

DIN EN ISO 22600-3

ICS 35.240.80

Einsprüche bis 2013-04-25

Entwurf

**Medizinische Informatik –
Privilegmanagement und Zugriffssteuerung –
Teil 3: Implementierungen (ISO/DIS 22600-3:2012);
Deutsche Fassung prEN ISO 22600-3:2012**

Health informatics –
Privilege management and access control –
Part 3: Implementations (ISO/DIS 22600-3:2012);
German version prEN ISO 22600-3:2012

Informatique de santé –
Gestion de privilèges et contrôle d'accès –
Partie 3: Mises en oeuvre (ISO/DIS 22600-3:2012);
Version allemande prEN ISO 22600-3:2012

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2013-02-25 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

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

Gesamtumfang 84 Seiten

Normenausschuss Medizin (NAMed) im DIN

Nationales Vorwort

Dieses Dokument (prEN ISO 22600-3:2012) wurde vom Technischen Komitee ISO/TC 215 „Health Informatics“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ (Sekretariat: NEN, Niederlande) erarbeitet. Der Fachbereich 7 „Medizinische Informatik“ und insbesondere die Mitarbeiter des Arbeitsausschusses NA 063-07-04 AA „Sicherheit“ des Normenausschusses Medizin (NAMed) im DIN e. V. haben an der Erarbeitung mitgewirkt. Dieser Norm-Entwurf enthält unter Berücksichtigung der Präsidialbeschlüsse 13/1983 und 1/2004 in den Bildern 1 und 3 den englischen Originaltext des Internationalen Norm-Entwurfs ISO/DIS 22600-2:2012.

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

— *Teil 1: Übersicht und Policy-Management*

— *Teil 2: Formale Modelle*

— *Teil 3: Implementierungen*

Medizinische Informatik — Privilegienmanagement und Zugriffssteuerung — Teil 3: Implementierungen (ISO/DIS 22600-3:2012)

Informatique de santé — Gestion de privilèges et contrôle d'accès — Partie 3 : Mises en œuvre (ISO/DIS 22600-3:2012)

Health informatics — Privilege management and access control — Part 3: Implementations (ISO/DIS 22600-3:2012)

ICS: 35.240.80

Deskriptoren:

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokumentstufe: parallele Umfrage
Dokumentsprache: D

STD Version 2.5a

Inhalt

Seite

Vorwort	4
Einleitung.....	5
1 Anwendungsbereich	9
2 Normative Verweisungen.....	9
3 Begriffe	10
4 Abkürzungen	23
5 Strukturen und Dienste für Privilegienmanagement und Zugriffssteuerung	24
6 Interpretation der in ISO 22600-2 festgelegten formalen Modelle in Umgebungen des Gesundheitswesens	27
7 Begriffsdarstellung für Informationssysteme im Gesundheitswesen	28
7.1 Übersicht	28
7.2 Domainsprachen	28
7.3 OCL-Randbedingungsmodellierung	29
7.4 Sonstige Randbedingungsdarstellungen	30
7.4.1 Allgemeines	30
7.4.2 Extended Access Control Markup Language	30
7.4.3 Web Services Description Language	30
7.4.4 Business Process Execution Language	31
7.4.5 WS-Policy	31
7.4.6 Web Services Policy Language	31
7.4.7 Domain-Independent Web Services Policy Assertion Language (DIPAL)	31
7.4.8 Security Assertion Markup Language	31
8 Einverständniserklärung	32
8.1 Übersicht	32
8.2 Einverständniserklärung des Patienten	32
8.3 Verwaltung der Einverständniserklärungen von Patienten.....	32
9 Zugriff im Notfall	32
10 Verfeinerung des Steuerungsmodells	32
11 Verfeinerung des Delegierungsmodells	33
Anhang A (informativ) Infrastruktur für das Privilegienmanagement.....	34
A.1 Verwendung von Anhang A in weitgehender Harmonisierung mit ASTM E 2595-07	34
A.2 Framework für die Infrastruktur des Privilegienmanagements	34
A.2.1 PMI-Dienste	34
A.2.2 Zugriffssteuerungsinformationen	35
A.2.3 Governance, Risiko und Konformität	37
A.2.4 Vertrauensmanagement.....	38
A.2.5 Identitätsmanagement.....	38
A.3 Infrastrukturdienste für das Privilegienmanagement in ASN.1	39
A.3.1 X.509-basierte Zertifikatsspezifikationen	39
A.3.2 Freigabe	44
A.3.3 Anwärterverfahren	45
A.3.4 Zielsensibilitätsverfahren	45
A.3.5 Zugriffssteuerungs-Framework.....	48
A.4 Infrastrukturdienste für das Privilegienmanagement in XML	49
A.4.1 XACML-basierte Rollenzuweisung.....	49
A.4.2 Weitere PMI-Dienste	49
A.5 Beispiele für die Privilegienmanagement- und Zugriffssteuerungsszenarien und -dienste	50
A.5.1 Organisationsbasierte Privilegienzuweisung	50
A.5.2 Workflow-basierte Privilegienzuweisungen.....	50
A.5.3 Policy-basiertes Privilegienmanagement.....	50

