

DIN EN ISO 21091

ICS 35.240.80

Einsprüche bis 2011-10-01

Ersatz für

E DIN EN ISO 21091:2009-03

Entwurf

**Medizinische Informatik –
Verzeichnisdienste für Anbieter, zu Behandelnde und andere Entitäten
im Gesundheitswesen (ISO/DIS 21091:2011);
Englische Fassung prEN ISO 21091:2011**

Health informatics –

Directory services for healthcare providers, subjects of care and other entities
(ISO/DIS 21091:2011);

English version prEN ISO 21091:2011

Informatique de santé –

Services d'annuaires pour les fournisseurs, médecin traitants et d'autres entités en
systèmes de santé publique (ISO/DIS 21091:2011);

Version anglaise prEN ISO 21091:2011

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2011-08-01 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses
Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an named@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de, sofern dort wiedergegeben;
- oder in Papierform an den Normenausschuss Medizin (NAMed) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 69 Seiten

Normenausschuss Medizin (NAMed) im DIN

Nationales Vorwort

Dieses Dokument (prEN ISO 21091:2011) wurde vom Technischen Komitee ISO/TC 215 „Health informatics“ erarbeitet, in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“, dessen Sekretariat von NEN (Niederlande) gehalten wird.

Das zuständige deutsche Gremium ist der Arbeitsausschuss NA 063-07-04 AA „Sicherheit“ im Normenausschuss Medizin (NAMed) im DIN.

Für die im Abschnitt 2 zitierten Internationalen Standards wird darauf hingewiesen, dass ITU Standards von ISO und IEC als Normenteile der Reihe ISO/IEC 9594 übernommen wurden.

Zusammenfassung

Dieser Norm-Entwurf legt Mindestanforderungen für Verzeichnisdienste im Gesundheitswesen, unter Verwendung des X.500 Frameworks fest. Das Dokument bietet Common Directory Informationen und Verzeichnisdienste an, die benötigt werden, um den sicheren Austausch von Gesundheitsinformationen über öffentliche Netze zu unterstützen. Es richtet sich aus der gemeinschaftlichen Perspektive an Verzeichnisse im Gesundheitswesen, um die Unterstützung von Gesundheitskommunikation zwischen Unternehmen, zwischen Gerichtsbarkeiten und zwischen Staaten vorzubereiten. Neben den technischen Sicherheitsvorkehrungen, die in anderen ISO Standards behandelt werden, erfordert die Kommunikation von Gesundheitsdaten eine vertrauenswürdige und rechtssichere „Sicherheitskette“. Um diese Sicherheitskette innerhalb einer Public-Key-Infrastruktur zu erhalten, müssen die Nutzer (die Vertrauenden) in der Lage sein, aktuelle, korrekte Zertifikate und auch deren Statusinformationen über ein sicheres Verzeichnismangement zu beziehen.

Zusätzlich zur Unterstützung von Sicherheitsdiensten wie Zugriffskontrolle und Vertraulichkeit, muss ein Standard die Spezifikationen für andere Aspekte der Kommunikation, wie Adressierung und Protokolle der Kommunikationsentitäten, bereitstellen.

Dieser Norm-Entwurf unterstützt auch Verzeichnisdienste, die dazu bestimmt sind, die Identifikation von Heilberuflern, Organisationen des Gesundheitswesens und Patienten/Konsumenten zu unterstützen. Diese letztgenannten Dienste beinhalten auch Aspekte, die bisweilen als Master-Patient-Indizes bezeichnet werden.

Das Verzeichnis im Gesundheitswesen wird nur übliche Suchen nach LDAP-Clients unterstützen. Spezielle Implementierungsanleitungen, und auch Suchkriterien und Unterstützung einer Suche werden in diesem Dokument nicht beschrieben.

