

DIN EN ISO 22600-2

ICS 35.240.80

**Medizinische Informatik –
Privilegienmanagement und Zugriffssteuerung –
Teil 2: Formale Modelle (ISO 22600-2:2014);
Deutsche Fassung EN ISO 22600-2:2014**

Health informatics –
Privilege management and access control –
Part 2: Formal models (ISO 22600-2:2014);
German version EN ISO 22600-2:2014

Informatique de santé –
Gestion de privilèges et contrôle d'accès –
Partie 2: Modèles formels (ISO 22600-2:2014);
Version allemande EN ISO 22600-2:2014

Gesamtumfang 35 Seiten

DIN-Normenausschuss Medizin (NAMed)

Nationales Vorwort

Die vorliegende Norm enthält die deutsche Übersetzung der ISO 22600-2:2014, 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 22600-2 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 4, 5, 6, 9, 10, A.3, A.4 und A.5 sowie die Tabellen 1, 2 und A.1 wurden im englischen Original beibehalten, da ihre Übersetzung nicht notwendig erschien und die angesprochene IT-Zielgruppe üblicherweise über ausreichende Englischkenntnisse verfügt.

Für die in diesem Dokument zitierte Internationale Norm wird im Folgenden auf die entsprechende Deutsche Norm hingewiesen:

ISO/IEC 27002 siehe DIN ISO/IEC 27002

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

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 27002 *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informations-sicherheits-Management (zurzeit Entwurf)*

Deutsche Fassung

Medizinische Informatik —
Privilegienmanagement und Zugriffssteuerung —
Teil 2: Formale Modelle (ISO 22600-2:2014)

Health informatics —
Privilege management and access control —
Part 2: Formal models (ISO 22600-2:2014)

Informatique de santé —
Gestion de privilèges et contrôle d'accès —
Partie 2: Modèles formels (ISO 22600-2:2014)

Diese Europäische Norm wurde vom CEN am 22. Mai 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	13
5 Komponentenparadigma	13
6 Generische Modelle	14
6.1 Framework.....	14
6.2 Domainmodell	16
6.3 Dokumentmodell	17
6.4 Policy-Modell	18
6.5 Rollenmodell	21
6.6 Autorisierungsmodell – Rollen- und Privilegienzuweisung	22
6.7 Steuerungsmodell.....	23
6.8 Delegierungsmodell	23
6.9 Zugriffssteuerungsmodell	25
Anhang A (informativ) Funktionelle und strukturelle Rollen	27
A.1 Mit dem Gesundheitswesen verbundene Rollen	27
A.2 Modell der funktionellen Rollen	28
A.3 Modell der strukturellen Rollen	30
A.4 Spezifikation der generischen Rollen.....	30
Literaturhinweise	32

Vorwort

Dieses Dokument (EN ISO 22600-2:2014) 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 22600-2:2014 wurde vom CEN als EN ISO 22600-2:2014 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 Szenariums 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 definieren, 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 Norm vorgegebenen Richtung vorgehen werden. Der Grad der Formalisierung und Granularität der Policies und die Objekte dieser Policies sind daran gebunden, die Lösung in Richtung der vorgestellten Spezifikation zu definieren.

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 (alle Teile), ISO 22857, ISO 21091 und ISO 21298.

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

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 22600 führt das zugrundeliegende Paradigma von formalen High-Level-Modellen für Architekturkomponenten ein. Es basiert auf ISO/IEC 10746 (alle Teile) und führt das Domainmodell, das Dokumentmodell, das Policy-Modell, das Rollenmodell, das Autorisierungsmodell, das Delegierungsmodell, das Steuerungsmodell und das Zugriffssteuerungsmodell ein.

Die Spezifikationen werden unter Verwendung der Metasprachen Unified Modelling Language (UML, de: Vereinheitlichte Modellierungssprache) und Extensible Markup Language (XML, de: Erweiterbare Auszeichnungssprache) angegeben. Zur Erläuterung der Grundsätze werden weitere Diagramme verwendet. Die verwendeten Attribute wurden auf das HL7-Referenzinformationsmodell (siehe ISO 21731:2006) und die HL7-Datentypdefinitionen referenziert.

Das Rollenmodell wird nur umrissartig und unter Verweisung auf ISO 21298 vorgestellt.

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 21298:—¹⁾, *Health informatics — Functional and structural roles*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden 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

Zurechenbarkeit

(en: accountability)

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

[QUELLE: ISO 7498-2:1989]

1) Zu veröffentlichen

3.3

Attributautorisierer

(en: attribute authority, AA)

Behörde, die durch Ausgabe von Attributzertifikaten Privilegien zuweist

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

3.4

Attributzertifikat

(en: attribute certificate)

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

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

3.5

Authentisierung

(en: authentication)

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

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

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

3.6

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.

3.7

Autorisierung

(en: authorisation)

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

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

3.8

Verfügbarkeit

(en: availability)

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

[QUELLE: ISO 7498-2:1989]

3.9

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

3.10

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

Anmerkung 1 zum Begriff: Wahlweise kann die Zertifizierungsstelle die Schlüssel der vertrauenden Parteien erzeugen. Die CA gibt Zertifikate durch Signieren von Zertifikatsdaten mit ihrem privaten Signaturschlüssel aus.

Anmerkung 2 zum Begriff: 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.

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

3.11

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

3.12

Vertraulichkeit

(en: confidentiality)

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

[QUELLE: ISO 7498-2:1989]

3.13

Identitätsnachweis

(en: credential)

als Voraussetzung ausgegebener Beleg für den Anspruch auf oder die Berechtigung zu einer Rolle

3.14

Delegierung

(en: delegation)

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

3.15

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

3.16

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 örtliches Mittel zur Verfügung stehen (z. B. Tageszeit oder aktueller Kontostand)