

**DIN EN ISO 21091**

ICS 35.240.80

**Medizinische Informatik –  
Verzeichnisdienste für Anbieter, zu Behandelnde und andere Entitäten  
im Gesundheitswesen (ISO 21091:2013);  
Englische Fassung EN ISO 21091:2013**

Health informatics –

Directory services for healthcare providers, subjects of care and other entities  
(ISO 21091:2013);

English version EN ISO 21091:2013

Informatique de santé –

Services d'annuaires pour les fournisseurs de soins de santé, les sujets de soins et autre  
entités (ISO 21091:2013);

Version anglaise EN ISO 21091:2013

Gesamtumfang 60 Seiten

Normenausschuss Medizin (NAMed) im DIN

## Nationales Vorwort

Dieses Dokument (EN ISO 21091:2013) 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.

## Zusammenfassung

Diese Norm legt Mindestanforderungen für Verzeichnisdienste im Gesundheitswesen fest. Sie kann verwendet werden, um Kommunikationen zwischen Organisationen, Einheiten, Servern, Anwendungskomponenten, Systemen, Technikern und Geräten zu ermöglichen.

Diese Norm 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. Während verschiedene Optionen durch diese Norm unterstützt werden, wird ein gegebener Dienst nicht benötigt, um alle Optionen einzuschließen.

Zusätzlich zur Unterstützung von Sicherheitsdiensten wie Zugriffskontrolle und Vertraulichkeit, stellt diese Norm Spezifikationen für weitere Aspekte der Kommunikation, wie Adressierung und Protokolle der Kommunikationsentitäten, bereit.

Diese Norm unterstützt auch Verzeichnisdienste, die die Identifikation von Heilberuflern, Organisationen des Gesundheitswesens und Behandelten bzw. zu Behandelnden zu unterstützen.

## Nationaler Anhang NA (informativ)

### Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

#### Begriffe

| Begriff auf Englisch                                                                                                                                                         | Begriff auf Deutsch                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>access control</b><br>means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways<br>[ISO/IEC 2382-8] | <b>Zugriffskontrolle</b><br>Mittel zur Sicherstellung, dass auf die Ressourcen eines Datenverarbeitungssystems nur von dazu berechtigten Entitäten und in autorisierter Art und Weise zugegriffen werden kann<br>[ISO/IEC 2382-8] |
| <b>attribute authority</b><br><b>AA</b><br>authority which assigns privileges by issuing attribute certificates<br>[X.509]                                                   | <b>Attributautorität</b><br><b>AA</b><br>Autorität, die durch die Ausgabe von Attribut-zertifikaten Privilegien zuweist<br>[X.509]                                                                                                |
| <b>attribute certificate</b><br>data structure, digitally signed by an attribute authority, that binds some attribute values with identification about its holder<br>[X.509] | <b>Attributzertifikat</b><br>von einer Attributautorität mit einer digitalen Signatur versehene Datenstruktur, die Attributwerte an die Identifizierung ihres Inhabers bindet<br>[X.509]                                          |
| <b>authentication</b><br>process of reliably identifying security subjects by securely associating an identifier and its authenticator.<br>[ISO 7498-2]                      | <b>Authentisierung</b><br>Prozess der zuverlässigen Identifizierung von Sicherheitssubjekten durch sichere Zuordnung eines Bezeichners und dessen Authentikators<br>[ISO 7498-2]                                                  |
| <b>authorization</b><br>granting of rights, which includes the granting of access rights<br>[ISO 7498-2]                                                                     | <b>Autorisierung</b><br>Erteilung von Rechten, wozu auch die Gewährung von Zugriffsrechten gehören<br>[ISO 7498-2]                                                                                                                |
| <b>availability</b><br>property of being accessible and useable upon demand by an authorized entity<br>[ISO 7498-2]                                                          | <b>Verfügbarkeit</b><br>Eigenschaft, auf Anforderung durch eine berechnigte Entität zugänglich und nutzbar zu sein<br>[ISO 7498-2]                                                                                                |
| <b>certificate</b><br>public key certificate                                                                                                                                 | <b>Zertifikat</b><br>Public-Key-Zertifikat                                                                                                                                                                                        |
| <b>certificate distribution</b><br>act of publishing certificates and transferring certificates to security subjects                                                         | <b>Zertifikatverteilung</b><br>Vorgang der Veröffentlichung von Zertifikaten und deren Übertragung auf Sicherheitssubjekte                                                                                                        |