Begriffe

Begriff auf Englisch	Begriff auf Deutsch
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]	Zugriffskontrolle Mittel zur Sicherstellung, dass auf die Ressourcen eines Datenverarbeitungssystems nur von dazu berechtigten Entitäten und in autorisierter Art und Weise zugegriffen werden kann [ISO/IEC 2382-8]
accountability property that ensures that the actions of an entity may be traced uniquely to the entity [ISO 7498-2]	Zurechenbarkeit Eigenschaft, durch die sichergestellt wird, dass die Handlungen einer Entität eindeutig auf diese zurückverfolgt werden können [ISO/IEC 2382-8:1998]
attribute authority (AA) authority which assigns privileges by issuing attribute certificates [X.509]	Attributautorität (AA) Autorität, die durch die Ausgabe von Attributzertifikaten Privilegien zuweist [X.509]
attribute certificate data structure, digitally signed by an attribute authority, that binds some attribute values with identification about its holder [X.509]	Attributzertifikat von einer Attributautorität mit einer digitalen Signatur versehene Datenstruktur, die Attributwerte an die Identifizierung ihres Inhabers bindet [X.509]
authentication process of reliably identifying security subjects by securely associating an identifier and its authenticator. See also data origin authentication and peer entity authentication [ISO 7498-2]	Authentisierung Prozess der zuverlässigen Identifizierung von Sicherheitssubjekten durch sichere Zuordnung eines Bezeichners und dessen Authentikators. Siehe auch Authentisierung der Datenquelle (en: data origin authentication) und Authentisierung auf Partnerebene (en: peer entity authentication) [ISO 7498-2]
authorization granting of privileges, which includes the granting of access based on access privileges [adapted from ISO 7498-2]	Autorisierung Erteilung von Privilegien, wozu auch die Gewährung des Zugriffs basierend auf Zugriffsprivilegien gehört [nach ISO 7498-2]
availability property of being accessible and useable upon demand by an authorized entity [ISO 7498-2]	Verfügbarkeit Eigenschaft, auf Anforderung durch eine berechnigte Entität zugänglich und nutzbar zu sein [ISO 7498-2]
certificate public key certificate	Zertifikat Public-Key-Zertifikat
certificate distribution act of publishing certificates and transferring certificates to security subjects	Zertifikatverteilung Vorgang der Veröffentlichung von Zertifikaten und deren Übertragung auf Sicherheitssubjekte
certificate issuer authority trusted by one or more relying parties to create and assign certificates. Optionally the certification authority may create the relying parties' keys [ISO 9594-8]	Zertifikataussteller Autorität, die von einer oder mehreren vertrauenden Parteien mit der Erzeugung und Zuweisung von Zertifikaten betraut ist. Wahlweise darf die Zertifizierungsstelle die Schlüssel der vertrauenden Partei erzeugen [ISO 9594-8]

