

DIN EN ISO 22600-3

ICS 35.240.80

**Medizinische Informatik –
Privilegmanagement und Zugriffssteuerung –
Teil 3: Implementierungen (ISO 22600-3:2014);
Deutsche Fassung EN ISO 22600-3:2014**

Health informatics –
Privilege management and access control –
Part 3: Implementations (ISO 22600-3:2014);
German version EN ISO 22600-3:2014

Informatique de santé –
Gestion de privilèges et contrôle d'accès –
Partie 3: Mises en oeuvre (ISO 22600-3:2014);
Version allemande EN ISO 22600-3:2014

Gesamtumfang 83 Seiten

DIN-Normenausschuss Medizin (NAMed)

Nationales Vorwort

Die vorliegende Norm enthält die deutsche Übersetzung der ISO 22600-3:2014, die vom Technischen Komitee ISO/TC 215 „Health Informatics“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ (Sekretariat: NEN, Niederlande) unter Beteiligung deutscher Experten erarbeitet wurde. Von deutscher Seite ist hierfür der DIN-Normenausschuss Medizin (NAMed), Arbeitsausschuss NA 063-07-04 AA „Sicherheit“ zuständig.

Die Festlegungen der ISO 22600-3 wurden sachlich unverändert in diese Deutsche Norm übernommen. Bei der Übersetzung wurde auf eine einwandfreie und durchgängige Terminologie der verwendeten deutschen Fachbegriffe geachtet. Die jeweils englischen Benennungen sind im Abschnitt 3 „Begriffe“ mit aufgeführt. Die Bilder 1 und 3, die Tabellen 2 und C.1 und die in den Anhängen A und D aufgeführten Programmzeilen wurden im englischen Original beibehalten, da ihre Übersetzung nicht notwendig erschien und die angesprochene IT-Zielgruppe üblicherweise über ausreichende Englischkenntnisse verfügt.

Die Normenreihe DIN EN ISO 22600 unter dem allgemeinen Titel *Medizinische Informatik — Privilegienmanagement und Zugriffssteuerung* besteht aus folgenden Teilen:

- *Teil 1: Übersicht und Policy-Management*
- *Teil 2: Formale Modelle*
- *Teil 3: Implementierungen*

Deutsche Fassung

Medizinische Informatik —
Privilegienmanagement und Zugriffssteuerung —
Teil 3: Implementierungen (ISO 22600-3:2014)

Health informatics —
Privilege management and access control —
Part 3: Implementations (ISO 22600-3:2014)

Informatique de santé —
Gestion de privilèges et contrôle d'accès —
Partie 3: Mises en oeuvre (ISO 22600-3:2014)

Diese Europäische Norm wurde vom CEN am 21. Juni 2014 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Vorwort	3
Einleitung.....	4
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Abkürzungen	22
5 Strukturen und Dienste für Privilegienmanagement und Zugriffssteuerung	23
6 Interpretation der in ISO 22600-2 festgelegten formalen Modelle in Umgebungen des Gesundheitswesens	26
7 Begriffsdarstellung für Informationssysteme im Gesundheitswesen	27
7.1 Übersicht	27
7.2 Domainsprachen	27
7.3 OCL-Randbedingungsmodellierung	28
7.4 Sonstige Randbedingungsdarstellungen	29
8 Einverständniserklärung	31
8.1 Übersicht	31
8.2 Einverständniserklärung des Patienten	31
8.3 Verwaltung der Einverständniserklärungen von Patienten	31
9 Zugriff im Notfall	31
10 Verfeinerung des Steuerungsmodells	31
11 Verfeinerung des Delegierungsmodells	32
Anhang A (informativ) Infrastruktur für das Privilegienmanagement	33
Anhang B (informativ) Attributzertifikatserweiterungen	74
Anhang C (informativ) Terminologievergleich	76
Anhang D (informativ) Beispiele für das Policy-Management und die Policy-Darstellung	77
Literaturhinweise	80

Vorwort

Dieses Dokument (EN ISO 22600-3:2014) wurde vom Technischen Komitee ISO/TC 215 „Health Informatics“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ erarbeitet, dessen Sekretariat vom NEN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis April 2015, und etwaige entgegenstehende nationale Normen müssen bis April 2015 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 22600-3:2014 wurde vom CEN als EN ISO 22600-3:2014 ohne irgendeine Abänderung genehmigt.

Einleitung

Die verteilte Architektur von gemeinsam genutzten Informationssystemen im Gesundheitswesen zur Unterstützung der serviceorientierten Architektur (SOA) ist zunehmend auf Firmennetzwerke und virtuelle Privatnetze orientiert. Um der Herausforderung der Interoperabilität gerecht zu werden, werden immer häufiger genormte Benutzerschnittstellen, Tools und Protokolle verwendet, wodurch die Unabhängigkeit der Plattform sichergestellt wird. Auch die Anzahl der tatsächlich offenen Informationssysteme ist in den letzten Jahren rasch angestiegen.

Gegenwärtig werden Krankenhäuser gemeinhin von mehreren Anbietern unterstützt, die verschiedene Anwendungen zur Verfügung stellen, die nicht in der Lage sind, Authentisierungen und Autorisierungen zu kommunizieren, weil sie diese Funktionen auf jeweils unterschiedliche Art und Weise handhaben. Zur Erreichung eines einheitlichen Szenarios ist ein erheblicher finanzieller, zeitlicher und arbeitstechnischer Aufwand erforderlich, um Benutzer und sich verändernde Organisationsumgebungen dynamisch vor Beginn der Kommunikation und Kooperation aufeinander abzubilden. Die für die Entwicklung und Pflege von Sicherheitsfunktionen erforderlichen Ressourcen wachsen exponentiell mit der Anzahl der Anwendungen, mit der Komplexität von Organisationen in Ausrichtung auf die regionale, nationale und auch internationale Ebene und mit der Flexibilität von Benutzern, die mehrfache Rollen manchmal sogar simultan spielen, an.

Die Lage wird bei organisationsübergreifender Kommunikation noch herausfordernder, weil in diesem Falle die Grenzen von Domains überschritten werden, die durch entsprechende Sicherheits-Policies geregelt werden. Von einem medizinischen Versorgungszentrum zum nächsten und von Land zu Land können für ähnliche Arten von Benutzern sowohl in Bezug auf die Ausübung spezieller Funktionen als auch auf den Zugriff auf Informationen unterschiedliche Regeln zu den Privilegien und zu deren Management gelten. Die Unterschiede zwischen diesen Domains in Bezug auf die geltenden Policies müssen automatisch oder durch entsprechende Policy-Vereinbarungen überbrückt werden, die eine Reihe von allen Beteiligten zu befolgenden Regeln festlegen, um eine Interoperabilität zu erreichen.

Eine weitere Herausforderung liegt in der Art und Weise, wie die Qualität im Gesundheitswesen durch die Nutzung von IT zu verbessern ist, ohne die Privatsphäre des Patienten zu verletzen. Um den Ärzten alle erforderlichen Informationen über den Patienten zur Verfügung stellen zu können, ist eine virtuelle elektronische Gesundheitsakte erforderlich, die es ermöglicht, sämtliche an einem Patienten durchgeführten Aktivitäten zu verfolgen – unabhängig davon, wo oder von wem sie vorgenommen und dokumentiert wurden. In einer solchen Umgebung ist ein generisches Modell oder eine spezielle Vereinbarung zwischen den beteiligten Parteien zum Privilegienmanagement und zur Zugriffssteuerung einschließlich des Patienten oder seines Vertreters erforderlich.