| Begriff auf Englisch                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Begriff auf Deutsch                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>certificate issuer</b><br>authority trusted by one or more relying parties to create and assign certificates.<br>Note 1 to entry: Optionally the certification authority may create the relying parties' keys<br>[ISO/IEC 9594-8]                                                                                                                                                                                                                                    | <b>Zertifikataussteller</b><br>Autorität, die von einer oder mehreren vertrauenden Parteien mit der Erzeugung und Zuweisung von Zertifikaten betraut ist.<br>Anmerkung 1 zum Eintrag: Wahlweise darf die Zertifizierungsstelle die Schlüssel der vertrauenden Partei erzeugen<br>[ISO 9594-8]                                                                                                                                                                                                                                                                                                                                           |
| <b>certificate management</b><br>procedures relating to certificates, i.e. certificate generation, certificate distribution, certificate archiving and revocation                                                                                                                                                                                                                                                                                                       | <b>Zertifikatverwaltung</b><br>Verfahren im Zusammenhang mit Zertifikaten, d. h. Zertifikaterzeugung, Zertifikatverteilung, Zertifikatarchivierung und -sperrung                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>certificate revocation</b><br>act of removing any reliable link between a certificate and its related owner (or security subject owner) because the certificate is not trusted any more, even though it is unexpired                                                                                                                                                                                                                                                 | <b>Zertifikatssperrung</b><br>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 es noch nicht abgelaufen ist                                                                                                                                                                                                                                                                                                                                                          |
| <b>certificate revocation list</b><br>published list of the suspended and revoked certificates (digitally signed by the CA)                                                                                                                                                                                                                                                                                                                                             | <b>Zertifikatssperrliste</b><br>veröffentlichte Liste der vorübergehend oder dauerhaft gesperrten Zertifikate (von der Zertifizierungsstelle mit digitaler Signatur versehen)                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>certificate verification</b><br>verifying that a <i>certificate</i> (3.7) is authentic                                                                                                                                                                                                                                                                                                                                                                               | <b>Zertifikatprüfung</b><br>Überprüfung der Echtheit eines <i>Zertifikats</i> (3.7)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>certification authority</b><br><b>CA</b><br>authority trusted by one or more relying parties to create and assign certificates and which may, optionally, create the relying parties' keys<br>Note 1 to entry: Adapted from ISO/IEC 9594-8<br>Note 2 to entry: Authority in the CA term does not imply any government authorization, but only denotes that it is trusted.<br>Note 3 to entry: "Certificate issuer" may be a better term, but CA is very widely used. | <b>Zertifizierungsstelle</b><br><b>CA</b><br>durch eine oder mehrere vertrauende Partei(en) betraute Autorität zur Ausstellung und Anweisung von Zertifikaten, die optional die Schlüssel der vertrauenden Parteien ausstellt.<br>Anmerkung 1 zum Eintrag: Abgeleitet aus ISO/IEC 9594-8<br>Anmerkung 2 zum Eintrag: „Stelle“ deutet hier nicht auf eine Genehmigung durch staatliche Einrichtungen hin, sondern bedeutet nur, dass es sich um eine vertrauenswürdige Stelle handelt.<br>Anmerkung 3 zum Eintrag: „Zertifikataussteller“ wäre möglicherweise ein besserer Begriff, aber Zertifizierungsstelle ist sehr weit verbreitet. |
| <b>confidentiality</b><br>property that information is not made available or disclosed to unauthorized individuals, entities, or processes<br>[ISO 7498-2]                                                                                                                                                                                                                                                                                                              | <b>Vertraulichkeit</b><br>Eigenschaft, dass Informationen unberechtigten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder enthüllt werden<br>[ISO 7498-2]                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>data integrity</b><br>property that data has not been altered or destroyed in an unauthorized manner<br>[ISO 7498-2]                                                                                                                                                                                                                                                                                                                                                 | <b>Datenintegrität</b><br>Eigenschaft, die Daten besitzen, wenn sie nicht auf unberechtigte Weise verändert oder zerstört wurden<br>[ISO 7498-2]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Begriff auf Englisch                                                                                                                                                                                                                                          | Begriff auf Deutsch                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>digital signature</b><br>data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient<br>[ISO 7498-2] | <b>digitale Signatur</b><br>an eine Dateneinheit angehängte Daten oder eine kryptographische Umwandlung 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<br>[ISO 7498-2] |
| <b>identification</b><br>performance of tests to enable a data processing system to recognize entities<br>[ISO/IEC 2382-08]                                                                                                                                   | <b>Identifizierung</b><br>Durchführung von Prüfungen, um einem Datenverarbeitungssystem die Erkennung von Entitäten zu ermöglichen<br>[ISO/IEC 2382-08]                                                                                                                                                                            |
| <b>identifier</b><br>piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator<br>[ENV 13608-1]                                                                                                       | <b>Bezeichner</b><br>Information, die vor einer möglichen Bestätigung durch einen entsprechenden Authentifikator verwendet wird, um eine Identität zu beanspruchen<br>[ENV 13608-1]                                                                                                                                                |
| <b>integrity</b><br>property that data has not been altered or destroyed in an unauthorized manner<br>[ISO 7498-2]                                                                                                                                            | <b>Integrität</b><br>Eigenschaft, dass Daten nicht auf unautorisierte Art geändert oder zerstört worden sind<br>[ISO 7498-2]                                                                                                                                                                                                       |
| <b>key</b><br>sequence of symbols that controls the operations of encipherment and decipherment<br>[ISO 7498-2]                                                                                                                                               | <b>Schlüssel</b><br>Folge von Symbolen, die Chiffrier- und Dechiffrieroperationen steuern<br>[ISO 7498-2]                                                                                                                                                                                                                          |
| <b>key management</b><br>generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy<br>[ISO 7498-2]                                                                                                  | <b>Schlüsselverwaltung</b><br>Erzeugung, Speicherung, Verteilung, Löschung, Archivierung und Anwendung von Schlüsseln entsprechend einer Sicherheitsrichtlinie<br>[ISO 7498-2]                                                                                                                                                     |
| <b>lightweight directory access protocol</b><br><b>LDAP</b><br>standard access protocol for directories allowing public or controlled access to certificates and other information needed in a PKI                                                            | <b>LDAP</b><br>en: lightweight directory access protocol<br>Standardzugriffsprotokoll für Verzeichnisse, das den öffentlichen oder geregelten Zugriff auf Zertifikate und sonstige Informationen, die in einer PKI benötigt werden, erlaubt                                                                                        |
| <b>object identifier</b><br><b>OID</b><br>unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class                                                                                | <b>Objektbezeichner</b><br><b>OID</b><br>eindeutiger alphanumerischer/numerischer Bezeichner zur Referenzierung eines bestimmten Objekts oder einer bestimmten Objektklasse, der nach der ISO-Registrierungsnorm registriert ist                                                                                                   |
| <b>privacy</b><br>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<br>[ISO/IEC 2382-8]                                              | <b>Privatsphäre</b><br>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<br>[ISO/IEC 2382-8]                                                            |