Begriff auf Englisch	Begriff auf Deutsch
certificate management procedures relating to certificates such as: certificate generation, certificate distribution, certificate archiving and revocation	Zertifikatverwaltung Verfahren im Zusammenhang mit Zertifikaten, wie zum Beispiel: Zertifikaterzeugung, Zertifikatverteilung, Zertifikatarchivierung und -sperrung
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	Zertifikatsperrung Vorgang der Entfernung einer zuverlässigen Verknüpfung zwischen einem Zertifikat und dessen Eigentümer (oder dem Eigentümer eines Sicherheitssubjekts), weil das Zertifikat nicht mehr vertrauenswürdig ist, obwohl Zeit und Datum noch innerhalb des Gültigkeitszeitraums des Zertifikats liegen
certificate Revocation List (CRL) published list of the suspended and revoked certificates (digitally signed by the CA)	Zertifikatsperrliste (CRL) veröffentlichte Liste der vorübergehend oder dauerhaft gesperrten Zertifikate (von der Zertifizierungsstelle mit digitaler Signatur versehen)
certificate verification verifying that a certificate is authentic	Zertifikatprüfung Überprüfung der Echtheit eines Zertifikats
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.	Zertifizierungsstelle (CA) Entität, die Zertifikate ausstellt, indem sie Zertifikatsdaten mit ihrem privaten Signaturschlüssel unterzeichnet ANMERKUNG „Stelle“ deutet hier nicht auf eine Genehmigung durch staatliche Einrichtungen hin, sondern bedeutet nur, dass es sich um eine vertrauenswürdige Stelle handelt. Zertifikatsaussteller wäre möglicherweise ein besserer Begriff, aber Zertifizierungsstelle ist sehr weit verbreitet.
confidentiality property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO 7498-2]	Vertraulichkeit Eigenschaft, dass Informationen unberechtigten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder enthüllt werden [ISO 7498-2]
data integrity property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2]	Datenintegrität Eigenschaft, die Daten besitzen, wenn sie nicht auf unberechtigte Weise verändert oder zerstört wurden [ISO 7498-2]
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]	digitale Signatur an eine Dateneinheit angehängte Daten oder eine kryptographische Umwandlung (siehe Kryptographie) dieser Dateneinheit, die es einem Empfänger der Dateneinheit erlauben, die Quelle und Integrität der Einheit zu überprüfen, und die einen Schutz gegen Fälschung, zum Beispiel durch den Empfänger, bieten [ISO 7498-2]
identification performance of tests to enable a data processing system to recognize entities [ISO/IEC 2382-08]	Identifizierung Durchführung von Prüfungen, um einem Datenverarbeitungssystem die Erkennung von Entitäten zu ermöglichen [ISO/IEC 2382-08]

Begriff auf Englisch	Begriff auf Deutsch
identifier piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator [ENV 13608-1]	Bezeichner Information, die vor einer möglichen Bestätigung durch einen entsprechenden Authentifikator verwendet wird, um eine Identität zu beanspruchen [ENV 13608-1]
integrity proof that the message content has not altered, deliberately or accidentally in any way, during transmission [ISO/IEC 7498-2]	Integrität Nachweis darüber, dass sich der Nachrichteninhalt während der Übertragung nicht verändert hat, sei es absichtlich oder versehentlich [ISO/IEC 7498-2]
key sequence of symbols that controls the operations of encipherment and decipherment [ISO 7498-2]	Schlüssel Folge von Symbolen, die Chiffrier- und Dechiffrieroperationen steuern [ISO 7498-2]
key management generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy [ISO 7498-2]	Schlüsselverwaltung Erzeugung, Speicherung, Verteilung, Löschung, Archivierung und Anwendung von Schlüsseln entsprechend einer Sicherheitsrichtlinie [ISO 7498-2]
lightweight directory access protocol (LDAP) standard access protocol for directories allowing public or controlled access to certificates and other information needed in a PKI	LDAP (en: lightweight directory access protocol) Standardzugriffsprotokoll für Verzeichnisse, das den öffentlichen oder geregelten Zugriff auf Zertifikate und sonstige Informationen, die in einer PKI benötigt werden, erlaubt
object identifier (OID) unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class	Objektbezeichner (OID) eindeutiger alphanumerischer/numerischer Bezeichner zur Referenzierung eines bestimmten Objekts oder einer bestimmten Objektklasse, der nach der ISO-Registrierungsnorm registriert ist
subject of care person that is the receiver of health related services and that is a person in a health information system	Behandelte(r) bzw. zu Behandelnde(r) Person, die Dienstleistungen des Gesundheitswesens erhält und die eine Person in einem Gesundheitsinformationssystem ist
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 2382-08]	Privatsphäre Nichtvorliegen des Eindringens in das Privatleben oder die Privatangelegenheiten einer Person, wenn dieses Eindringen aus der unzulässigen oder illegalen Zusammentragung und Verwendung von Daten zu dieser Person herrührt [ISO/IEC 2382-08]
private key key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity) [ISO 10181-1]	privater Schlüssel Schlüssel, der mit einem asymmetrischen kryptographischen Algorithmus verwendet wird und dessen Besitz eingeschränkt ist (üblicherweise auf nur eine Entität) [ISO 10181-1]
public key key that is used with an asymmetric cryptographic algorithm and that can be made publicly available [ISO 10181-1]	öffentlicher Schlüssel Schlüssel, der mit einem asymmetrischen kryptographischen Algorithmus verwendet wird und der öffentlich verfügbar gemacht werden kann [ISO 10181-1]

