore substrings match	Yes
HL7CountyCode	1.0.21091.2.1.11	The HL-7 defined county code	Directory string	Case ignore match, Case ignore substrings match	Yes
HL7Religion	1.0.21091.2.1.16	The HL-7 defined religion. While this attribute is important for spiritual aspects of patient care, it must be managed with the utmost protection as this can be sensitive private information	Directory string	Case Ignore match, Case ignore substrings match	Yes
HL7BirthPlace	1.0.21091.2.1.22	The HL-7 defined place of birth	Directory string	Case ignore match, Case ignore substrings match	Yes
HL7PatientDeathDateandTime	1.0.21091.2.1.28	The HL-7 defined patient death date and time	Date	Generalized time match Generalized time ordering match	No

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

The following HL-7 PIDS attributes should be populated with the referenced schema attribute using the defined HL-7 formatting within the relevant constraints of the referenced LDAP attribute:

HL7 PIDS Attribute	***inetOrgPerson/HcConsumer Attribute***
PatientName	Include the XPN formatted name in cn as a second cn value
PhoneNumber_Home	homePhone
PhoneNumber_Business	telephoneNumber
PrimaryLanguage	preferredLanguage
PatientAddress	homePostalAddress
PatientAccountNumber	Use HcConsumerID if needed
SSNNumber	Use HcConsumerID if needed
DriversLicenseNumber	Use HcConsumerID if needed

8.1.3 Health care 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 health care identifier. Where this is a regulated health care professional, this must 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

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 HL-7 coding for roles	Directory string	Case ignore match, Case ignore substrings match	Yes
HcSpecialization	1.0.21091.2.0.6	(Issuing authority: Code system: Code) Populate with HL-7 coding for specialization	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 health care 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 HL-7 coding for roles	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 health care professionals, there will be an instantiation for each health care 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

8.2.1 General

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

1) regulated health care organizations;

2) payers;

3) supporting organizations;

4) regulatory agencies.

Each organization type shall be further specialized as needed to accommodate health care 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 health care organization so as to appropriately accommodate all relevant office staff.

8.2.2 Regulated health care 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 health care 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)	Directory string	Case ignore match, Case ignore substrings match	Yes
EdiAdministrativeContact	1.0.21091.2.0.7	The entry for the individual responsible for EDI administration	DN	Distinguished name match	Yes
ClinicalInformationContact	1.0.21091.2.0.8	The entry for the individual to contact with clinical issues	DN	Distinguished name match	Yes
HcOrganizationCertificates	1.0.21091.2.0.9	Used for storing health care 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 health care regulating authority	Directory string	Case ignore match, Case ignore substrings match	Yes

Attribute	*OID*	*Description*	*Syntax*	*Matching rules*	*Multi-valued*
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	Health care organizations where health care services are rendered	DN	Distinguished name match	Yes

8.2.3 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 health care 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
EdiAdministrativeContact	1.0.21091.2.0.7	The entry for the individual responsible for EDI administration	DN	Distinguished name match	Yes
ClinicalInformationContact	1.0.21091.2.0.8	The entry for the individual to contact with clinical issues.	DN	Distinguished name match	Yes
HcOrganizationCertificates	1.0.21091.2.0.9	Used for storing health care 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

8.2.4 Supporting organizations

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 health care 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
EdiAdministrativeContact	1.0.21091.2.0.7	The entry for the individual responsible for EDI administration	DN	Distinguished name match	Yes
ClinicalInformationContact	1.0.21091.2.0.8	The entry for the individual to contact with clinical issues.	DN	Distinguished name match	Yes
HcOrganizationCertificates	1.0.21091.2.0.9	Used for storing health care 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

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.

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 HL-7 defined roles.	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 Health care standard role

Role is a special type of Group intended to represent the multiple types of roles in health care. These shall be restricted to standard defined roles. Members of these Roles shall be identified by the DN of the OrganizationalRole 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)	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
HcRoleLocationRestriction	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 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)	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
HcRoleLocationRestriction	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

Health care 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 health care-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
HcReferenceEffectiveDate	1.0.21091.2.10.2	Date on which the reference vocabulary is/was effective	Date	Generalized time match Generalized time ordering match	No
HcReferenceDescription	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 health care vocabulary used	Object identifier	Object identifier match	No
HcReferenceDateOfIssue	1.0.21091.2.10.5	Date on which the reference vocabulary was issued	Date	Generalized time match Generalized time ordering match	No
HcReferenceInvalidDate	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 Device property management

Device support shall be as described by DICOM Supplement 67[1] or relevant ISO device specifications with the following additional support for 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 is 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
HcDeviceTrackingNumber	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 NumberMatch and telephoneSubstringsNumber 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 you search your directory 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 we wish to represent multiple concepts within this directory, it is important to establish a common unique naming convention within the health care domain. This unique RDN shall be composed of a concatenation of issuing authority name and identifier, using a ':' 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 Health care professionals

9.2.2.1 Directory identifier

For health care professionals, the directory identifier must be able to account for the professional with:

- *multiple license 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 health care 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 health care, 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 medical regulatory authority.

