

DIN EN ISO/IEC 29146



ICS 35.030

Einsprüche bis 2023-01-18

Entwurf

**Informationstechnologie –
Sicherheitstechniken –
Ein Rahmen für die Zugangsverwaltung (ISO/IEC 29146:2016);
Deutsche und Englische Fassung prEN ISO/IEC 29146:2022**

Information technology –
Security techniques –
A framework for access management (ISO/IEC 29146:2016);
German and English version prEN ISO/IEC 29146:2022

Technologies de l'information –
Techniques de sécurité –
Cadre pour gestion d'accès (ISO/IEC 29146:2016);
Version allemande et anglaise prEN ISO/IEC 29146:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-11-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe 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 nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, 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 89 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 29146:2016 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 29146:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-14 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 24760-2:2015	siehe	DIN EN ISO/IEC 24760-2:202X-XX*
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06**
ISO/IEC 29100	siehe	DIN EN ISO/IEC 29100
ISO/IEC 29101	siehe	DIN EN ISO/IEC 29101

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

* Veröffentlichung in Vorbereitung.

** Enthält zusätzlich die Internationalen Berichtigungen ISO/IEC 27002 Technical Corrigendum 1:2013 und ISO/IEC 27002 Technical Corrigendum 2:2015.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 24760-2:202X-XX, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement — Teil 2: Referenzarchitektur und Anforderungen (ISO/IEC 24760-2:2015); Deutsche Fassung EN ISO/IEC 24760-2:2022*

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

DIN EN ISO/IEC 29100, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz*

DIN EN ISO/IEC 29101, *Informationstechnik — Sicherheitstechniken — Architekturrahmenwerk für Datenschutz*

– *Entwurf* –

E DIN EN ISO/IEC 29146:2022-12

– Leerseite –

**Informationstechnologie – Sicherheitstechniken – Ein Rahmen für die
Zugangsverwaltung (ISO/IEC 29146:2016)**

Information technology – Security techniques – A framework for access management (ISO/IEC 29146:2016)

Technologies de l'information – Techniques de sécurité – Cadre pour gestion d'accès (ISO/IEC 29146:2016)

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Abkürzungen	11
5 Konzepte	11
5.1 Ein Modell für die Steuerung des Zugriffs auf Ressourcen	11
5.1.1 Überblick	11
5.1.2 Beziehung zwischen Identitätsverwaltungssystem und Zugangsverwaltungssystem	12
5.1.3 Sicherheitsmerkmale des Zugangsverfahrens	13
5.2 Beziehungen zwischen logischer und physischer Zugangssteuerung	14
5.3 Funktionen und Prozesse des Zugangsverwaltungssystems	14
5.3.1 Überblick	14
5.3.2 Zugangssteuerungsrichtlinie	15
5.3.3 Rechteverwaltung	16
5.3.4 Verwaltung richtlinienbezogener Attributinformationen	17
5.3.5 Autorisierung	18
5.3.6 Überwachungsmanagement	19
5.3.7 Alarmverwaltung	20
5.3.8 Föderierte Zugangssteuerung	20
6 Referenzarchitektur	21
6.1 Überblick	21
6.2 Grundlegende Komponenten eines Zugangsverwaltungssystems	22
6.2.1 Authentisierungsendpunkt	22
6.2.2 Richtlinienentscheidungspunkt (PDP)	22
6.2.3 Richtlinieninformationspunkt (PIP)	22
6.2.4 Richtlinienverwaltungspunkt (PAP)	23
6.2.5 Richtlinienumsetzungspunkt (PEP)	23
6.3 Zusätzliche Dienstekomponenten	23
6.3.1 Allgemein	23
6.3.2 Subjektzentrierte Implementation	23
6.3.3 Unternehmenszentrierte Implementation	25
7 Zusätzliche Anforderungen und zu beachtende Punkte	27
7.1 Zugang zu administrativen Informationen	27
7.2 AMS-Modelle und Richtlinien	27
7.2.1 Zugangssteuerungsmodelle	27
7.2.2 Richtlinien in der Zugangsverwaltung	28
7.3 Rechtliche und behördliche Anforderungen	28
8 Praxis	29
8.1 Prozesse	29
8.1.1 Autorisierungsprozesse	29
8.1.2 Rechteverwaltungsprozesse	29
8.2 Bedrohungen	30
8.3 Maßnahmenziele	31
8.3.1 Allgemein	31
8.3.2 Validierung des Zugangsverwaltungsrahmens	31
8.3.3 Validierung des Zugangsverwaltungssystems	34
8.3.4 Validierung der Pflege eines implementierten AMS	38
Anhang A (informativ) Aktuelle Zugangsmodelle	41