Begriff auf Englisch	Begriff auf Deutsch
public key certificate X.509 public key certificates (PKCs) [X.509], bind an identity and a public key. The identity may be used to support identity-based access control decisions after the client proves that it has access to the private key that corresponds to the public key contained in the PKC [RFC 3280]	Public-Key-Zertifikat Public-Key-Zertifikate (PKCs) nach X.509, binden eine Identität und einen öffentlichen Schlüssel aneinander. Die Identität darf verwendet werden, um Entscheidungen hinsichtlich einer identitätsbasierten Zugriffskontrolle zu unterstützen, nachdem der Client nachgewiesen hat, dass er Zugriff auf den privaten Schlüssel hat, der das Gegenstück zu dem im PKC enthaltenen öffentlichen Schlüssel bildet [RFC 3280]
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	Public-Key-Infrastruktur (PKI) Struktur aus Hardware, Software, Menschen, Prozessen und Richtlinien, die die Technologie der digitalen Signatur nutzt, um vertrauenden Parteien eine überprüfbare Zuordnung zwischen der öffentlichen Komponente eines asymmetrischen Schlüsselpaars und einem bestimmten Subjekt zu bieten
relying party recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate [RFC 3647]	vertrauende Partei Empfänger eines Zertifikats, der im Vertrauen auf dieses Zertifikat und/oder die mittels dieses Zertifikats überprüfte digitale Signatur handelt [RFC 3647]
role set of competencies and/or performances that are associated with a set of tasks	Rolle Satz von Zuständigkeiten und/oder Leistungen, die einem Satz von Aufgabe zugewiesen sind
security combination of availability, confidentiality, integrity and accountability [CEN]	Sicherheit Kombination aus Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit [CEN]
security policy plan or course of action adopted for providing computer security [ISO/IEC 2382-08]	Sicherheitsrichtlinie Aktionsplan oder -ablauf, der zum Zweck der Rechnersicherheit befolgt wird [ISO/IEC 2382-08]
security service service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers [ISO 7498]	Sicherheitsdienst Dienst, der von einer Schicht miteinander kommunizierender offener Systeme erbracht wird und die angemessene Sicherheit der Systeme oder des Datentransfers sicherstellt [ISO 7498]
security subject entity in an active role to which a security policy applies [RFC 2920]	Sicherheitssubjekt Entität in einer aktiven Rolle, für die eine Sicherheitsrichtlinie gilt [RFC 2920]
subject entity whose public key is certified in the certificate	Subjekt Entität, deren öffentlicher Schlüssel im Zertifikat zertifiziert ist
third party party other than data originator, or data recipient, required to perform a security function as part of a communication protocol	Dritte(r) Partei, die nicht der Datenurheber oder Datenempfänger ist, die eine Sicherheitsfunktion als Teil eines Kommunikationsprotokolls ausführen muss

Begriff auf Englisch	Begriff auf Deutsch
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.	vertrauenswürdige(r) Dritte(r) Dritte, die im Zusammenhang mit einem Sicherheitsprotokoll als vertrauenswürdig gelten [ENV 13608-1] ANMERKUNG Dieser Begriff wird in vielen ISO/IEC-Normen und sonstigen Dokumenten verwendet, die vorwiegend die Dienste einer Zertifizierungsstelle beschreiben. Der Begriff ist jedoch weiter gefasst und schließt auch Dienste wie das Versehen mit Zeitstempeln und eventuell Hinterlegung ein.
X.500 ITU-T Standard X.500. The ITU-T standard for directories and their corresponding concepts, models, and services	X.500 ITU-T-Norm X.500. Die ITU-T-Norm für Verzeichnisse und die zugehörigen Begriffe, Modelle und Dienste
X.509 ITU-T Standard X.509. The ITU-T standard for certificates and their corresponding authentication framework	X.509 ITU-T-Norm X.509. Die ITU-T-Norm für Zertifikate und deren zugehörigen Authentisierungsrahmen