| Begriff auf Englisch                                                                                                                                                                                                                                                                             | Begriff auf Deutsch                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>private key</b><br>key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)<br>[ISO/IEC 10181-1]                                                                                                                           | <b>privater Schlüssel</b><br>Schlüssel, der mit einem asymmetrischen kryptographischen Algorithmus verwendet wird und dessen Besitz eingeschränkt ist (üblicherweise auf nur eine Entität)<br>[ISO/IEC 10181-1]                                                                                                                                                |
| <b>public key</b><br>key that is used with an asymmetric cryptographic algorithm and that can be made publicly available<br>[ISO/IEC 10181-1]                                                                                                                                                    | <b>öffentlicher Schlüssel</b><br>Schlüssel, der mit einem asymmetrischen kryptographischen Algorithmus verwendet wird und der öffentlich verfügbar gemacht werden kann<br>[ISO/IEC 10181-1]                                                                                                                                                                    |
| <b>public key certificate</b><br><b>PKC</b><br>certificate that binds an identity and a public key<br>[RFC 3280]                                                                                                                                                                                 | <b>Zertifikat für öffentlichen Schlüssel</b><br><b>PKC</b><br>Zertifikat, dass eine Identität und einen öffentlichen Schlüssel aneinander bindet<br>[RFC 3280]                                                                                                                                                                                                 |
| <b>public key infrastructure</b><br><b>PKI</b><br>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 | <b>Infrastruktur des öffentlichen Schlüssels</b><br><b>PKI</b><br>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 |
| <b>relying party</b><br>recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate<br>[RFC 3647]                                                                                                                               | <b>vertrauende Partei</b><br>Empfänger eines Zertifikats, der im Vertrauen auf dieses Zertifikat und/oder die mittels dieses Zertifikats überprüfte digitale Signatur handelt<br>[RFC 3647]                                                                                                                                                                    |
| <b>role</b><br>set of competences and/or performances associated with a task                                                                                                                                                                                                                     | <b>Rolle</b><br>Satz von Zuständigkeiten und/oder Leistungen verbunden mit einer Aufgabe                                                                                                                                                                                                                                                                       |
| <b>security</b><br>combination of availability, confidentiality, integrity and accountability<br>[ENV 13608-1]                                                                                                                                                                                   | <b>Sicherheit</b><br>Kombination aus Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit<br>[ENV 13608-1]                                                                                                                                                                                                                                           |
| <b>security policy</b><br>plan or course of action adopted for providing computer security<br>[ISO/IEC 2382-8]                                                                                                                                                                                   | <b>Sicherheitsrichtlinie</b><br>Aktionsplan oder -ablauf, der zum Zweck der Rechensicherheit befolgt wird<br>[ISO/IEC 2382-8]                                                                                                                                                                                                                                  |
| <b>security service</b><br>service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers<br>[ISO/IEC 7498]                                                                                                                     | <b>Sicherheitsdienst</b><br>Dienst, der von einer Schicht miteinander kommunizierender offener Systeme erbracht wird und die angemessene Sicherheit der Systeme oder des Datentransfers sicherstellt<br>[ISO/IEC 7498]                                                                                                                                         |