A.1	Allgemein	41
A.2	Zugangssteuerungsmodelle	41
A.2.1	Allgemein	41
A.2.2	Benutzerbestimmbare Zugriffssteuerung (DAC)	41
A.2.3	Systembestimmte Zugangssteuerung (MAC)	41
A.2.4	Identitätsbasierte Zugangssteuerung (IBAC)	42
A.2.5	Rollenbasierte Zugangssteuerung (RBAC)	42
A.2.6	Attributbasierte Zugangssteuerung (ABAC)	43
A.2.7	Pseudonymbasierte Zugangssteuerung (PBAC)	43
A.2.8	Fähigkeitsbasierte Zugangssteuerung (CBAC)	44
	Literaturhinweise	46

Bilder

Bild 1	Modellhafte Abfolge der Zugangssteuerung	12
Bild 2	Beziehung zwischen Identitätsverwaltungssystem und Zugangsverwaltungssystem	13
Bild 3	Autorisierung des Zugriffs durch Delegierte	19
Bild 4	Föderierte Zugangssteuerung	21
Bild 5	AMS-Referenzarchitektur	22
Bild 6	Interaktionen der Komponentendienste in einer subjektzentrierten Situation	24
Bild 7	Interaktionen der Komponentendienste in einer unternehmenszentrierten Situation	26

Europäisches Vorwort

Der Text von ISO/IEC 29146:2016 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ als prEN ISO/IEC 29146:2022 übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Anerkennungsnotiz

Der Text von ISO/IEC 29146:2016 wurde von CEN als prEN ISO/IEC 29146:2022 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Eine Erläuterung der Bedeutung ISO spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der Grundsätze der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: Foreword-Supplementaryinformation.

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques*.

Einleitung

Das Management der Informationssicherheit ist eine komplexe Aufgabe, die in erster Linie auf einem risikobasierten Ansatz beruht und von verschiedenen Sicherheitstechniken unterstützt wird. Die Komplexität wird von verschiedenen unterstützenden Systemen gehandhabt, die automatisch und konsistent einen Satz von Regeln oder Richtlinien anwenden können.

Im Rahmen des Managements der Informationssicherheit spielt die Zugangsverwaltung eine Schlüsselrolle für die Verwaltung der Beziehungen zwischen der den Zugang fordernden Partei (menschliche oder nicht-menschliche Subjekte) und den Informationstechnologieressourcen. Dank der Entwicklung des Internets können Informationstechnologieressourcen über verschiedene Netzwerke verteilt sein. Der Zugang zu ihnen muss in Übereinstimmung mit einer Richtlinie verwaltet werden. Es werden gemeinsame Bedingungen und Modelle als Rahmen für die Zugangsverwaltung erwartet.

Auch die Identitätsverwaltung ist ein wichtiger Teil der Zugangsverwaltung. Die Zugangsverwaltung wird durch die Identifizierung und Authentisierung von Subjekten, die Zugang zu Informationstechnologieressourcen anfordern, bewirkt. Diese Internationale Norm beruht auf das Vorhandensein eines zugrundeliegenden Identitätsverwaltungssystems oder einer Identitätsverwaltungsinfrastruktur (siehe Verweisungen in Abschnitt 2).

Der Rahmen für die Zugangsverwaltung ist ein Teil eines allgemeinen Identitäts- und Zugangsverwaltungsrahmens. Der andere Teil ist der Rahmen für die Identitätsverwaltung, der in ISO/IEC 24760 festgelegt ist.

Diese Internationale Norm beschreibt die Konzepte, Akteure, Komponenten, Referenzarchitektur, funktionellen Anforderungen und Praktiken für die Zugangssteuerung. Beispielhafte Modelle für die Zugangssteuerung sind enthalten.

Sie konzentriert sich hauptsächlich auf die Zugangssteuerung für eine Einzelorganisation, enthält jedoch auch Überlegungen für die Zugangssteuerung in kollaborativen Umgebungen über mehrere Organisationen hinweg.