A.5.4	Rollen- und Genehmigungszuweisung	50
A.5.5	Autorisierungsspezifikation	50
A.5.6	Zertifikatsbasiertes Privilegienmanagement	51
A.5.7	Infrastruktur für das Privilegienmanagement	52
A.5.8	Genehmigungsrandbedingungen	53
A.5.9	Trennung der Sicherheit von der Geschäftslogik	54
A.5.10	Leitlinien zum Policy Enforcement Point	54
A.6	LDAP-aktivierter Verzeichnisdienst versus Policy-Engines	55
A.6.1	Allgemeines	55
A.6.2	LDAP	55
A.6.3	Policy-Engine	55
A.6.4	Policy Decision Point (PDP)	56
A.7	Identitätsmanagementsysteme	56
A.8	Audit	57
A.9	Weitere PMI-Dienste	59
A.9.1	Auditzuordnung	59
A.9.2	Nachweis und Meldung von Eindringversuchen	59
A.9.3	Anwärterverfahren	59
A.9.4	LDAP-Suche (Rollensuche)	60
A.9.5	Zertifikate	61
A.9.6	Medizinische Identitätsnachweise	62
A.9.7	SAML-Assertions	62
A.9.8	Zielsensibilitätsverfahren	62
A.9.9	Signierte Datenkapselung	63
A.9.10	Verwendung von XML	63
A.9.11	Framework für die Zugriffssteuerung	63
A.9.12	Policy-Spezifikationsverfahren	64
A.9.13	Übertragung von XACML-Policies	65
A.9.14	Mapping zwischen ANS.1-Typen und XML-Elementen	67
A.9.15	Einverständniserklärung des Patienten	68
A.9.16	Abgleich der Identitätsnachweise	68
A.9.17	Abgleich der Sicherheits-Labels	68
A.9.18	Allgemeiner Abgleich der Geltendmachungen (Assertions)	68
A.9.19	Signaturanforderungen	70
A.10	Integration mit PKI	70
A.11	Beispiele für die Anwendung von Privilegienmanagement- und Zugriffssteuerungslösungen	71
A.11.1	Allgemeines	71
A.11.2	Anwendung von Identitätsnachweisen	71
A.11.3	Zugriffssteuerung	71
A.11.4	Signaturanforderungen	72
A.11.5	Dokumentautorisierung	72
A.11.6	ANSI-RBAC-Modell	73
A.12	Policy-Bridging	74
Anhang B (informativ)	Attributzertifikatserweiterungen	75
B.1	Grundlegende Erweiterungen zum Privilegienmanagement	75
B.2	Erweiterungen zum Widerruf bzw. zur Sperrung von Privilegien	75
B.3	Erweiterungen zur Quelle der Autorität	75
B.4	Erweiterungen zu den Rollen	75
B.5	Erweiterungen zur Delegierung	76
B.6	IETF-Erweiterungen	76
Anhang C (informativ)	Terminologievergleich	77
Anhang D (informativ)	Beispiele für das Policy-Management und die Policy-Darstellung	78
D.1	Beispiel für eine SAML-Assertion	78
D.2	Beispiel für die Darstellung von Policies in anderer Form als XML	78
D.3	XACML-Beispiel	79
Literaturhinweise		81

Vorwort

Dieses Dokument (prEN ISO 22600-3:2012) 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.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wird EN ISO/TS 22600-3:2009 ersetzen.

Anerkennungsnotiz

Der Text von ISO/DIS 22600-3:2012 wurde vom CEN als prEN ISO 22600-3:2012 ohne irgendeine Abänderung genehmigt.