| Begriff auf Englisch                                                                                                                                                                                                                                                                                                                                                 | Begriff auf Deutsch                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>security subject</b><br>active entity, generally in the form of a person, process or device, that causes information to flow among objects or changes the system state<br>Note 1 to entry: Technically, a process/domain pair.                                                                                                                                    | <b>Sicherheitssubjekt</b><br>aktive Entität, normalerweise in Form einer Person, eines Prozesses oder Gerätes, die einen Informationsfluss zwischen Objekten oder Änderungen des Systemstatus verursacht<br>Anmerkung 1 zum Eintrag: Technisch gesehen ein Prozess/Domäne-Paar.                                                                                                                                                                                     |
| <b>subject</b><br>entity whose public key is certified in the certificate                                                                                                                                                                                                                                                                                            | <b>Subjekt</b><br>Entität, deren öffentlicher Schlüssel im Zertifikat zertifiziert ist                                                                                                                                                                                                                                                                                                                                                                              |
| <b>subject of care</b><br>person that is the receiver of health related services and that is a person in a health information system                                                                                                                                                                                                                                 | <b>Behandelte(r) bzw. zu Behandelnde(r)</b><br>Person, die Dienstleistungen des Gesundheitswesens erhält und die eine Person in einem Gesundheitssystem ist                                                                                                                                                                                                                                                                                                         |
| <b>third party</b><br>party other than data originator, or data recipient, required to perform a security function as part of a communication protocol                                                                                                                                                                                                               | <b>Dritte(r)</b><br>Partei, die nicht der Datenurheber oder Datenempfänger ist, die eine Sicherheitsfunktion als Teil eines Kommunikationsprotokolls ausführen muss                                                                                                                                                                                                                                                                                                 |
| <b>trusted third party</b><br><b>TTP</b><br>third party which is considered trusted for purposes of a security protocol<br>[ENV 13608-1]<br>Note 1 to entry: This term is used in many ISO/IEC standards and other documents describing mainly the services of a CA. The concept is however broader and includes services like time stamping and possibly escrowing. | <b>vertrauenswürdige(r) Dritte(r)</b><br>Dritte, die im Zusammenhang mit einem Sicherheitsprotokoll als vertrauenswürdig gelten<br>[ENV 13608-1]<br>Anmerkung 1 zum Eintrag: 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. |

