

DIN EN ISO 22600-1

ICS 35.240.80

Einsprüche bis 2013-04-25

Entwurf

**Medizinische Informatik –
Privilegienmanagement und Zugriffssteuerung –
Teil 1: Übersicht und Policy-Management (ISO/DIS 22600-1:2012);
Deutsche Fassung prEN ISO 22600-1:2012**

Health informatics –
Privilege management and access control –
Part 1: Overview and policy management (ISO/DIS 22600-1:2012);
German version prEN ISO 22600-1:2012

Informatique de santé –
Gestion de privilèges et contrôle d'accès –
Partie 1: Vue d'ensemble et gestion des politiques (ISO/DIS 22600-1:2012);
Version allemande prEN ISO 22600-1:2012

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 36 Seiten

Normenausschuss Medizin (NAMed) im DIN

Nationales Vorwort

Dieses Dokument (prEN ISO 22600-1:2012) 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.

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 1: Übersicht und Policy-Management (ISO/DIS 22600-1:2012)

Informatique de santé — Gestion de privilèges et contrôle d'accès — Partie 1 : Vue d'ensemble et gestion des politiques (ISO/DIS 22600-1:2012)

Health informatics — Privilege management and access control — Part 1: Overview and policy management (ISO/DIS 22600-1:2012)

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	8
2 Begriffe	9
3 Abkürzungen	12
4 Ziel und Struktur von Privilegienmanagement und Zugriffssteuerung	12
4.1 Ziel von Privilegienmanagement und Zugriffssteuerung	12
4.2 Struktur von Privilegienmanagement und Zugriffssteuerung	12
4.2.1 Strukturelemente	12
4.2.2 Domain	13
4.2.3 Policy	13
4.2.4 Rollen	14
4.2.5 Policy-Repository	14
4.2.6 Verzeichnis	14
4.2.7 Authentisierung	15
4.2.8 Prozess	15
5 Policy-Vereinbarung	17
5.1 Übersicht	17
5.2 Identifizierung	17
5.3 Zustimmung des Patienten	17
5.4 Schutz von Patientendaten	17
5.5 Informationsidentifizierung	17
5.6 Speicherort der Information(en).....	18
5.7 Integrität der Information(en)	18
5.8 Sicherheit.....	18
5.9 Autorisierung	18
5.10 Rollenstrukturen	18
5.11 Zuweisungs- und Bestätigungsautorität	18
5.12 Delegation.....	18
5.13 Gültigkeitsdauer.....	19
5.14 Authentisierung von Benutzern/Rollen	19
5.15 Zugriff.....	19
5.16 Gültigkeitsdauer der Policy-Vereinbarung.....	19
5.17 Ethos	19
5.18 Sichere Zugriffsprotokollierung	19
5.19 Auditprüfung	20
5.20 Risikoanalyse	20
5.21 Kontinuitäts- und Katastrophenmanagement	20
5.22 Zukünftige Systementwicklungen.....	20
6 Dokumentation.....	20
Anhang A (informativ) Beispiel einer Textschablone für die Dokumentation.....	21
A.1 Beschreibung der Systeme und des Informationsaustauschs.....	21
A.2 Administrativer Abschnitt der Dokumenttextschablone	21
A.3 Auswertungsabschnitt der Textschablone für die Dokumentation.....	22
A.3.1 Klassifizierungsschema	22
A.3.2 Grundlegende Checklisten	23
A.3.3 Sicherheitschecklisten	25
A.3.4 Checklisten für Administratoren	26

Anhang B (informativ) Beispiel einer Policy-Vereinbarung für den Informationsaustausch.....	28
B.1 Einleitung zur Vereinbarung	28
B.2 Administrativer Teil	28
B.2.1 An dieser Vereinbarung beteiligte Parteien	28
B.2.2 Geltungsbereich der Vereinbarung	28
B.2.3 Spezifizierung der Informationen	28
B.2.4 Ansprechpartner.....	28
B.2.5 Anmerkungen der Informationssicherheitsabteilung.....	29
B.2.6 Sonstige Aspekte/Probleme	29
B.2.7 Unterschriften	30
B.3 Beispiel für den Inhalt einer „Allgemeinen Policy-Vereinbarung“	30
B.3.1 Geltungsbereich	30
B.3.2 Begriffe	30
B.3.3 Das System	30
B.3.4 Informationsaustausch	31
B.3.5 Örtliche Informationsverantwortungen.....	31
B.3.6 Übertragung und Empfang der Informationen	31
B.3.7 Sicherheit	31
B.3.8 Datenschutz	31
B.3.9 Verfügbarkeit	32
B.3.10 Informationsverpflichtung	32
B.3.11 Archivierung	32
B.3.12 Verantwortlichkeiten	32
B.3.13 Hindernisgründe.....	32
B.3.14 Bedingungen der Vereinbarung.....	33
B.3.15 Änderungen und Hinzufügungen	33
B.3.16 Übertragung	33
B.3.17 Streitfälle	33
Literaturhinweise	34