Neben der für alle Arten von großen Organisationen typischen Vielzahl unterschiedlicher Rollen und Verantwortlichkeiten sind im Gesundheitswesen wegen der Sensitivität der zu verwaltenden personenbezogenen Gesundheitsinformationen und deren persönlichen und sozialen Einfluss auch ethische und rechtliche Aspekte zu berücksichtigen.

Schon heute sind moderne Lösungen für das Privilegienmanagement und die Zugriffssteuerung erforderlich, die damit verbundenen Herausforderungen werden aber in den nächsten Jahren noch zunehmen. Der Grund hierfür liegt in der Zunahme an Informationen, die zwischen den einzelnen Systemen ausgetauscht werden, um den Bedarf der Gesundheitsdienstleister auf verschiedenen Pflegestufen den Zugriff auf immer mehr patientenbezogene Informationen im Sinne der Sicherstellung von Qualität und Effizienz bei der Diagnose und Behandlung des Patienten zu erfüllen; jedoch kombiniert mit erhöhten Sicherheits- und Datenschutzrisiken.

Die Implementierung der vorliegenden Internationalen Norm kann sich gegenwärtig noch als zu anspruchsvoll gestalten und daher in bestimmten organisatorischen und technischen Umgebungen ungeeignet sein. Um dem Grundsatz des Strebens nach dem Bestmöglichen gerecht zu werden, ist es daher sehr wichtig, dass die beteiligten Parteien mindestens eine schriftliche Policy-Vereinbarung treffen, der sich entnehmen lässt, dass die Beteiligten bei jeder geplanten Aktualisierung oder Erweiterung der betreffenden Systeme in der durch diese Internationale Norm vorgegebenen Richtung vorgehen werden. Der Grad der Formalisierung und Granularität der Policies und die Objekte dieser Policies ist daran gebunden, die Lösung in Richtung der vorgestellten Spezifikation festzulegen.

Die Policy-Vereinbarung muss auch festgestellte Unterschiede zwischen den betreffenden Sicherheitssystemen und die zu deren Überwindung vereinbarten Lösungen enthalten. So müssen z. B. der Authentisierungsdienst und die Privilegien einer anfordernden Partei auf der antwortenden Seite nach der in der Vereinbarung festgelegten Policy verwaltet werden. Aus diesem Grund müssen sowohl diejenigen, die Informationen und Dienstleistungen anfordern und/oder sie bereitstellen, als auch die angeforderten und bereit gestellten Informationen und Dienste in einer begrenzten Anzahl von Konzepten zusammengefasst und klassifiziert werden, um die Festlegung einer begrenzten Anzahl von Lösungskategorien zu ermöglichen. Basierend auf dieser Klassifizierung können dann Anwarterprozesse, Zielsensibilitätsprozesse und Policies über Festlegungs- und Managementprozesse implementiert werden. Sobald alle Beteiligten die Policy-Vereinbarung unterzeichnet haben, können die Kommunikation und der Informationsaustausch mit den vorhandenen Systemen gestartet werden, sofern die beteiligten Parteien die damit verbundenen Risiken akzeptieren können. Falls Risiken bestehen, die als unannehmbar gelten und noch vor Beginn des Informationsaustauschs beseitigt werden müssen, sind diese ebenfalls in der Policy-Vereinbarung festzuhalten und zwar in Verbindung mit einem Maßnahmenplan, aus dem hervorgeht, auf welche Art und Weise diese Risiken zu beseitigen sind. Die Policy-Vereinbarung muss darüber hinaus einen Zeitplan für diese Aktionen und eine Vereinbarung zu deren Finanzierung enthalten.

Die Dokumentation des Verhandlungsprozesses ist sehr wichtig und bildet die Plattform für die Policy-Vereinbarung.

Das Privilegienmanagement und die Zugriffssteuerung gelten für die Sicherheits- und Datenschutzdienste, die für die Kommunikation und Kooperation, d. h. für die verteilte Nutzung von gesundheitsbezogenen Informationen erforderlich sind. Dies schließt auch Sicherheitsaspekte, professionelle Standards sowie rechtliche und ethische Gesichtspunkte ein. Diese Internationale Norm führt Grundsätze ein und spezifiziert Dienste, die für das Management von Privilegien und für die Zugriffssteuerung erforderlich sind. Die Verschlüsselungsprotokolle sind nicht Gegenstand dieser Internationalen Norm.

Diese aus drei Teilen bestehende Internationale Norm verweist auf bestehende architektur- und sicherheitsbezogene Normen sowie auf Spezifikationen für den Bereich des Gesundheitswesens, wie z. B. von ISO, CEN, ASTM, OMG, W3C und unterstützt bestehende einschlägige Normen oder benennt Erweiterungen oder Änderungen oder weist auf den Bedarf an neuen Normen hin. Die Norm besteht aus:

- ISO 22600-1: beschreibt die für den Informationsaustausch über die Grenzen von Policy-Domains hinweg geltenden Szenarien und die wesentlichen Parameter. Außerdem enthält dieser Teil Beispiele für die als Grundlage der Policy-Vereinbarung erforderlichen Dokumentationsverfahren.
- ISO 22600-2: beschreibt und erläutert ausführlich die Architekturen und zugrundeliegenden Modelle für das Privilegienmanagement und die Zugriffssteuerung, die für die Sicherheit bei der gemeinsamen Nutzung von Informationen erforderlich sind, einschließlich der formalen Darstellung von Policies.
- ISO 22600-3: beschreibt Beispiele für implementierbare Spezifikationen von Anwendungssicherheitsdiensten und Infrastrukturdiensten mit Hilfe verschiedener Spezifikationssprachen.

Sie ermöglicht die Überbrückung von Policies. Sie basiert auf einem begrifflichen Modell, bei dem örtliche Autorisierungsserver und grenzüberschreitende Verzeichnis- und Policy-Repository-Dienste für die Zugriffssteuerung in verschiedenen Anwendungen (Softwarekomponenten) dienen können. Das Policy-Repository liefert Informationen zu den Regeln für den Zugriff auf unterschiedliche Anwendungsfunktionen basierend auf Rollen und anderen Attributen. Der Verzeichnisdienst ermöglicht es, den jeweiligen Benutzer zu identifizieren. Ob das Zugriffsrecht erteilt wird, hängt von den folgenden vier Aspekten ab:

- der authentisierten Identifikation der beteiligten Auftraggeber (d. h. menschliche Benutzer und Objekte, die unter ihren eigenen Rechten arbeiten müssen);
- den Regeln für den Zugriff auf ein bestimmtes Informationsobjekt einschließlich Verwendungszweck;
- den Regeln bezüglich der mit dem Auftraggeber verknüpften und vom Berechtigungsmanager bereitgestellten Autorisierungsattribute;
- den Funktionen der betreffenden Anwendung.

Diese Internationale Norm unterstützt die Zusammenarbeit zwischen mehreren Autorisierungsmanagern, die über die Grenzen von Organisationen oder Policies hinaus tätig werden können.

Diese Internationale Norm ist eng mit anderen Projekten des ISO/TC 215 verbunden, so z. B. mit ISO 17090, ISO 22857, ISO 21091 und ISO 21298.

Die vorliegende Internationale Norm ist in Verbindung mit dem gesamten Satz der dazugehörigen Normen zu lesen.