Einleitung

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. Das Ziel eines einheitlichen Szenariums erfordert erheblichen finanziellen, zeitlichen und arbeitstechnischen Aufwand, um benutzerbezogene und organisatorische Informationen vor Beginn der Kommunikation aufeinander abzubilden. Für die Entwicklung und Pflege von Sicherheitsfunktionen werden Ressourcen in einem Maße benötigt, das mit der Anzahl der Anwendungen exponentiell ansteigt.

Auf der anderen Seite erfordert die Betrachtung der Autorisierung vom Standpunkt einer Organisation des Gesundheitswesens aus aufgrund der Tatsache, dass sich diese Organisationen durch die Schließung, Neugründung und Zusammenlegung von Abteilungen beständig verändern, ein flexibles Management.

Die Lage wird bei organisationsübergreifender Kommunikation noch komplizierter, weil in diesem Falle die Grenzen von Domains überschritten werden, die durch entsprechende Sicherheits-Policies geregelt werden. Die Unterschiede zwischen diesen Domains in Bezug auf die geltenden Policies müssen dann durch entsprechende Policy-Vereinbarungen überbrückt werden, d. h. eine Reihe von Regeln, die von allen Beteiligten befolgt werden.

Ein weiteres Komplexitätsproblem ist zu lösen, wenn es um die Benutzer und ihre funktionellen und strukturellen Rollen geht. Ein und derselbe Benutzer kann autorisiert sein, unter mehreren funktionellen und strukturellen Rollen zu operieren. Während ein Benutzer mehrere strukturelle Rollen gleichzeitig innehaben kann, kann er für eine gegebene Informationsanforderung nur in einer einzigen funktionellen Rolle tätig sein. Die geltende Policy bestimmt die Beziehungen zwischen den diversen funktionellen Rollen, die ein Benutzer innehaben kann, einschließlich möglicher Bündelungsbeziehungen, Hierarchien, zusammengesetzter struktureller Rollen, nacheinander ausgeübter funktioneller Rollen und der Rollen, die besser nicht miteinander kombiniert werden sollten. Falls z. B. ein Allgemeinarzt auch ein Psychiater ist, kann die Policy festlegen, dass der Psychiater mit anderen ähnlich privilegierten strukturellen Rollen gebündelt werden darf, dass der Psychiater die Privilegien des Allgemeinarztes übernimmt, dass eine neue zusammengesetzte strukturelle Rolle erzeugt wird oder dass diese beiden strukturellen Rollen nicht miteinander kombiniert werden dürfen. Ein Beispiel für die Einschränkung von nacheinander ausgeübten funktionellen Rollen wäre ein Konflikt der Pflichten, der durch geltendes Recht begrenzt werden kann (so kann z. B. diejenige Person, die eine Kostenerstattung beantragt, nicht gleichzeitig die Person sein, die diese Kostenerstattung abzeichnet). Darüber hinaus können innerhalb der betreffenden Organisation des Gesundheitswesens unterschiedliche Verantwortungen bezüglich der Rolle und der Aktivitäten der Benutzer identifiziert werden. Von Land zu Land und von einer medizinischen Versorgungseinrichtung zur nächsten können für ähnliche Arten von Benutzern sowohl in Bezug auf die Ausübung spezieller Funktionen als auch auf den Zugriff auf die Informationen unterschiedliche Arten oder Stufen der Autorisierung gelten.

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 erforderlich.

Neben der für alle Arten von großen Organisationen typischen Vielzahl unterschiedlicher Rollen und Verantwortlichkeiten sind im Gesundheitswesen wegen der speziellen Art der hier zu verwaltenden Informationen auch ethische und rechtliche Aspekte zu berücksichtigen.

Schon heute sind moderne Lösungen für das Privilegienmanagement erforderlich, die damit verbundenen Herausforderungen werden aber in den nächsten Jahren noch zunehmen. Der Grund hierfür liegt in der wachsenden Menge an Informationen, die zwischen den einzelnen Anwendungen ausgetauscht werden, um den Bedarf der Ärzte in Bezug auf den Zugriff auf immer mehr patientenbezogene Informationen im Sinne der Sicherstellung von Qualität und Effizienz bei der Diagnose und Behandlung des Patienten zu erfüllen.