— Leerseite —

English Version

Health informatics - Directory services for healthcare providers,  
subjects of care and other entities (ISO 21091:2013)

Informatique de santé - Services d'annuaires pour les  
fournisseurs de soins de santé, les sujets de soins et  
autres entités (ISO 21091:2013)

Medizinische Informatik - Verzeichnisdienste für Anbieter,  
zu Behandelnde und andere Entitäten im  
Gesundheitswesen (ISO 21091:2013)

This European Standard was approved by CEN on 2 February 2013.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

## Contents

Page

|                                                            |    |
|------------------------------------------------------------|----|
| Foreword.....                                              | 3  |
| Introduction .....                                         | 4  |
| 1 Scope.....                                               | 5  |
| 2 Normative references .....                               | 5  |
| 3 Terms and definitions.....                               | 5  |
| 4 Symbols (and abbreviated terms).....                     | 9  |
| 5 Healthcare context.....                                  | 10 |
| 5.1 General .....                                          | 10 |
| 5.2 Healthcare persons .....                               | 11 |
| 5.3 Multiple affiliations .....                            | 11 |
| 5.4 Healthcare organizations .....                         | 12 |
| 5.5 Hardware/software.....                                 | 12 |
| 5.6 Healthcare security services.....                      | 12 |
| 6 Directory security management framework.....             | 12 |
| 7 Interoperability.....                                    | 13 |
| 7.1 Requirements.....                                      | 13 |
| 7.2 Name space/tree structure .....                        | 13 |
| 8 Healthcare schema .....                                  | 15 |
| 8.1 Healthcare persons .....                               | 15 |
| 8.2 Organization identities .....                          | 22 |
| 8.3 Roles, Job Function and Group.....                     | 27 |
| 9 Distinguished Name .....                                 | 32 |
| 9.1 General .....                                          | 32 |
| 9.2 Relative Distinguished Name.....                       | 33 |
| Annex A (informative) Healthcare directory scenarios ..... | 36 |
| Annex B (informative) Referenced object classes.....       | 44 |
| Bibliography .....                                         | 51 |

## **Foreword**

This document (EN ISO 21091:2013) 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 European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2013, and conflicting national standards shall be withdrawn at the latest by August 2013.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

### **Endorsement notice**

The text of ISO 21091:2013 has been approved by CEN as EN ISO 21091:2013 without any modification.

## **Introduction**

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

The directory is becoming an increasingly popular method of providing a means for single sign-on capabilities to support authentication. This goal has resulted in the inclusion of authentication and identity attributes to authenticate the identity of a healthcare person or entity.

The directory also supports the communication of additional attributes that can be used to support authorization decisions. This goal has driven directory schema extensions to include organization employee management information, healthcare-specific contact information, and healthcare identifiers. This International Standard addresses the healthcare-specific requirements of the directory, and defines, as appropriate, standard specifications for inclusion of this information in the healthcare directory.

Besides technical security measures that are discussed in other ISO standards, communication of healthcare data requires a reliable accountable “chain of trust.” In order to maintain this chain of trust within a public key infrastructure, users (relying parties) need to be able to obtain current correct certificates and certificate status information through secure directory management.

The healthcare directory will support standard lightweight directory access protocol (LDAP) client searches, interface engines for message transformation, and service oriented architecture (SOA) implementations to enable the service in any environment. Specific implementation guidance, search criteria and support are outside the scope of this International Standard.

While specific security measures and access control specifications are out of scope of this International Standard, due to the sensitive nature of health related and privacy information that may be supported through the directory services, significant controls need to be enabled at branch, object classes, and attribute levels. Processes and procedures should be in place to ensure information integrity represented within the health directory, and responsibility for the content of the directory should be clearly allocated through policy and process. It is anticipated that appropriate access controls managing who can read, write or modify all items in the healthcare directory will be applied. This may be accomplished by assigning individuals within the directory to the HCOrganizationalRole and assigning appropriate privileges (e.g. read, modify, delete) to that role in directory management configuration.

## 1 Scope

This International Standard defines minimal specifications for directory services for healthcare. It can be used to enable communications between organizations, devices, servers, application components, systems, technical actors, and devices.