Basierend auf dem vereinheitlichten Prozess wurde ein dreidimensionales architektonisches Referenzmodell für die Festlegung der erforderlichen Randbedingungsmodelle abgeleitet. Die Dimensionen des verwendeten Generischen Komponentenmodells sind die Domainachse, die Achse der Dekomposition/Komposition und die Achse, die die Sichtweisen auf ein System und seine Komponenten beschreibt. Um Zukunftssicherheit, Nachhaltigkeit, Flexibilität, Übertragbarkeit und Skalierbarkeit sicherzustellen, werden nur der Prozess der Festlegung der Randbedingungen und die sich daraus ergebenden sicherheitsbezogenen Metamodelle vorgestellt. Bei der Instanziierung und Implementierung, z. B. der Festlegung von Verfahren und Verschlüsselungsdefinitionen, handelt es sich um einen lang andauernden Prozess, der anderen Normen und Projekten oder der Anbieter- bzw. Providergemeinde gewidmet ist.

Nach einer kurzen Zusammenfassung der in ISO 22600-2 wiedergegebenen Grundlagen werden die unterschiedlichen Möglichkeiten zur Darstellung der unterschiedlichen Reifegrade bei unterschiedlichen Graden der Interoperabilität unter der idealen Situation einer semantisch gültigen Stufe erörtert.

Für diese unterschiedlichen Umgebungen und Grade bzw. Stufen gibt dieser Teil von ISO 22600 Beispiele für die Spezialisierung und Implementierung der auf ISO/IEC 10746 basierenden und in ISO 22600-2 festgelegten formalen High-Level-Modelle für Architekturkomponenten. Diese Beispiele und dazugehörige Dienste werden in verschiedenen Anhängen zusammengefasst.

Die Spezifikationen werden mit Hilfe von Derivaten der erweiterbaren Auszeichnungssprache XML, d. h. in erster Linie in den von OASIS festgelegten Sprachen Security Assertion Markup Language (SAML) und Extensible Access Control Markup Language (XACML) angegeben. Zusätzliche Spezifikationen werden auch in der traditionellen ASN.1-Syntax dargestellt.

Diese Internationale Norm wurde in wesentlichen Teilen mit ASTM E2595-07 harmonisiert.

1 Anwendungsbereich

Diese mehrteilige Internationale Norm legt Grundsätze fest und spezifiziert die für das Privilegienmanagement und die Zugriffssteuerung auf Daten und Funktionen erforderlichen Dienste.

Sie konzentriert sich auf die Kommunikation und Nutzung von gesundheitsbezogenen Informationen, die über die Grenzen von Policy-Domains hinweg verteilt werden. Das umfasst die gemeinsame Nutzung von gesundheitsbezogenen Informationen durch nicht miteinander verbundene Anbieter und Organisationen des Gesundheitswesens, Krankenversicherungen, deren Patienten, Mitarbeiter und Handelspartner sowohl durch Einzelpersonen als auch durch Anwendungssysteme im Bereich von einer lokalen zu einer regionalen oder auch nationalen Situation.

Sie legt die erforderlichen komponentenbasierten Begriffe fest und soll deren technische Implementierung unterstützen. Sie legt jedoch nicht fest, wie diese Begriffe in speziellen klinischen Prozessabläufen zu verwenden sind.

Dieser Teil von ISO 26000 instanziiert Anforderungen an Repositories für Zugriffssteuerungs-Policies und Anforderungen an Infrastrukturen für das Privilegienmanagement. Er gibt Beispiele für die Implementierung der in ISO 22600-2 spezifizierten formalen Modelle.

Dieser Teil von ISO 22600 enthält weder plattformspezifische noch implementierungstechnische Einzelheiten. Sie legt keine technischen Kommunikationssicherheitsdienste, Authentisierungsverfahren und -protokolle fest, die bereits in anderen Internationalen Normen festgelegt sind, wie z. B. in ISO 7498-2, ISO/IEC 10745 (ITU-T X.803), ISO/IEC TR 13594 (ITU-T X.802), ISO/IEC 10181-1 (ITU-T X.810), ISO/IEC 9594-8 (ITU-T X.509), ISO/IEC 9796 (alle Teile), ISO/IEC 9797 (alle Teile) und ISO/IEC 9798 (alle Teile).

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

ISO/IEC 10181-3, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework — Part 3*

ASTM E2084-00, *Standard Specification for Authentication of Healthcare Information Using Digital Signatures*

3 Begriffe

3.1

Zugriffssteuerung

(en: access control)

Mittel zur Sicherstellung, dass nur autorisierte Entitäten in entsprechend autorisierter Weise Zugriff auf die Ressourcen eines Datenverarbeitungssystems nehmen können

[QUELLE: ISO/IEC 2382-8:1998]

3.2

Entscheidungsfunktion der Zugriffssteuerung

(en: access control decision function, ADF)

spezialisierte Funktion, die durch Anwenden der Regeln einer Zugriffssteuerungs-Policy Zugriffsentscheidungen für eine angeforderte Aktion trifft

3.3

Durchsetzungsfunktion der Zugriffssteuerung

(en: access control enforcement function, AEF)

spezialisierte Funktion, die Bestandteil des Zugriffspfades zwischen einem Anforderer (en: requester) und einer geschützten Ressource ist, die die von der ADF getroffenen die Entscheidungen durchsetzt

3.4

Zugriffssteuerungsinformation(en)

(en: access control information)

Information, die für die Zwecke der Zugriffssteuerung verwendet wird, einschließlich kontextueller Informationen

3.5

Zurechenbarkeit

(en: accountability)

Eigenschaft, durch die sichergestellt wird, dass die Handlungen einer Entität eindeutig auf diese zurückverfolgt werden können

[QUELLE: ISO 7498-2:1989]

3.6

asymmetrischer Verschlüsselungsalgorithmus

(en: asymmetric cryptographic algorithm)

Algorithmus für die Ausführung einer Chiffrierung oder einer entsprechenden Dechiffrierung, bei der für Chiffrierung und Dechiffrierung unterschiedliche Schlüssel zur Anwendung kommen

[QUELLE: ISO/IEC 10181-1:1996]

3.7

Attributautorisierer

(en: attribute authority, AA)

Behörde, die durch Ausgabe von Attributzertifikaten Privilegien zuweist

[QUELLE: ISO/IEC 9594-8:2008]

3.8

Sperrliste des Attributautorisierers

(en: attribute authority revocation list, AARL)

Sperrliste, die eine Liste von Verweisungen auf an Attributautorisierer ausgegebene Attributzertifikate enthält, die von der Behörde, die das Zertifikat ausgegeben hat, als nicht mehr gültig angesehen werden

3.9

Attributzertifikat

(en: attribute certificate)

digital von einem Attributautorisierer signierte Datenstruktur, die einige Attributwerte mit einer Identifikation über ihren Halter bindet

[QUELLE: ISO/IEC 9594-8 :2008]

3.10

Attributzertifikate-Sperrliste

(en: attribute certificate revocation list, ACRL)

Sperrliste, die eine Liste von Verweisungen auf Attributzertifikate enthält, die von der Behörde, die das Zertifikat ausgegeben hat, als nicht mehr gültig angesehen werden

3.11

Authentisierung

(en: authentication)

Beibringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators

[QUELLE: ISO/IEC 15944-5:2008, 3.5]

Anmerkung 1 zum Begriff: Siehe auch Authentisierung des Absenders der Daten und Authentisierung der Partnerinstanz.