There shall be no titles used in the representation of common name (i.e. MD, DVM). However, titles 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, MPI, 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 health care, 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 by 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 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 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, titles 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 health care, 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 health care 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 health care 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)

Health care directory scenarios

A.1 Introduction

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

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

1) a description of the scenario, or health care situation requiring health care directory services;

2) resulting business and technical requirements that a directory service must provide.

A.2 Scenario explanation

The scenarios described in A.4 show how directory services can be used in health care. Each scenario is intended to describe potential and probable uses of a health care directory service to provide clinical, administrative and security support to secure electronic health information sharing. With the dispersed nature of health care across the world, together with the range of different persons and organizations that will need to actively co-operate to provide seamless health care, it is essential that any directory service be able to operate across and support different health care settings, including hospital and community based care, public and private sectors.

A.3 Services exemplified in health care 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/health care information	X	X	X	X	X	X		X			X	X	X	X	X	X
System contact/health care information	X	X					X					X	X			
Organization contact/health care 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. Credentialling 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

The health care 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 health care professional institution from the directory, retrieving the contact and public certificate information in the e-mail system. An enciphered e-mail message is sent to the health care professional contact group requesting clarification and back-up documentation from the health care professional. The health care professional attaches the appropriate documentation containing patient information and sends an enciphered e-mail 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 uses the directory for personal and system contact information, e-mail to group and retrieval of public keys for encipherment.

A.4.2 Laboratory orders and results handling

A.4.2.1 Scenario description

Health care professional sends an encrypted e-mail for medical order for laboratory services to another health care professional, looking up the public key of the laboratory contact and communication information in the directory. The physician signs the request using his/her private key. The laboratory conducts the requested tests on the patient and e-mails or result to the requesting health care professional, 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 health care professional sends a signed, encrypted e-mail containing the test results to the patient identifying the contact information and encryption key from the directory.

A.4.2.2 Directory services used

This scenario uses the directory for personal and system contact information and retrieval of public keys for encryption

A.4.3 Electronic prescription

A.4.3.1 Scenario description

A physician writes a prescription signing with his/her signature key. The CRL is checked for revocation prior to applying certificate to avoid potential professional embarrassment. The signed, encrypted prescription is sent to the pharmacy, contact information and encryption certificate information for the organization 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 checked for revocation against the directory and is checked to assure that it was issued by a trusted CA. In the case where 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 uses 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

An update to clinical practice guidelines for childhood immunizations is sent out as a broadcast message to all paediatricians. The directory is used to identify the group of all paediatricians. 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 signatory's certificate.

A.4.4.2 Directory services used

This scenario uses 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

An update to disease state management guidelines is published. The clinical resource identifies patients affected by the guidelines, and uses the directory to identify the patient contact information and public key to initiate a broadcast message to those patients agreeing to receive such messages. The e-mail message is signed and encrypted to the patient. The patient e-mail system then verifies the signatory's certificate against the directory and validates the signature.

A.4.5.2 Directory services used

This scenario uses 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

Patient referral application interacts with directory to identify the health care professional to receive patient referral information. The healthcare professional is both an administrator and clinician at the receiving organization. The health directory is queried for e-mail 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 identified via LDAP query and the application, sends signed notification and care instructions to recipient of 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 uses the directory for personal contact information, retrieval of public keys for encipherment and signature verification, organization lookup, and CRL checking.

A.4.7 Longitudinal patient history (MPI)

A.4.7.1 Scenario description

The patient presents him- or herself to a clinician for primary, ambulatory or urgent care. Patient signs consent for authorization to view medical record. 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 patient without digital credentials presents to the health care professional. The patient MPI locator is identified through query of the directory with the known PIDS data. The MPI resource is identified and after obtaining patient consent, the information is retrieved form the MPI resource.

A.4.7.2 Directory services used

This scenario uses the directory for MPI location information, and to verify the patient consent credentials against signature verification of the CRL from the directory. The directory is also use 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

The patient subscribes to a disease state management program. The patient authenticates using user-id and password or digital certificate to the journal application to enter routine measurements. CRL is checked for authentication purposes. Secondary biometric verification may be provided as well, to assure patient identity. Encrypted alerts are generated from either the automated system or from an individual conducting case review and sent to the patient to remind the patient 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 uses 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

The directory used for the health care certification authority contains the CA hierarchy and the CA contact information. A health care 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 health care 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.