This International Standard provides the common directory information and services needed to support the secure exchange of healthcare information over public networks where directory information and services are used for these purposes. It addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction, and international healthcare communications. While several options are supported by this International Standard, a given service will not need to include all of the options.

In addition to the support of security services, such as access control and confidentiality, this International Standard provides specification for other aspects of communication, such as addresses and protocols of communication entities.

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

## 2 Normative references

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

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

## 3 Terms and definitions

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

### 3.1

#### **access control**

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

[ISO/IEC 2382-8]

### 3.2

#### **attribute authority**

##### **AA**

authority which assigns privileges by issuing attribute certificates

[X.509]

### 3.3

#### **attribute certificate**

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

[X.509]

### 3.4

#### **authentication**

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

[ISO 7498-2]

### 3.5

#### **authorization**

granting of rights, which includes the granting of access based on access rights

[ISO 7498-2]

### 3.6

#### **availability**

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

[ISO 7498-2]

### 3.7

#### **certificate**

public key certificate

### 3.8

#### **certificate distribution**

act of publishing certificates and transferring certificates to security subjects

### 3.9

#### **certificate issuer**

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

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

[ISO/IEC 9594-8]

### 3.10

#### **certificate management**

procedures relating to certificates, i.e. certificate generation, certificate distribution, certificate archiving and revocation

### 3.11

#### **certificate revocation**

act of removing any reliable link between a certificate and its related owner (or security subject owner) because the certificate is not trusted any more, even though it is unexpired

### 3.12

#### **certificate revocation list**

##### **CRL**

published list of the suspended and revoked certificates (digitally signed by the CA)

### 3.13

#### **certificate verification**

verifying that a **certificate** (3.7) is authentic

### 3.14

#### **certification authority**

##### **CA**

authority trusted by one or more relying parties to create and assign certificates and which may, optionally, create the relying parties' keys

NOTE 1 Adapted from ISO/IEC 9594-8.

NOTE 2 Authority in the CA term does not imply any government authorization, but only denotes that it is trusted.

NOTE 3 "Certificate issuer" may be a better term, but CA is very widely used.

### 3.15

#### **confidentiality**

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

[ISO 7498-2]

### 3.16

#### **data integrity**

property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

### 3.17

#### **digital signature**

data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[ISO 7498-2]

### 3.18

#### **identification**

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

[ISO/IEC 2382-8]

### 3.19

#### **identifier**

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

[ENV 13608-1]

### 3.20

#### **integrity**

property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

### 3.21

#### **key**

sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2]

### 3.22

#### **key management**

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

[ISO 7498-2]

### 3.23

#### **lightweight directory access protocol**

##### **LDAP**

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

### 3.24

#### **object identifier**

##### **OID**

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

### 3.25

#### **privacy**

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

[ISO/IEC 2382-8]

### 3.26

#### **private key**

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

[ISO/IEC 10181-1]

### 3.27

#### **public key**

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

[ISO/IEC 10181-1]

### 3.28

#### **public key certificate**

##### **PKC**

certificate that binds an identity and a public key

[RFC 3280]

### 3.29

#### **public key infrastructure**

##### **PKI**

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

### 3.30

#### **relying party**

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

[RFC 3647]

### 3.31

#### **role**

set of competences and/or performances associated with a task

### 3.32

#### **security**

combination of availability, confidentiality, integrity and accountability

[ENV 13608-1]

### 3.33

#### **security policy**

plan or course of action adopted for providing computer security

[ISO/IEC 2382-8]

### 3.34

#### **security service**

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

[ISO/IEC 7498]

### 3.35

#### **security subject**

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

NOTE      Technically, a process/domain pair.

### 3.36

#### **subject**

entity whose public key is certified in the certificate

### 3.37

#### **subject of care**

person scheduled to receive, receiving, or having received healthcare

### 3.38

#### **third party**

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

### 3.39

#### **trusted third party**

#### **TTP**

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

[ENV 13608-1]

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

## 4 Symbols (and abbreviated terms)

|     |                             |
|-----|-----------------------------|
| CA  | Certification Authority     |
| CN  | Common Name                 |
| CRL | Certificate Revocation List |

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

## **5 Healthcare context**

### **5.1 General**

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

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

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

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

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