3.12

Authentisierungs-Token

(en: authentication token)

im Rahmen eines für eine starke Authentisierung vorgesehenen Austauschs übermittelte Information, die zur Authentisierung ihres Absenders verwendet werden kann

3.13

Autorisierer

Behörde, Autorität

(en: authority)

Entität, die für die Ausgabe von Zertifikaten verantwortlich ist

Anmerkung 1 zum Begriff: In diesem Teil von ISO 22600 werden zwei Typen unterschieden: die Zertifizierungsstelle, die Public-Key-Zertifikate ausgibt, und der Attributautorisierer, der Attributzertifikate ausgibt.

3.14

Autoritätszertifikat

(en: authority certificate)

an eine Zertifizierungsstelle oder einen Attributautorisierer ausgegebenes Zertifikat

[QUELLE: ISO/IEC 9594-8:2008, modifiziert]

3.15

Behördensperrliste

(en: authority revocation list, ARL)

Sperrliste, die eine Liste von an Behörden ausgegebenen Public-Key-Zertifikaten enthält, die vom Zertifikatsaussteller als nicht mehr gültig angesehen werden

3.16

Autorisierung

(en: authorisation)

Erteilung von Privilegien, einschließlich des Privilegs für den Zugriff auf Daten und Funktionen

[QUELLE: ISO 7498-2:1989, modifiziert]

3.17

Autoritätszertifikat

(en: authority certificate)

an eine Behörde (z. B. an eine Zertifizierungsstelle oder einen Attributautorisierer) ausgegebenes Zertifikat

3.18

Autorisierungsnachweis

(en: authorization credential)

signierte Geltendmachung (en: assertion) der Erlaubnisattribute eines Benutzers

3.19

Verfügbarkeit

(en: availability)

Eigenschaft, auf Anforderung einer autorisierten Entität zugänglich und nutzbar zu sein

[QUELLE: ISO 7498-2:1989]

3.20

Basis-CRL

(en: base CRL)

CRL, die als Grundlage für die Erzeugung einer Delta-CRL verwendet wird

3.21

Geschäftsvereinbarung

(en: Business Partner Agreement)

Dokument, das zur Abgrenzung der rechtlichen, ethischen und praktischen Verantwortlichkeiten zwischen den Subskribenten einer PMI und zwischen miteinander kooperierenden PMI-Implementierungen verwendet wird

3.22

CA-Zertifikat

(en: CA certificate)

Zertifikat, das einer Zertifizierungsstelle (CA) von einer anderen Zertifizierungsstelle ausgestellt wird

3.23

Zertifikat

(en: certificate)

Public-Key-Zertifikat

3.24

Zertifikatsverteilung

(en: certificate distribution)

Vorgang der Veröffentlichung von Zertifikaten und der Übertragung von Zertifikaten auf Sicherheitssubjekte

3.25

Zertifikatsverwaltung

(en: certificate management)

Prozeduren, die sich Zertifikate beziehen: Zertifikatserzeugung, Zertifikatsverteilung, Zertifikatsarchivierung und Sperrung von Zertifikaten

3.26

Zertifikats-Policy

(en: certificate policy)

benannte Reihe von Regeln, die die Anwendbarkeit eines Zertifikats auf eine bestimmte Community und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen anzeigen

Anmerkung 1 zum Begriff: So kann z. B. eine Zertifikats-Policy die Anwendbarkeit eines bestimmten Zertifikatstyps bei der Authentisierung von elektronischen Datenaustausch-Transaktionen für den Handel von Waren innerhalb einer gegebenen Preisspanne anzeigen.

3.27

Widerruf bzw. Sperrung eines Zertifikats

(en: certificate revocation)

Vorgang der Beseitigung aller zuverlässigen Verknüpfungen zwischen einem Zertifikat und seinem Zertifikathalter, weil dem betreffenden Zertifikat, obgleich seine Gültigkeitsdauer noch nicht abgelaufen ist, nicht mehr vertraut wird

3.28

Zertifikatesperrliste

(en: certificate revocation list, CRL)

signierte Liste, die eine Menge von Zertifikaten anzeigt, die vom Zertifikatsaussteller als nicht mehr gültig angesehen werden

Anmerkung 1 zum Begriff: Zusätzlich zum Oberbegriff der CRL werden einige spezielle CRL-Typen für CRLs definiert, die besondere Anwendungsbereiche abdecken. Eine (von der Zertifizierungsstelle digital signierte) veröffentlichte Liste der suspendierten und widerrufenen Zertifikate.

3.29

laufende Nummer des Zertifikats

(en: certificate serial number)

ganzzahliger Wert, der innerhalb des Wirkungsbereichs der ausstellenden Behörde nur einmal verwendet wird und eindeutig zu einem von dieser Zertifizierungsstelle ausgestellten Zertifikat gehört

3.30

Liste der suspendierten Zertifikate

(en: certificate suspension list, CSL)

(von der Zertifizierungsstelle digital signierte) veröffentlichte Liste der suspendierten Zertifikate

3.31

Zertifikatsnutzer

(en: certificate user)

Entität, die den öffentlichen Schlüssel einer anderen Entität mit Gewissheit kennen muss

3.32

System, das das Zertifikat nutzt

(en: certificate using system)

Implementierung derjenigen der in diesem Teil von ISO 22600 festgelegten Funktionen, die von einem Zertifikatbenutzer verwendet werden

3.33

Zertifikatsvalidierung

(en: certificate validation)

Prozess der Sicherstellung, dass ein Zertifikat zu einem bestimmten Zeitpunkt gültig war, gegebenenfalls einschließlich der Struktur und Verarbeitung eines Zertifizierungspfades, und der Sicherstellung, dass alle Zertifikate in diesem Pfad zu diesem Zeitpunkt gültig (d. h. nicht abgelaufen oder widerrufen) waren

3.34

Zertifikatsüberprüfung

(en: certificate verification)

Überprüfung eines Zertifikats auf seine Authentizität

3.35

Zertifizierungsstelle

Zertifikatsaussteller

(en: certification authority, CA)

Behörde, die von einer oder mehreren vertrauenden Parteien als vertrauenswürdig erachtet wird, um Zertifikate erstellen, zuweisen und verwalten zu können

[QUELLE: ISO/IEC 9594-8:2008]

Anmerkung 1 zum Begriff: Wahlweise kann die Zertifizierungsstelle die Schlüssel der vertrauenden Parteien erzeugen.

Anmerkung 2 zum Begriff: Entität, die Zertifikate durch Signieren von Zertifikatsdaten mit ihrem privaten Signaturschlüssel ausgibt.

ANMERKUNG 2 Die Bezeichnung als Behörde meint in diesem Zusammenhang keine Regierungsbehörde, sondern nur, dass die betreffende Einrichtung als vertrauenswürdig erachtet wird. Zertifikatsaussteller (en: certificate issuer) ist

möglicherweise die bessere Benennung, Zertifizierungsstelle (en: certification authority, CA) ist aber wesentlich gebräuchlicher.

3.36

Sperrliste der Zertifizierungsstelle

(en: certification authority revocation list, CARL)

Sperrliste, die eine Liste von an Zertifizierungsstellen ausgegebenen Public-Key-Zertifikaten enthält, die vom Zertifikatsaussteller als nicht mehr gültig angesehen werden

3.37

Zertifizierungspfad

(en: certification path)

geordnete Abfolge der Zertifikate von Objekten im DIT, die zusammen mit dem öffentlichen Schlüssel des Ausgangsobjektes im Pfad verarbeitet werden können, um den Schlüssel des letzten Objektes im Pfad zu ermitteln

3.38

chiffrierter Text

(en: ciphertext)

Daten, die durch Anwendung einer Verschlüsselung erzeugt wurden

Anmerkung 1 zum Begriff: Der semantische Gehalt der so erzeugten Daten ist nicht verfügbar.