Vorwort

Dieses Dokument (prEN ISO 22600-1:2012) 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 ISO/TS 22600-1:2006 ersetzen.

Anerkennungsnotiz

Der Text von ISO/DIS 22600-1:2012 wurde vom CEN als prEN ISO 22600-1:2012 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 Rollen geht. Ein und derselbe Benutzer kann zu verschiedenen Zeiten unterschiedliche Rollen und auch zwei oder mehr Rollen gleichzeitig innehaben. So kann ein Benutzer z. B. für zwei Monate als Krankenschwester und dann für die nächsten beiden Monate als Hebamme arbeiten oder diese beiden Rollen innerhalb desselben Zeitraums gleichzeitig innehaben.

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 die Informationen unterschiedliche Regeln zu den Privilegien und zu deren Management 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 und die Privilegien 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 Konzepten zusammengefasst und klassifiziert werden, um die Festlegung einer begrenzten Anzahl von Lösungskategorien zu ermöglichen. Basierend auf dieser Klassifizierung können dann Anwärterprozesse, 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 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.

Im Teil 1 *Übersicht und Policy-Management* werden die für den Informationsaustausch über die Grenzen von Policy-Domains hinweg 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 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.

1 Anwendungsbereich

Die verteilte Architektur von gemeinsam genutzten Informationssystemen im Gesundheitswesen 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.

Diese mehrteilige Internationale Norm legt die Privilegienmanagement- und Zugriffssteuerungsdienste fest, die für die Kommunikation und Nutzung von über die Grenzen von Policy-Domains 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.

Diese Internationale Norm ist eng mit anderen Arbeitsprojekten des ISO/TC 215 verbunden, so z. B. mit ISO 17090 „Medizinische Informatik — Public-Key-Infrastruktur“, ISO 22857 „Medizinische Informatik — Leitlinien für den Datenschutz zur Ermöglichung grenzüberschreitender Kommunikation von persönlichen Gesundheitsinformationen“ und ISO 21091 „Medizinische Informatik — Verzeichnisdienste für Anbieter, zu Behandelnde und andere Entitäten im Gesundheitswesen“. Sie steht darüber hinaus in Zusammenhang mit der laufenden Arbeit an ISO/TS 21298 „Medizinische Informatik — Funktionelle und strukturelle Rollen“.

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 die Handhabung von Autorisierungen 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 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 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.

In Teil 1 wird ein Dokumentationsformat vorgeschlagen, das als Textschablone (Template) für die Darstellung der Policy-Vereinbarung gedacht ist und das es ermöglicht, von allen am Informationsaustausch beteiligten Parteien jeweils vergleichbare Dokumentationen zu erhalten.

Die vorliegende Internationale Norm enthält weder plattformspezifische noch implementierungstechnische Einzelheiten. Sie legt keine technischen Kommunikationsdienste und -protokolle fest, die bereits in anderen Normen festgelegt sind. Sie enthält auch keine Authentisierungsverfahren.

2 Begriffe

Die nachstehende Liste von Begriffen enthält alle in dieser Spezifikation verwendeten Benennungen und ihre Definitionen.

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

Zurechenbarkeit

(en: accountability)

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

[ISO 7498-2]

3.3

Attributzertifikat

(en: attribute certificate)

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

3.4

Authentisierung

(en: authentication)

Beibringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators. Siehe auch Authentisierung des Absenders der Daten und Authentisierung der Partnerinstanz

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

3.5

Autorisierer, Behörde, Autorität

(en: authority)

Entität, die für die Ausgabe von Zertifikaten verantwortlich ist. In der vorliegenden Spezifikation werden zwei Typen definiert: die Zertifizierungsstelle, die Public-Key-Zertifikate ausgibt, und der Attributautorisierer, der Attributzertifikate ausgibt

3.6

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.