1 Anwendungsbereich

Diese Internationale Norm legt einen Rahmen für die Zugangsverwaltung (AM, en: access management) und die sichere Verwaltung des Prozesses für den Zugriff auf Ressourcen der Informations- und Kommunikationstechnologie (IKT) im Zusammenhang mit der Rechenschaftspflicht eines Subjekts in einem gegebenen Kontext fest.

Diese Internationale Norm stellt Konzepte und Begriffe zur Verfügung, die auf verteilte Zugangsverwaltungstechniken in Netzwerkumgebungen anwendbar sind.

Diese Internationale Norm enthält ferner Erläuterungen zu zugehörigen Architekturen, Komponenten und Verwaltungsfunktionen.

Die an der Zugangsverwaltung beteiligten Subjekte könnten eindeutig als auf Informationssysteme wie in ISO/IEC 24760 zugreifend angesehen werden.

Art und Eigenschaften der zu Zugangsverwaltungssystemen gehörenden physischen Zugangssteuerung liegen nicht im Anwendungsbereich dieser Internationalen Norm.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 24760-1:2011, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

ISO/IEC 24760-2:2015, *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*

ISO/IEC 29115:2013, *Information technology — Security techniques — Entity authentication assurance framework*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 24760-1, ISO/IEC 29115 und die folgenden Begriffe.

3.1

Zugangssteuerung

Gewährung oder Verweigerung einer an einer *Ressource* (3.14) auszuführenden Operation

Anmerkung 1 zum Begriff: Ein primärer Zweck der Zugangssteuerung ist die Verhinderung des unbefugten Zugangs zu Informationen oder der unbefugten Nutzung von IKT-Ressourcen auf Grundlage der Geschäfts- und Sicherheitsanforderungen, d. h. die Anwendung von Autorisierungsrichtlinien auf einzelne Zugangsanfragen.

Anmerkung 2 zum Begriff: Wenn ein authentisiertes *Subjekt* (3.15) eine Anfrage stellt, gewährt (oder verweigert) der Eigentümer der Ressource den Zugang in Übereinstimmung mit den Zugangsrichtlinien und den Rechten des Subjekts.

3.2

Zugangsverwaltung

Satz von Prozessen für die Verwaltung der *Zugangssteuerung* (3.1) für einen Satz an *Ressourcen* (3.14)

3.3

Zugangstoken

vertrauenswürdige Objekt, das die Berechtigung eines *Subjekts* (3.15) beinhaltet, auf eine *Ressource* (3.14) zuzugreifen

Anmerkung 1 zum Begriff: Zugangstoken werden vom Richtlinienentscheidungspunkt (PDP, en: policy decision point) ausgegeben und vom Richtliniendurchsetzungspunkt (PEP, en: policy enforcement point) für die Ressource verbraucht.

Anmerkung 2 zum Begriff: Ein Zugangstoken darf Informationen für die Berechtigung eines Subjekts, auf die Ressource zuzugreifen, und Identifikationsinformationen für die Berechtigung der Autorisierungsentscheidung enthalten.

Anmerkung 3 zum Begriff: Ein Zugangstoken darf Informationen enthalten, die die Validierung seiner Integrität ermöglichen.

Anmerkung 4 zum Begriff: Die Form eines Zugangstokens darf physisch oder virtuell sein.

3.4

Attribut

Merkmal oder Eigenschaft, das bzw. die für die Beschreibung und die Steuerung des Zugangs zu einer *Ressource* (3.14) verwendet wird

Anmerkung 1 zum Begriff: Die Regeln für den Zugriff auf eine Ressource sind in einer Zugangssteuerungsrichtlinie (*Zugangssteuerung*, 3.1) festgelegt, die die für die Gewährung des Zugangs auf eine Ressource für eine bestimmte Operation durch ein *Subjekt* (3.15) benötigten Attribute spezifiziert.

Anmerkung 2 zum Begriff: Attribute können Subjektattribute, Ressourcenattribute, Umgebungsattribute und sonstige Attribute sein, die wie in der Zugangssteuerungsrichtlinie spezifiziert für die Zugangssteuerung verwendet werden.