[QUELLE: ISO 7498-2:1989]

3.39

Anwärter

(en: claimant)

Entität, die, basierend auf ihren im eigenen Attributzertifikat oder in der Erweiterung der Subject-Verzeichnisattribute ihres Public-Key-Zertifikats angegebenen Privilegien, die Ausführung eines sensiblen Dienstes oder dessen Bereitstellung durch einen Prüfer beantragt

3.40

Vertraulichkeit

(en: confidentiality)

Eigenschaft, die dazu führt, dass die betreffende(n) Information(en) keinen Personen, Entitäten oder Prozessen, die nicht über die entsprechende Autorisation verfügen, verfügbar gemacht oder diesen gegenüber offenlegt wird (werden)

[QUELLE: ISO 7498-2:1989]

3.40

Zustimmung

(en: consent)

spezielle Policy, die eine Vereinbarung zwischen einer Entität, die die Rolle des Gegenstandes einer Handlung spielt, und einer handelnden Entität festlegt

3.42

Identitätsnachweis

(en: credential)

als Voraussetzung ausgegebener Beleg für den Anspruch auf oder die Berechtigung zu einer Rolle. Informationen, die die Sicherheitsattribute (Identität oder Privileg oder beides) eines Principals beschreiben

Anmerkung 1 zum Begriff: Identitätsnachweise werden durch Authentisierung oder Delegation verlangt und von der Zugriffssteuerung verwendet.

3.43

CRL-Verteilungspunkt

(en: CRL Distribution Point)

Verzeichniseintrag oder sonstige Verteilungsquelle für CRLs

Anmerkung 1 zum Begriff: Eine durch einen CRL-Verteilungspunkt verteilte CRL kann Sperrungseinträge für nur eine Untermenge der Gesamtanzahl der von einer Zertifizierungsstelle ausgestellten Zertifikate oder Sperrungseinträge für mehrere Zertifizierungsstellen enthalten.

3.44

Kryptographie

(en: cryptography)

Disziplin, die Grundsätze, Mittel und Verfahren für die Umwandlung von Daten verkörpert, um deren Informationsinhalte zu verbergen, deren unentdeckte Änderung und/oder deren unautorisierte Verwendung zu verhindern

[QUELLE: ISO 7498-2:1989]

3.45

Verschlüsselungsalgorithmus

Chiffrierung

(en: cryptographic algorithm, cipher)

Verfahren für die Umwandlung von Daten mit dem Ziel, deren Informationsgehalt zu verbergen und ihre unerkannte Änderung und/oder nicht autorisierte Nutzung zu verhindern

[QUELLE: ISO 7498-2:1989]

3.46

Verschlüsselungssystem

Kryptosystem

(en: cryptographic system, cryptosystem)

eine Reihe von Prozessen zur Umwandlung von Klartext in chiffrierten Text und umgekehrt, wobei die im jeweiligen Fall anzuwendende(n) Umwandlung(en) durch entsprechende Schlüssel ausgewählt wird (werden).

Anmerkung 1 zum Begriff: Diese Umwandlungen werden üblicherweise durch einen mathematischen Algorithmus definiert.

3.47

Vertraulichkeit von Daten

(en: data confidentiality)

Dienst, der für den Schutz von Daten vor nicht autorisierter Offenlegung genutzt werden kann

Anmerkung 1 zum Begriff: Der Datenvertraulichkeitsdienst wird durch das Authentisierungs-Framework unterstützt. Er kann auch genutzt werden, um zu verhindern, dass Daten abgefangen werden.

3.48

Datenintegrität

(en: data integrity)

Eigenschaft, dass Daten nicht in unautorisierter Art und Weise verändert oder zerstört wurden

[QUELLE: ISO 7498-2:1989]

3.49

Authentisierung der Datenherkunft

(en: data origin authentication)

Bestätigung, dass die Quelle der empfangenen Daten tatsächlich den Angaben entspricht

[QUELLE: ISO 7498-2:1989]

3.50

Entschlüsselung

Dechiffrierung

(en: decipherment, decryption)

Prozess, in dem aus einem chiffrierten Text die entsprechenden ursprünglichen Daten erhalten werden

[QUELLE: ISO/IEC 2382-8:1998]

Anmerkung 1 zum Begriff: Ein chiffrierter Text kann ein zweites Mal verschlüsselt werden, was dazu führt, dass eine einzelne Entschlüsselung nicht den ursprünglichen Klartext ergibt.

3.51

Delegierung

(en: delegation)

Übertragung eines Privilegs von einer Entität, die dieses Privileg besitzt, auf eine andere Entität

3.52

Delegierungspfad

(en: delegation path)

geordnete Abfolge von Zertifikaten, die zusammen mit der Authentifizierung der Identität eines Privilegienverfechters verarbeitet werden können, um die Authentizität des Privilegs eines solchen Privilegienverfechters zu überprüfen

3.53

Delta-CRL

(en: delta CRL, dCRL)

Teil einer Sperrliste, der nur Einträge für Zertifikate enthält, deren Sperrstatus seit der Herausgabe der referenzierten Basis-CRL geändert wurde

3.54

digitale Signatur

(en: digital signature)

an eine Dateneinheit angehängte Daten oder eine kryptographische Umwandlung dieser Dateneinheit [siehe *Kryptographie* (3.44)], die es einem Empfänger der Dateneinheit erlaubt, die Quelle und Integrität der Einheit zu überprüfen, und die einen Schutz gegen Fälschung, z. B. durch den Empfänger, bietet

[QUELLE: ISO 7498-2:1989]

3.55

Chiffrierung

Verschlüsselung

(en: encipherment, encryption)

kryptographische Umwandlung von Daten [siehe *Kryptographie* (3.44)] zur Erzeugung eines chiffrierten Textes

[QUELLE: ISO 7498-2:1989]

3.56

Endentität

(en: end entity)

Zertifikatsgegenstand, der seinen privaten Schlüssel für andere Zwecke als zur Signierung von Zertifikaten nutzt, oder eine Entität, bei der es sich um eine vertrauende Partei handelt

3.57

Attributzertifikat-Sperrliste der Endentität

(en: end-entity attribute certificate revocation list, EARL)

Sperrliste, die eine Liste von Attributzertifikaten enthält, die vom Zertifikataussteller als nicht mehr gültig angesehen werden und an Zertifikathalter ausgegeben wurden, die nicht auch Attributautorisierer waren

3.58

Public-Key-Zertifikat-Sperrliste der Endentität

(en: end-entity public-key certificate revocation list, EPRL)

Sperrliste, die eine Liste von Public-Key-Zertifikaten enthält, die an Subjekte ausgestellt wurden, die nicht auch Attributautorisierer sind, und die vom Zertifikataussteller als nicht mehr gültig angesehen werden

3.59

Umgebungsvariable

(en: environmental variables)

Aspekte der Policy, die für eine Autorisierungsentscheidung benötigt werden und nicht in statischen Strukturen enthalten sind, aber einem Privilegienprüfer durch irgendein lokales Mittel zur Verfügung stehen (z. B. Tageszeit oder aktueller Kontostand)

3.60

vollständige CRL

(en: full CRL)

vollständige Sperrliste, die Einträge für alle Zertifikate enthält, die für den betreffenden Geltungsbereich widerrufen wurden

3.61

funktionelle Rolle

(en: functional role)

an eine Handlung gebundene Rolle

Anmerkung 1 zum Begriff: Funktionelle Rollen können so zugewiesen werden, dass sie während einer Handlung ausgeführt werden müssen.