Im letzten Jahrzehnt hat sich die Situation in Bezug auf die Gesundheitsversorgung und ihre sicherheits- und datenschutzbezogenen Dienstleistungen geändert. Die Gründe hierfür sind z. B.:

- der Übergang von großrechnergestützten proprietären Altsystemen zu verteilten lokalisierten Systemen;
- die wachsende Menge der in Informationssystemen gespeicherten Daten in Kombination mit wachsenden Risiken in Bezug auf Sicherheit und Datenschutz;
- dass die Versorgung der Patienten von einer immer größer werdenden Anzahl von Einrichtungen des Gesundheitswesens auf unterschiedlichen Stufen übernommen wird, weswegen die medizinischen Informationen der Patienten an unterschiedlichen Stellen zur Verfügung stehen müssen.

In dieser Situation sind aufgrund der Sensibilität von personenbezogenen Informationen und ihrer möglichen persönlichen und sozialen Auswirkungen moderne Maßnahmen zur Sicherstellung von Sicherheit und Datenschutz bei der Kommunikation und Nutzung von gesundheitsbezogenen Informationen erforderlich. Entsprechend betreffen die auf Sicherheit und Datenschutz ausgerichteten Dienstleistungen sowohl Kommunikations- als auch Anwendungsdienste. Unter den kommunikationsbezogenen Diensten, wie Authentisierung, Integrität, Vertraulichkeit, Verfügbarkeit, Zurechenbarkeit (einschließlich Rückverfolgbarkeit und Unleugbarkeit), Steuerung des Zugriffs auf Entitäten, die sämtlich durch Dienste vertrauenswürdiger Dritter unterstützt werden, ist es die Authentisierung, die von entscheidender Bedeutung für die meisten anderen Dienste ist. Dies gilt auch für anwendungsorientierte Dienste, wie z. B. die Steuerung des Zugriffs auf Daten und Funktionen von Anwendungen, die bei der zuvor erwähnten Entität laufen, die Integrität, Vertraulichkeit, Verfügbarkeit, Zurechenbarkeit, Hörbarkeit und die unterstützenden Dienste vertrauenswürdiger Dritter.

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 eine schriftliche Vereinbarung zur anzuwendenden Politik (d. h. eine Policy-Vereinbarung) treffen, der sich entnehmen lässt, dass die Beteiligten bei jeder geplanten Aktualisierung oder Erweiterung der betreffenden Systeme in der durch diese Norm vorgegebenen Richtung vorgehen werden.

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, die Privilegien und die Pflichten einer anfordernden Partei auf der antwortenden Seite nach der in der Vereinbarung festgelegten Politik bzw. Policy verwaltet werden. Aus diesem Grund müssen sowohl diejenigen, die Informationen und Dienstleistungen anfordern und/oder sie bereitstellen, als auch die angeforderten Informationen und Dienste in einer begrenzten Anzahl von Begriffen zusammengefasst und klassifiziert werden, um die Festlegung einer begrenzten Anzahl von Lösungskategorien zu ermöglichen. Basierend auf dieser Klassifizierung können dann Anwarterprozesse, Zielsensibilitätsprozesse und Policy-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 Aktionsplan, aus dem hervorgeht, auf welche Art und Weise diese Risiken zu beseitigen sind. Die Policy-Vereinbarung muss darüber hinaus einen Zeitplan für diese Maßnahmen und eine Vereinbarung zu deren Finanzierung enthalten.

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

Im Teil 1 *Übersicht und Policy-Management* werden die für den grenzüberschreitenden Informationsaustausch geltenden Szenarien und die wesentlichen Parameter beschrieben. Außerdem enthält dieser Teil Beispiele für die als Grundlage der Policy-Vereinbarung erforderlichen Dokumentationsverfahren.

In Teil 2 *Formale Modelle* werden die Architekturen und zugrundeliegenden Modelle für das Privilegienmanagement und die Zugriffssteuerung beschrieben und ausführlicher erläutert, die für die Sicherheit bei der gemeinsamen Nutzung von Informationen erforderlich sind, einschließlich der formalen Darstellung von Policies.

In Teil 3 *Implementierungen* werden Beispiele für implementierbare Spezifikationen von Anwendungssicherheitsdiensten und Infrastrukturdiensten mit Hilfe verschiedener Spezifikationssprachen beschrieben.