— Leerseite —

Health Informatics — Directory services for security, communications and identification of professional and patients (ISO 21091:2008)

Einführendes Element — Haupt-Element — Ergänzendes Element (ISO 21091:2008)

Informatique de santé — Services d'annuaires pour la sécurité, les communications et l'identification des patients et des professionnels (ISO 21091:2008)

ICS:

Descriptors:

Document type: European Standard
Document subtype:
Document stage: CEN Enquiry
Document language: E

STD Version 2.2

Contents

Page

Foreword.....	4
Introduction	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Abbreviated terms	10
5 Health care context.....	11
5.1 General.....	11
5.2 Health care persons	12
5.3 Multiple affiliations	12
5.4 Health care organizations	12
5.5 Hardware/Software	13
5.6 Health care security services	13
6 Directory security management framework.....	13
7 Interoperability.....	14
7.1 Requirements.....	14
7.2 Name space/tree structure.....	14
7.2.1 General.....	14
7.2.2 Country	14
7.2.3 Locality	14
7.2.4 Organization.....	14
7.2.5 Organization unit	15
7.2.6 Structural roles	15
7.2.7 Multiple instantiations of individuals.....	15
8 Health care schema	16
8.1 Health care persons	16
8.1.1 General.....	16
8.1.2 Subjects of care (Health Care Consumer).....	17
8.1.3 Health care professional	23
8.1.4 Employees	25
8.2 Organizational identities	27
8.2.1 General.....	27
8.2.2 Regulated health care organization	27
8.2.3 Payer organizations.....	29
8.2.4 Supporting organizations (including agencies)	31
8.3 Roles, job function and group.....	33
8.3.1 Organizational role individual	33
8.3.2 Health care standard role.....	34
8.3.3 Local role	35
8.3.4 Coded references.....	36
8.3.5 Device property management	37
9 Distinguished name.....	39
9.1 General.....	39
9.2 Relative distinguished name	39
9.2.1 General.....	39
9.2.2 Health care professionals	39
9.2.3 Health consumers.....	40
9.2.4 Organization.....	41
9.2.5 Roles/jobs	41

Annex A (informative) Health care directory scenarios	43
A.1 Introduction.....	43
A.2 Scenario explanation	43
A.3 Services exemplified in health care scenarios.....	43
A.4 Scenario descriptions.....	44
A.4.1 Claims processing.....	44
A.4.2 Laboratory orders and results handling	45
A.4.3 Electronic prescription	45
A.4.4 Group broadcast of clinical practice guidelines	45
A.4.5 Group broadcast disease state management guidelines.....	46
A.4.6 Patient referral	46
A.4.7 Longitudinal patient history	46
A.4.8 Routine disease state management communications	47
A.4.9 CA certification process support.....	47
A.4.10 Attribute certification process support.....	48
A.4.11 Credentialing process support	48
A.4.12 Patient care in another country	48
A.4.13 Medical referral from another country	48
A.4.14 Remote access to clinical application.....	49
A.4.15 Privilege delegation.....	49
A.4.16 Mobile user authentication	49
Annex B (informative) Referenced object classes.....	50
B.1 inetOrgPerson.....	50
B.2 Organisation	54
B.3 OrganizationalRole	56
B.4 GroupOfNames	58
Bibliography	60

Foreword

This document (prEN ISO 21091:2011) has been prepared by Technical Committee ISO/TC 215 "Health informatics" in collaboration with Technical Committee CEN/TC 251 "Health informatics" the secretariat of which is held by NEN.