Anmerkung 2 zum Begriff: Funktionelle Rollen entsprechen der RIM-Beteiligung ISO/HL7 21731.

Anmerkung 3 zum Begriff: Siehe auch *strukturelle Rolle* (3.105).

[QUELLE: ISO 21298:—, Definition 3.10, geändert]

3.62

Hash-Funktion

(en: hash function)

(mathematische) Funktion, die Werte eines großen (möglicherweise sehr großen) Bereichs (hier: Domain) auf einen kleineren Bereich abbildet

Anmerkung 1 zum Begriff: Eine „gute“ Hash-Funktion ist gegeben, wenn die Ergebnisse der auf einen (großen) Wertesatz im Bereich angewendeten Funktion gleichmäßig (und scheinbar zufällig) über den Bereich verteilt sind

3.63

Halter

(en: holder)

Entität, an die bestimmte Privilegien entweder direkt von der Quelle der Autorität oder indirekt durch einen anderen Attributautorisierer delegiert wurden

3.64

Identifikation

(en: identification)

Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen

[QUELLE: ISO/IEC 2382-8 :1998]

3.65

Identifikator

(en: identifier)

Information, die verwendet wird, um vor einer möglichen Bestätigung durch einen entsprechenden Authentifikator eine Identität zu beanspruchen

[QUELLE : ENV 13608-1:2000]

3.66

indirekte CRL

(en: indirect CRL, iCRL)

Sperrliste, die mindestens Sperrinformationen über Zertifikate enthält, die von anderen Behörden als der, die diese CRL herausgegeben hat, ausgestellt wurden

3.67

Integrität

(en: integrity)

Beleg dafür, dass die Information während der Übertragung in keiner Weise, weder absichtlich noch unabsichtlich, geändert wurde

[QUELLE: ISO 7498-2:1989]

3.68

Schlüssel

(en: key)

Symbolfolge, die die Verschlüsselungs- und Entschlüsselungsoperationen steuert

[QUELLE: ISO 7498-2:1989]

3.69

Schlüsselvereinbarung

(en: key agreement)

Verfahren für die Aushandlung eines Schlüssels, das online erfolgt und ohne dabei den Schlüssel zu übertragen, noch nicht einmal in verschlüsselter Form; z. B. das Diffie-Hellman-Verfahren

Anmerkung 1 zum Begriff: Zu weiteren Informationen über Schlüsselvereinbarungsverfahren siehe ISO/IEC 11770-1:2010.

3.70

Schlüsselmanagement

(en: key management)

Erzeugung, Speicherung, Verteilung, Löschung, Archivierung und Anwendung von Schlüsseln in Übereinstimmung mit einer Sicherheits-Policy

[QUELLE: ISO 7498-2:1989]

3.71

leichtes Verzeichniszugriffsprotokoll

(en: lightweight directory access protocol, LDAP)

Standardzugriffsprotokoll für Verzeichnisse, das den öffentlichen oder kontrollierten Zugriff auf Zertifikate und sonstige in einer PKI benötigte Informationen ermöglicht

3.72

Unleugbarkeit

(en: non-repudiation)

Dienstleistung, die einen Nachweis für die Integrität und die Herkunft der Daten (beides auf fälschungssichere Art und Weise) erbringt, der von einer beliebigen anderen Partei verifiziert werden kann

[QUELLE: ISO 17090-1:2013]

3.73

Objektidentifikator

(en: object identifier, OID)

eindeutiger alphanumerischer/numerischer Identifikator, der unter der ISO-Meldenorm für die Referenzierung eines bestimmten Objektes oder einer Objektklasse registriert ist

Anmerkung 1 zum Begriff: Dies ist ein Name für eine Zertifikats-Policy, der in einem Feld jedes nach dieser Policy ausgestellten Zertifikats vermerkt ist.

3.74

Objektmethode

(en: object method)

Aktion, die auf einer Ressource aufgerufen werden kann (so kann z. B. ein Dateisystem Objektmethoden gelesen haben, schreiben und ausführen)

3.75

Einweg-Funktion

(en: one-way function)

(mathematische) Funktion f , die leicht zu berechnen ist, für die es aber rechnerisch schwierig ist, einen Wert x in der Domain für einen allgemeinen Wert y im Bereich zu finden, für den gilt: $f(x) = y$

Anmerkung 1 zum Begriff: Es kann einige Werte y geben, für die sich x ohne Schwierigkeiten errechnen lässt.

3.76

Zertifikathalter

(en: certificate holder)

Entität, die als der Gegenstand eines gültigen Zertifikats benannt wurde

3.77

Genehmigung

(en: permission)

Erlaubnis zur Ausführung einer Operation an einem oder mehreren RBAC-geschützten Objekten

[QUELLE: INCITS 359-2004]

3.78

Policy

Reihe von gesetzlichen, politischen, organisatorischen, funktionellen und technischen Verpflichtungen oder Unterlassungen, die sich auf Kommunikation und Kooperation beziehen

3.79

Policy-Vereinbarung

(en: policy agreement)

schriftliche Vereinbarung, nach der sich alle Beteiligten zur Einhaltung einer festgelegten Reihe von Policies verpflichten

3.80

Policy Decision Point

PDP

Systementität, die die anwendbare Policy bewertet und eine Autorisierungsentscheidung trifft

Anmerkung 1 zum Begriff: Dieser Begriff wurde gemeinschaftlich von der IETF Policy Framework Working Group und der Distributed Management Task Force (DMTF)/Common Information Model (CIM) in [RFC 3198:2001] definiert.

Anmerkung 2 zum Begriff: Dieser Begriff entspricht dem Begriff der „Zugriffsentscheidungsfunktion“ (en: Access Decision Function, ADF) in ISO 10181-3:1996.

3.81

Policy Enforcement Point

PEP

Systementität, die die Zugriffssteuerung ausführt, indem sie Entscheidungsanträge stellt und Autorisierungsentscheidung durchsetzt

Anmerkung 1 zum Begriff: Dieser Begriff wurde gemeinschaftlich von der IETF Policy Framework Working Group und der Distributed Management Task Force (DMTF)/Common Information Model (CIM) in [RFC 3198:2001] definiert.

Anmerkung 2 zum Begriff: Dieser Begriff entspricht dem Begriff der „Zugriffsdurchsetzungsfunktion“ (en: Access Enforcement Function, AEF) in ISO 10181-3:1996.

3.82

Policy-Mapping

(en: policy mapping)

Anerkennung, dass eine bestimmte Zertifikats-Policy in einer zweiten Domain, wenn eine Zertifizierungsstelle einer ersten Domain eine Zertifizierungsstelle in dieser zweiten Domain zertifiziert, von der Behörde der ersten Domain als gleichwertig (jedoch nicht notwendigerweise in jeder Hinsicht identisch) mit einer bestimmten Zertifikats-Policy in der ersten Domain angesehen werden kann

3.83

Principal

menschliche Benutzer und Objekte, die unter ihren eigenen Rechten arbeiten müssen

[QUELLE: OMG Security Services Specification:2001]

3.84

privater Schlüssel

(en: private key)

Schlüssel, der sich im Besitz einer begrenzten Anzahl von Entitäten (in der Regel nur einer Entität) befindet und mit einem asymmetrischen Verschlüsselungsalgorithmus verwendet wird

[QUELLE: ISO/IEC 10181-1:1996]

3.85

Privileg

(en: privilege)

Kapazität, die einer Entität von einer Behörde entsprechend dem Attribut dieser Entität zugewiesen wird

3.86

Privilegienverfechter

(en: privilege assenter)

Privilegienhalter, der sein Attributzertifikat oder ein Public-Key-Zertifikat verwendet, um sein Privileg geltend zu machen

3.87

Infrastruktur für das Privilegienmanagement

(en: privilege management infrastructure, PMI)

Infrastruktur, die das Management von Privilegien in Unterstützung eines umfassenden Autorisierungsdienstes und in Beziehung zu einer Public-Key-Infrastruktur unterstützen kann

3.88

Privilegien-Policy

(en: privilege policy)

Policy, die die Bedingungen für Privilegienprüfer umreißt, um qualifizierten Privilegienverfechtern sensible Dienste zur Verfügung zu stellen oder sie für diese auszuführen.