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 und professionelle Normen sowie rechtliche und ethische Gesichtspunkte ein. Dieses Dokument führt Grundsätze ein und spezifiziert Dienste, die für das Management von Privilegien und für die Zugriffssteuerung erforderlich sind. Die Verschlüsselungsprotokolle sind nicht Gegenstand des vorliegenden Dokuments.

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. auf ISO-, CEN-, ASTM-, OMG-, W3C- und ähnliche Dokumente, und unterstützt bestehende einschlägige Normen oder benennt Erweiterungen oder Änderungen oder weist auf den Bedarf an neuen Normen hin.

Diese Internationale Norm ist eng mit anderen einschlägigen ISO-Normen und -Spezifikationen verbunden, so z. B. mit ISO 17090 „*Medizinische Informatik — Public-Key-Infrastruktur*“, und ISO 21091 „*Medizinische Informatik — Verzeichnisdienste für Anbieter, zu Behandelnde und andere Entitäten im Gesundheitswesen*“, und ISO/TS 21298 „*Medizinische Informatik — Funktionelle und strukturelle Rollen*“.

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

Die verteilte Architektur von gemeinsam genutzten Informationssystemen im Gesundheitswesen mit dem Trend zu einer die persönliche Gesundheit unterstützenden dienstorientierten Architektur (en: Service Oriented Architecture, SOA) ist zunehmend netzwerkorientiert. Um der Herausforderung der Interoperabilität gerecht zu werden, werden immer häufiger genormte Benutzerschnittstellen, Tools und Protokolle verwendet, wodurch sichergestellt wird, dass es egal ist, welche Plattform zum Einsatz kommt, und entsprechend ist in den letzten Jahren auch die Anzahl der auf Firmennetzwerken und virtuellen Privatnetzen basierenden, tatsächlich offenen Informationssysteme rasch angestiegen.

Die vorliegende Internationale Norm soll dem Bedarf in Bezug auf die gemeinsame Nutzung von gesundheitsbezogenen Informationen durch nicht miteinander verbundene Anbieter und Organisationen des Gesundheitswesens, Krankenversicherungen, deren Patienten, Mitarbeiter und Handelspartner Rechnung tragen.

Diese Internationale Norm soll den Abruf von Informationen durch sowohl Einzelpersonen als auch Anwendungssysteme unterstützen.

Diese mehrteilige Internationale Norm legt Verfahren für das Management von Privilegien und für die Steuerung des Zugriffs auf Daten und/oder Funktionen fest. Sie ermöglicht die Überbrückung von Policies. Sie basiert auf einem begrifflichen Modell, bei dem lokale Server für das Management von Autorisierungen und ein grenzüberschreitender Verzeichnisserver in verschiedenen Anwendungen (Softwarekomponenten) zur Zugriffssteuerung dienen können. Dieser Verzeichnisserver liefert Informationen zu den Regeln für den Zugriff auf unterschiedliche Anwendungsfunktionen basierend auf Rollen und anderen Attributen des betreffenden Benutzers. Ob das Zugriffsrecht erteilt wird, hängt von den folgenden Aspekten ab:

- der authentisierten Identifikation des Benutzers;
- den Regeln für den Zugriff auf ein bestimmtes Informationsobjekt einschließlich Verwendungszweck;
- den Regeln bezüglich der mit dem Benutzer verknüpften und vom Berechtigungsmanager bereitgestellten Autorisierungsattribute;
- den Funktionen der betreffenden Anwendung.

Diese Internationale Norm sollte in einem Gesichtsfeld Anwendung finden, das von lokalen über regionale hin zu nationalen Situationen reicht. Einer der Hauptpunkte dieser Gesichtsfelder ist, dass organisatorische Kriterien mit Autorisierungsprofilen zu kombinieren sind, auf die sich sowohl die anfordernde als auch die die entsprechenden Informationen bereitstellende Seite in einer schriftlichen Policy-Vereinbarung geeinigt haben.

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

Diese Zusammenarbeit wird in einer von allen beteiligten Organisationen unterzeichneten *Policy-Vereinbarung* festgelegt, die die Regeln für den betreffenden Vorgang enthält.

Basierend auf dem oben genannten 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 Meta-modelle 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 Teil 2 wiedergegebenen Grundlagen werden die unterschiedlichen Möglichkeiten zur Darstellung der unterschiedlichen Reifegrade bei unterschiedlichen Gaden der Interoperabilität unter der idealen Situation einer semantisch ((...)) erörtert.