This document is currently submitted to the parallel Enquiry.

Endorsement notice

The text of ISO/DIS 21091:2011 has been approved by CEN as a prEN ISO 21091:2011 without any modification.

Introduction

The Health informatics — Directory services for health care providers, subjects of care, and other entities 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 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, health care-specific contact information, and health care identifiers. This standard addresses the health care specific requirements of the directory, and defines, as appropriate, standard specifications for inclusion of this information in the health care directory.

1 Scope

This standard defines minimal specifications for directory services for health care. This standard can be used to enable communications between organizations, devices, servers, application components, systems, technical actors, and devices. This standard provides the common directory information and services needed to support the secure exchange of health care information over public networks where directory information and services are used for these purposes. This specification addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction, and international health care communications. While several options are supported by this standard a given service will not need to include all of the options.

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, the standard shall provide specification for other aspects of communication, such as addresses and protocols of communication entities.

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

The health care directory will support standard LDAP Client searches, interface engines for message transformation, and SOA implementations to enable the service in any environment. 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.

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

ITU-T Recommendation X.521:2001 | ISO/IEC 9594-7:2008, *Information technology - Open Systems Interconnection - The Directory: Selected Object Classes*

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

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 which 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. See also data origin authentication and peer entity authentication [ISO 7498-2]

3.6

authorization

granting of privileges, which includes the granting of access based on access privileges [adapted from 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. Optionally the certification authority may create the relying parties' keys [ISO 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 has 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 2382-08]

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/IEC 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

subject of care

person that is the receiver of health related services and that is an 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 2382-08]

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

X.509 public key certificates (PKCs) [X.509], bind an identity and a public key. The identity may be used to support identity-based access control decisions after the client proves that it has access to the private key that corresponds to the public key contained in the PKC [RFC3280]

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 [RFC 3647]

3.33

role

set of competencies and/or performances that are associated with a set of tasks.

3.34

security

combination of availability, confidentiality, integrity and accountability [CEN]

3.35

security policy

plan or course of action adopted for providing computer security [ISO/IEC 2382-08]

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]

3.37

security subject

entity in an active role to which a security policy applies [RFC 2920]

3.38

subject

entity whose public key is certified in the certificate.

3.39

third party

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

3.40

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

3.41

X.500

ITU-T Standard X.500. The ITU-T standard for directories and their corresponding concepts, models, and services

3.42

X.509

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

4 Abbreviated terms

CA	Certification Authority
CN	Common NameCRL 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 Health care context

5.1 General

In order to accommodate health care-specific concerns, standard directory services must be extended. Data attributes that are required to manage and distinguish health professionals, subjects of care, organizations, and other health entities engaged in health care communications and security decisions are not address fully by X.500 defined attributes. The increasing use of networks for the communication and management of health information expands the need for health care-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 un-affiliated 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 relying on enhanced information technology infrastructures to simplify and enhance user management functions through the use of LDAP and SOA 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 in 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. By creating a single source for user management, health care 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 health care related attributes such as health care 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 health care directory is to support health care 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 health care 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 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 health care 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 health care directories. Additional use cases can be found in Annex A of this document.

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 the next section. Health care persons include:

- Regulated health care professionals;
- Non-regulated health care professionals;
- Employees of health care 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. Implementations of directories supporting such capabilities for the subjects of care should be separately managed from provider directories.

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, and 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.

Another important factor is that health care staff are also health care consumers, and their professional identities should be distinct from their health care consumer identity. From a privacy perspective, it is important that health care staff and their associated professional identities must be separate from their personal identities.

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. Professional colleges, 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. PDA's 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

The 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 principles defined in the international standards space. While the following standards are not directory specific, should be adhered to for the protection of Directory Infrastructures:

- ISO 17799 Part 1 (2000): Code of Practice for Information Security Management;
- ISO TR 13335: Guidelines for the Management of Information Technology Security-GMITS;
- 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 out of scope of this document, 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 are 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.