Anmerkung 1 zum Begriff: Die Privilegien-Policy setzt mit dem Dienst verknüpfte Attribute sowie mit Privilegienverfechtern verknüpfte Attribute in Beziehung.

3.89

Privilegienprüfer

(en: privilege verifier)

Entität, die Zertifikate im Vergleich mit einer Privilegien-Policy überprüft

3.90

öffentlicher Schlüssel

(en: public key)

Schlüssel, der mit einem asymmetrischen Verschlüsselungsalgorithmus verwendet wird und öffentlich zugänglich gemacht werden kann

[QUELLE: ISO/IEC 10181-1:1996]

3.91

Public-Key-Zertifikat

(en: public key certificate, PKC)

X.509-Zertifikat, das eine Identität und einen öffentlichen Schlüssel bindet

[QUELLE: ISO/IEC 9594-8:2008]

Anmerkung 1 zum Begriff: Die Identität kann zur Unterstützung identitätsbasierter Zugriffssteuerungsentscheidungen herangezogen werden, nachdem der Client beweist, dass er Zugriff auf den privaten Schlüssel hat, der dem im PKC enthaltenen öffentlichen Schlüssel entspricht.

[QUELLE: RFC 2459]

3.92

Public-Key-Infrastruktur

(en: public key infrastructure)

Infrastruktur, die in der Beziehung zwischen einem Schlüsselhalter und einer vertrauenden Partei verwendet wird und es einer vertrauenden Partei ermöglicht, ein auf den Schlüsselhalter bezogenes Zertifikat für mindestens eine Anwendung, die einen von einem öffentlichen Schlüssel abhängigen Sicherheitsdienst nutzt, zu nutzen

Anmerkung 1 zum Begriff: Die PKI umfasst eine Zertifizierungsstelle, eine Zertifikatsdatenstruktur, Mittel, mit deren Hilfe die vertrauende Partei aktuelle Informationen zum Sperrstatus des Zertifikats erhalten kann, eine Zertifizierungs-Policy und Verfahren für die Validierung der Zertifizierungspraxis.

3.93

vertrauende Partei

(en: relying party)

Empfänger eines Zertifikats, der im Vertrauen auf dieses Zertifikat und/oder die unter Verwendung dieses Zertifikats verifizierte digitale Signatur handelt

[QUELLE: RFC 2527:1999]

3.94

Rolle

(en: role)

Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen

[QUELLE: ISO 21298:—, Definition 3.22]

Anmerkung 1 zum Begriff: Für das Management von rollenbezogenen Beziehungen zwischen den Entitäten können strukturelle und funktionelle Rollen festgelegt werden.

3.95

Rollenzuweisungszertifikat

(en: role assignment certificate)

Zertifikat, das das Rollenattribut enthält und dem Zertifikathalter eine oder mehrere Rollen zuweist

3.96

Rollenzertifikat

(en: role certificate)

Zertifikat, das Privilegien zuweist und zwar eher einer Rolle als den betreffenden Personen direkt

Anmerkung 1 zum Begriff: Personen, denen diese Rolle durch ein Attributzertifikat oder ein Public-Key-Zertifikat mit einer Subject-Verzeichnis-Attributerweiterung, die diese Zuweisung enthält, zugewiesen wird, werden die in diesem Rollenzertifikat enthaltenen Privilegien indirekt zugewiesen.

3.97

Rollenspezifikationszertifikat

(en: role specification certificate)

Zertifikat, das die Zuweisung von Privilegien zu einer Rolle enthält

3.98

Sensibilität

(en: sensitivity)

Eigenschaft einer Ressource, die deren Wert oder Wichtigkeit impliziert

3.99

Sicherheit

(en: security)

Kombination von Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit

[QUELLE: ENV 13608-1:2000]

3.100

Sicherheits-Policy

(en: security policy)

Aktionsplan oder Vorgehensweise für die Sicherstellung der Rechtersicherheit

[QUELLE: ISO/IEC 2382-8:1998]

Anmerkung 1 zum Begriff: Dies ist eine Reihe von Regeln zur Nutzung und Bereitstellung von Sicherheitsdiensten und -einrichtungen, die von der Sicherheitsbehörde festgelegt wurde.

3.101

Sicherheitsdienst

(en: security service)

Dienst, der von einer Schicht miteinander kommunizierender offener Systeme bereitgestellt wird und die Sicherheit der Systeme oder der Datenübertragung in angemessenem Maße sicherstellt

[QUELLE: ISO 7498:1989]

3.102

einfache Authentifizierung

(en: simple authentication)

Authentifizierung mittels einfacher Passwortregeln

3.103

Quelle der Autorität

(en: source of authority, SoA)

Attributautorisierer, dem ein Privilegienprüfer für eine bestimmte Ressource als letzter Instanz für die Zuweisung einer Reihe von Privilegien vertraut

Anmerkung 1 zum Begriff: Dies ist ein besonderer Attributautorisierer, dem ein Prüfer ein unbegrenztes Privileg einräumt.

Anmerkung 2 zum Begriff: Der Prüfer vertraut der Quelle der Autorität so weit, dass er es ihr überlässt, dieses Privileg an Zertifikathalter zu delegieren, von denen einige dieses Privileg wiederum an andere Zertifikathalter delegieren können.

3.104

starke Authentifizierung

(en: strong authentication)

Authentifizierung mittels kryptografisch abgeleiteter multifaktorieller Identitätsnachweise

3.105

strukturelle Rolle

(en: structural role)

Rolle, die Beziehungen zwischen Entitäten im Sinne der Kompetenz spezifiziert und damit häufig organisatorische oder strukturelle Beziehungen (Hierarchien) widerspiegelt

Anmerkung 1 zum Begriff: Strukturelle Rollen entsprechen der RIM-Beteiligung ISO/HL7 21731.

Anmerkung 2 zum Begriff: Siehe auch *funktionelle Rolle* (3.61).

[QUELLE: ISO 21298:—, Definition 3.27, geändert]

3.106

Ziel

(en: target)

Ressource, auf die von einem Anwarter zugegriffen wird

Anmerkung 1 zum Begriff: Deren Sensibilität wird in diesem Teil von ISO 22600 als eine Sammlung von Attributen modelliert, die entweder als ASN.1-Attribute oder als XML-Elemente dargestellt werden.

3.107

Vertrauen

(en: trust)

bestehender Umstand zwischen zwei Entitäten, wobei eine Entität die Annahme macht, dass die andere Entität sich wie die erste Entität verhalten wird

Anmerkung 1 zum Begriff: Dieses Vertrauen gilt nur für eine bestimmte Funktion. Die Hauptaufgabe des Vertrauens in diesem Framework ist, die Beziehung zwischen einer authentisierenden Entität und einem Autorisierer zu beschreiben; eine Entität muss sich sicher sein, dass sie dem Autorisierer vertrauen kann, dass dieser nur gültige und zuverlässige Zertifikate erstellt.