- Für diese unterschiedlichen Umgebungen und Grade bzw. Stufen gibt der vorliegende Teil 3 dieser Technischen Spezifikation Beispiele für die Spezialisierung und Implementierung der auf ISO/IEC 10746 „*Informationstechnik — Verteilte Verarbeitung in Offenen Systemen — Referenzmodell*“ basierenden und in Teil 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, der Organization for the Advancement of Structured Information Standards, festgelegten Sprachen SAML (Security Assertion Markup Language) und XACML (XML Access Control Markup Language) angegeben. Zusätzliche Spezifikationen werden auch in der traditionellen ASN.1-Syntax dargestellt.

Diese Internationale Norm wurde in wesentlichen Teilen mit ASTM E2595-07 *Privilege Management Infrastructure* harmonisiert.

1 Anwendungsbereich

Diese mehrteilige Internationale Norm legt die Privilegienmanagement- und Zugriffssteuerungsdienste fest, die für die Kommunikation und Nutzung von über die Grenzen von Domains und Sicherheitsbereichen hinweg verteilten gesundheitsbezogenen Informationen erforderlich sind. Das vorliegende Dokument führt Grundsätze ein und spezifiziert die für das Privilegienmanagement und die Zugriffssteuerung erforderlichen Dienste. Es legt die erforderlichen komponentenbasierten Begriffe fest und soll deren technische Implementierung unterstützen. Es legt jedoch nicht fest, wie diese Begriffe in speziellen klinischen Prozessabläufen zu verwenden sind, und es befasst sich auch nicht mit den gegebenenfalls mit ihrer Nutzung verbundenen Sicherheitsproblemen.

Während Teil 1 eine beschreibende Einleitung zum Problem des Policy-Bridgings im Zusammenhang mit der Kommunikation und Kooperation zwischen Organisationen gibt, legt Teil 2 einen generischen Entwicklungsprozess für die semantische Analyse, Auslegung, Implementierung und Nutzung von Informationssystemen des Gesundheitswesens fest. Die aufgrund der gesetzlichen, sozialen, organisatorischen, benutzerbezogenen, funktionellen und technologischen Anforderungen erforderlichen Sicherheitsdienste müssen unter Einhaltung der Paradigmen für semantische Interoperabilität in die moderne und nachhaltige Systemarchitektur eingebunden werden.

Der vorliegende Teil 3 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 Teil 2 spezifizierten formalen Modelle.

Diese Internationale Norm enthält weder plattformspezifische noch implementierungstechnische Einzelheiten. Sie legt keine technischen Kommunikationssicherheitsdienste, Authentisierungsverfahren und -protokolle fest, die bereits in anderen Normen festgelegt sind, wie z. B. in ISO 7498-2 *Informationsverarbeitungssysteme — Kommunikation offener Systeme — Basisreferenzmodell — Teil 2: Sicherheitsarchitektur*, ISO/IEC 10745 (ITU-T X.803); ISO/IEC TR 13594, *Informationstechnik — Sicherheit in den unteren Schichten* (ITU-T X.802); ISO/IEC 10181-1 (ITU-T X.810); ISO/IEC 9594-8, *Informationstechnik — Kommunikation Offener Systeme — Verzeichnisdienst: Rahmenrichtlinien für "Public Key" und Attribut-Zertifikat* (äquivalent mit ITU-T X.509); ISO/IEC 9796 *Informationstechnik — IT-Sicherheitsverfahren — Digitale Signaturschemata welche die Nachricht wieder herstellen* (Teil 1 und Teil 2); ISO/IEC 9797, *Information technology — Security techniques — Message Authentication Codes (MACs)*; ISO/IEC 9798, *Informationstechnik — IT-Sicherheitsverfahren — Authentifikation von Instanzen*.

2 Normative Verweisungen

Die folgenden zitierten Dokumente 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).