3.108

Dritte

Dritter, dritte Partei

(en: third party)

Partei, die weder der Absender noch der Empfänger der Daten ist und als Teil eines Kommunikationsprotokolls eine Sicherheitsfunktion auszuführen hat

3.109

vertrauenswürdige dritte Partei

(en: trusted third party, TTP)

Dritte, die für die Zwecke eines Sicherheitsprotokolls als vertrauenswürdig erachtet werden

[QUELLE: ENV 13608-1:2000]

Anmerkung 1 zum Begriff: Diese Benennung wird in vielen ISO/IEC-Normen und anderen Dokumenten verwendet, die hauptsächlich die Dienste einer Zertifizierungsstelle beschreiben. Der Begriff ist jedoch weiter gefasst und schließt Dienste wie z. B. die Erzeugung von Zeitstempeln und gegebenenfalls auch Hinterlegungsdienste ein. TTPs leisten Basisdienste, infrastrukturbezogene Dienste und Mehrwertdienste.

3.110

Prüfer

(en: verifier)

Entität, die für die Ausführung oder Bereitstellung eines sensiblen Dienstes für qualifizierte Anwarter verantwortlich ist

Anmerkung 1 zum Begriff: Der Prüfer setzt die Privilegien-Policy durch. Im Falle der Validierung von Zertifizierungspfaden ist ein Prüfer eine spezielle vertrauende Partei.

4 Abkürzungen

Die nachstehende Liste von Abkürzungen enthält alle in den drei Teilen dieser Internationalen Norm verwendeten Abkürzungen.

Abkürzung	Englische Bedeutung	Deutsche Bedeutung (spiegelt nicht die Verwendung im Deutschen wider)
AA	Attribute Authority	Attributautorisierer
AARL	Attribute Authority Revocation List	Sperrliste des Attributautorisierers
ACO	Access Control Information	Zugriffssteuerungsinformation(en)
ACRL	Attribute Certificate Revocation List	Attributzertifikate-Sperrliste
ADF	Access Decision Function	Zugriffsentscheidungsfunktion
ADI	Access Control Decision Information	Zugriffssteuerungs-Entscheidungsfunktion
AEF	Access Enforcement Function	Zugriffsdurchsetzungsfunktion
ANSI	American National Standards Institute	Nationale Normungsorganisation der USA
ARL	Authority Revocation List	Behördensperrliste
CA	Certification Authority	Zertifizierungsstelle
CARL	Certification Authority Revocation List	Sperrliste der Zertifizierungsstelle
CIM	Common Information Model	Allgemeines Informationsmodell
CORBA	Common Object Request Broker Architecture	Allgemeine Objktanforderungsmakler-Architektur
CRL	Certificate Revocation List	Zertifikatssperrliste
dCRL	Delta Certificate Revocation List	Delta-Zertifikatssperrliste
DAP	Directory Access Protocol	Verzeichniszugriffsprotokoll
DEA	Drug Enforcement Administration	Drogenvollzugsbehörde
DIB	Directory Information Base	Verzeichnisinformationsbasis
DIT	Directory Information Tree	Verzeichnisinformationsbaum
DMTF	Distributed Management Task Force	Arbeitsgruppe für verteiltes Management
DSA	Directory System Agent	Verzeichnissystemagent
DTD	Data Type Definition	Datentypdefinition
DUA	Directory User Agent	Verzeichnisbenutzeragent
EARL	End-entity Attribute Certificate Revocation List	Attributzertifikat-Sperrliste der Endentität
EHR	Electronic Health Record	Elektronische Patientenakte
EPRL	End-entity Public Key Certificate Revocation List	Public-Key-Zertifikat-Sperrliste der Endentität
HL7	Health Level Seven	Health Level 7
iCRL	Indirect Certificate Revocation List	Indirekte Zertifikatssperrliste
IETF	Internet Engineering Task Force	Organisation für die technische Weiterentwicklung des Internets
ISO	International Standards Organization	Internationale Normungsorganisation
IT	Information Technology	Informationstechnik
LDAP	Lightweight Directory Access Protocol	Leichtes Verzeichniszugriffsprotokoll

OASIS	Organization for the Advancement of Structured Information Standards	OASIS-Konsortium
OCSP	Online Certificate Status Protocol	Online-Zertifikatsstatusprotokoll
OMG	Object Management Group	OMG-Konsortium
PA	Privilege Allocator	Privilegienzuordner
PDP	Policy Decision Point	Policy-Entscheidungspunkt
PEP	Policy Enforcement Point	Policy-Durchsetzungspunkt
PKC	Public Key Certificate	Public-Key-Zertifikat
PKCS	Public Key Cryptosystem	Public-Key-Kryptosystem
PKI	Public Key Infrastructure	Public-Key-Infrastruktur
PMI	Privilege Management Infrastructure	Infrastruktur für das Privilegienmanagement
PPS	Permission Policy Set	Reihe der Genehmigungs-Policies
RA	Registration Authority	Registrierungsbehörde
RBAC	Role-Based Access Control	Rollenbasierte Zugriffssteuerung
RPS	Role Policy Set	Reihe der Rollen-Policies
S/MIME	Secure Multipurpose Internet Mail Extensions	Sichere Mehrzweck-Internetmail-Erweiterungen
SAML	Security Assertion Markup Language	Sicherheits-Assertion-Auszeichnungssprache
SOA	Service-Oriented Architecture	Serviceorientierte Architektur
SoA	Source of Authority	Quelle der Autorität
SPML	Service Provisioning Markup Language	Dienstbereitstellungs-Auszeichnungssprache
TTP	Trusted Third Party	Vertrauenswürdige dritte Partei
UDDI	Universal Description, Discovery and Integration	Universelle Beschreibung, Auffindung und Einbindung
UHID	Universal Healthcare Identifier	Universeller Identifikator im Gesundheitswesen
UML	Unified Modeling Language	Vereinheitlichte Modellierungssprache
URI	Uniform Resource Identifier	Einheitlicher Bezeichner für Ressourcen
XACML	eXtensible Access Control Markup Language	Erweiterbare Zugriffssteuerungs-Auszeichnungssprache
XML	eXtensible Markup Language	Erweiterbare Auszeichnungssprache

5 Strukturen und Dienste für Privilegienmanagement und Zugriffssteuerung

Das Privilegienmanagement und die Zugriffssteuerung werden von Policies geregelt, die zur Sicherstellung der Interoperabilität formal ausgedrückt werden sollten. In Bezugnahme auf das Generische Komponentenmodell ist in ISO 22600-2 (siehe Bild 1) die Basisklassenstruktur der Policies festgelegt. Wie in ISO 22600-2 erwähnt, können Policies unterschiedlich dargestellt werden. So stellt z. B. die WS-Policy des OASIS-Konsortiums ein Allzweckmodell und eine entsprechende Syntax zur Beschreibung und Kommunikation der Policies eines Webservices zur Verfügung. Sie legt eine Reihe von gemeinsamen Message-Policy-Assertions innerhalb einer Policy und Verfahren für das Anhängen für die Verwendung von Policy-Ausdrücken mit bestehenden XML-Diensttechniken fest. Dieser Teil von ISO 22600 verlangt keine Policy-Darstellungssprache.