ASTM E1986, *Standard Guide for Information Access Privileges to Health Information list of "Healthcare Personnel that Warrant Differing Levels of Access Control"*

ASTM E2595-07, *Standard Guide on Privilege Management Infrastructure*

E 1714-00, *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)*

E 1762-95:2003, *Standard Guide for Electronic Authentication of Health Care Information*

E 1986-98, *Standard Guide for Information Access Privileges to Health Information*

E 1985-98, *Standard Guide for User Authentication and Authorization*

E 2084-00, *Standard Specification for Authentication of Healthcare Information Using Digital Signatures*

E 2085-00a, *Standard Guide on Security Framework for Healthcare Information*

E 2212-02a, *Standard Practice for Healthcare Certificate Policy*

ANSI INCITS 359-2004 19, *Role Based Access Control*, Februar 2004

ISO 9594-8:2000, *The Directory: Public-Key and Attribute Certificate Frameworks* (auch als ITU-T X.509:2000 verfügbar)

ISO 10181-3-00, *Security Frameworks for Open Systems: Access Control Framework* (auch als ITU-T X.812:1995 verfügbar)

Extensible Access Control Markup Language (XACML) v2.0, Februar 2005

XACML Profile for Role Based Access Control (RBAC): Committee Draft 01 (normativ; 13.02.2004)

OASIS, *Security Assertion Markup Language (SAML) v2.0*, März 2005

Security Provisioning Markup Language (SPML) V1.0, (OASIS 200306), Oktober 2003

Universal Description, Discovery and Integration v3.0.2 (UDDI), Februar 2005

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

[ISO/IEC 2382-8]

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)

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

3.5

Zurechenbarkeit

(en: accountability)

Eigenschaft, durch die sichergestellt wird, dass die Aktionen einer Entität eindeutig auf diese zurückgeführt werden können

[ISO 7498-2]

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

[ISO 10181-1]

3.7

Attributautorisierer

(en: attribute authority, AA)

Behörde, die durch Ausgabe von Attributzettifikaten Privilegien zuweist

[X.509]

3.8

Sperrliste des Attributautorisierers

(en: attribute authority revocation list, AARL)

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

3.9

Attributzettifikat

(en: attribute certificate)

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

[X.509]

3.10

Attributzettifikate-Sperrliste

(en: attribute certificate revocation list, ACRL)

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

3.11

Authentisierung

(en: authentication)

Bebringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators. Siehe auch Authentisierung der Datenherkunft und Authentisierung der Partnerinstanz

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

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. In der vorliegenden Spezifikation werden zwei Typen unterschieden: die Zertifizierungsstelle, die Public-Key-Zertifikate ausgibt, und der Attributautorisierer, der Attributzettifikate ausgibt

3.14

Autoritätszettifikat

(en: authority certificate)

an eine Zertifizierungsstelle oder einen Attributautorisierer ausgegebenes Zertifikat

[angepasst aus X.509]

3.15

Behördensperrliste

(en: authority revocation list, ARL)

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

3.16

Autorisierung

(en: authorisation)

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

ANMERKUNG Abgeleitet aus ISO 7498-2: Vergabe von Rechten, einschließlich der Gewährung des Zugriffs aufgrund von entsprechenden Zugriffsrechten.

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

[ISO 7498-2]

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. 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 Zertifikat-inhaber, 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. 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 dieser Verzeichnisspezifikation festgelegten Funktionen, die von einem Zertifikatsbenutzer 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

(en: certification authority, CA)

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

ANMERKUNG 1 Wahlweise darf die Zertifizierungsstelle die Schlüssel der vertrauenden Parteien erzeugen.

[ISO 9594-8]

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 bzw. 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. Der semantische Gehalt der so erzeugten Daten ist nicht verfügbar

[ISO 7498-2]

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)

[ISO 7498-2]

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. 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; 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 mit dem Ziel verkörpert, deren Informationsgehalt zu verbergen und ihre unerkannte Änderung und/oder nicht autorisierte Nutzung zu verhindern

[ISO 7498-2]

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

[ISO 7498-2]

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). 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. 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

[ISO 7498-2]

3.49

Authentisierung der Datenherkunft

(en: data origin authentication)

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

[ISO 7498-2]

3.50

Entschlüsselung, Dechiffrierung

(en: decipherment, decryption)

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

ANMERKUNG Ein chiffrierter Text kann ein zweites Mal verschlüsselt werden, was dazu führt, dass eine einzelne Entschlüsselung nicht den ursprünglichen Klartext ergibt.

[ISO/IEC 2382-8]

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), 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

[ISO 7498-2]

3.55

Chiffrierung, Verschlüsselung

(en: encipherment, encryption)

kryptographische Umwandlung von Daten (siehe Kryptographie) zur Erzeugung eines chiffrierten Textes

[ISO 7498-2]

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)

diejenigen 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)

funktionelle Rollen sind an eine Handlung gebunden. Funktionelle Rollen können so zugewiesen werden, dass sie während einer Handlung ausgeführt werden müssen. Sie entsprechen der RIM-Beteiligung

[ISO/TS 21298]

ANMERKUNG Siehe auch strukturelle Rolle.

3.62

Hash-Funktion

(en: hash function)

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

[ISO/IEC 2382-8]

3.65

Identifikator

(en: identifier)

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

[ENV 13608-1]

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

[ISO/IEC 7498-2]

3.68

Schlüssel

(en: key)

Symbolfolge, die die Verschlüsselungs- und Entschlüsselungsoperationen steuert

[ISO 7498-2]

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 Zu weiteren Informationen über Schlüsselvereinbarungsverfahren siehe ISO/IEC 11770-1.

3.70

Schlüsselmanagement

(en: key management)

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

[ISO 7498-2]

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

[ASTM]

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. 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 Objektmethode(n) 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: $f(x) = y$. 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

[NIST]

3.78

Policy

Menge 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. 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] definiert. Er entspricht dem Begriff der „Zugriffsentscheidungsfunktion“ (en: Access Decision Function, ADF) in [ISO 10181-3]

3.81

Policy Enforcement Point

PEP

Systementität, die die Zugriffssteuerung ausführt, indem sie Entscheidungsanträge stellt und Autorisierungsentscheidung durchsetzt. 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] definiert. Er entspricht dem Begriff der „Zugriffsdurchsetzungsfunktion“ (en: Access Enforcement Function, AEF) in [ISO 10181-3]

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

Akteur, der in der Lage ist, bestimmte Szenarien in die Realität umzusetzen (Benutzer, Organisation, System, Gerät, Anwendung, Komponente, Objekt)

[OMG]

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

[ISO 10181-1]

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 Attributzzertifikat 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. 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

[ISO 10181-1]

3.91

Public-Key-Zertifikat

(en: public key certificate, PKC)

Zertifikat, das eine Identität und einen öffentlichen Schlüssel bindet. 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

[X.509, 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. 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

[RFC 2527]

3.94

Rolle

(en: role)

Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen. Für das Management von rollenbezogenen Beziehungen zwischen den Entitäten können strukturelle und funktionelle Rollen festgelegt werden

[ISO/TS 21298]

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. 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

[CEN]

3.100

Sicherheits-Policy

(en: security policy)

Aktionsplan oder Vorgehensweise für die Sicherstellung der Rechnersicherheit

[ISO/IEC 2382-8]

Reihe der 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

[ISO 7498]

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. Ein besonderer Attributautorisierer, dem ein Prüfer ein unbegrenztes Privileg einräumt. 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)

strukturelle Rollen spezifizieren Beziehungen zwischen Entitäten im Sinne der Kompetenz (RIM-Rollen) und spiegeln damit häufig organisatorische oder strukturelle Beziehungen (Hierarchien) wider

[ISO/TS 21298]

ANMERKUNG Siehe auch funktionelle Rolle.

3.106

Ziel

(en: target)

Ressource, auf die von einem Anwarter zugegriffen wird. Deren Sensibilität wird in der vorliegenden Norm als eine Sammlung von Attributen modelliert, die entweder als ASN.1-Attribute oder als XML-Elemente dargestellt werden

3.107

Vertrauen

(en: trust)

im Allgemeinen kann davon ausgegangen werden, dass eine Entität einer anderen Entität „vertraut“, wenn sie annehmen kann, dass sich die zweite Entität genauso, wie von der ersten Entität erwartet, verhalten wird. Dieses Vertrauen kann möglicherweise nur für eine bestimmte Funktion gelten. Die Hauptaufgabe des Vertrauens in diesem Framework ist, die Beziehung zwischen einer authentisierenden Entität und einer Behörde zu beschreiben; eine Entität muss sich sicher sein, dass sie der Behörde vertrauen kann, dass diese 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

[ENV 13608-1]

ANMERKUNG 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. 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 Spezifikation 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
ACI	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 Objektanforderungsmakler-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 Kryptosystem	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	Dienstorientierte 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 (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. Die vorliegende Norm verlangt keine Policy-Darstellungssprache.