3.5

Endpunkt

Ort in einem Zugangsverwaltungssystem (*Zugangsverwaltung*, 3.2), an dem eine Zugangssteuerungsfunktion (*Zugangssteuerung*, 3.1) ausgeführt wird

Anmerkung 1 zum Begriff: Die folgenden Endpunkttypen sind möglich:

- Authentisierungsendpunkt, an dem die Authentisierung des *Subjekts* (3.15) erfolgt;
- Autorisierungsendpunkt, an dem die Autorisierung des Subjekts erfolgt;
- Endpunkt-Suchdienst, der Endpunkte sucht und lokalisiert;
- initialer Endpunkt-Suchdienst, der zu Beginn der Interaktionen eines Subjekts mit einem Zugangsverwaltungssystem verwendet wird.

Anmerkung 2 zum Begriff: Endpunkt-Suchdienste werden häufig in verteilten und Netzwerksystemen verwendet.

3.6

unternehmenszentrierte Implementation

Zugangsverwaltung (3.2), die unter Kontrolle eines Richtlinienentscheidungspunkts erfolgt

3.7

Need-to-know-Prinzip

Sicherheitszielsetzung, die den Zugriff des *Subjekts* (3.15) auf *Datenressourcen* (3.14) auf ein Mindestmaß begrenzt, das nötig ist, damit ein eine Anfrage stellender Anwender seine Funktionen ausführen kann

Anmerkung 1 zum Begriff: Das Need-to-know-Prinzip wird nach Ermessen des Eigentümers der Ressource autorisiert.

Anmerkung 2 zum Begriff: Das Need-to-have-Prinzip ist die Sicherheitszielsetzung, dass die Ausführung bestimmter Aufgaben durch den Anfragersteller nach Ermessen des Eigentümers der Ressource beschränkt sein darf.

3.8

Rechte

Zugangsberechtigung

Zugangsrecht

Autorisierung eines *Subjekts* (3.15), auf eine *Ressource* (3.14) zuzugreifen

Anmerkung 1 zum Begriff: Die Zugangsberechtigung ist eine notwendige, aber nicht hinreichende Bedingung für den Zugang. Der Zugang erfolgt, wenn die Zugangsanfrage in Übereinstimmung mit der entsprechenden Zugangssteuerungsrichtlinie gewährt wird. Die Zugangssteuerungsrichtlinie basiert auf Rechten und darf weitere Umgebungsfaktoren beinhalten (zum Beispiel Uhrzeit, Standort usw.).

Anmerkung 2 zum Begriff: Rechte haben die Form von von einem Subjekt präsentierten oder für ein Subjekt gewonnenen Daten, die von einem Richtlinienentscheidungspunkt verwendet werden, um eine Operation zu genehmigen oder zu verweigern, die ein Subjekt an einer Ressource vorzunehmen beabsichtigt.

Anmerkung 3 zum Begriff: Mit einer Ressource dürfen mehrere voneinander abgegrenzte Rechte verbunden sein, mit denen sie verschiedene festgelegte Zugangsniveaus erfüllt. So könnten Datenressourcen zum Beispiel Lese-, Schreib-, Ausführungs- und Lösungsrechte für die Zuweisung zu Subjekten aufweisen. Eine Anfrage eines Subjekts für den Zugriff auf eine Ressource könnte je nach dem Zugangsniveau der Anfrage und den Rechten für die betreffende Ressource, die dem Subjekt zugewiesen wurden, für bestimmte Zugangsniveaus genehmigt, für andere jedoch verweigert werden.

3.9

Rolle

Bezeichnung eines definierten Satzes von Systemfunktionen, die von mehreren Entitäten durchgeführt werden dürfen

Anmerkung 1 zum Begriff: Der Name beschreibt üblicherweise die Funktion.

Anmerkung 2 zum Begriff: Entitäten können natürliche Personen sein, müssen dies jedoch nicht.

Anmerkung 3 zum Begriff: Rollen werden von einem Satz von Rechteattributen (*Rechte*, 3.8) implementiert, um den notwendigen Zugriff auf Datenressourcen oder Objekte bereitzustellen.

Anmerkung 4 zum Begriff: Einer Rolle zugewiesene Subjekte übernehmen die mit der Rolle verknüpften Zugangsrechte. Im operativen Einsatz müssen Subjekte als Mitglieder der Rollengruppe authentisiert werden, um die Funktionen der Rolle ausüben zu dürfen.

3.10

Richtlinienentscheidungspunkt

PDP, en: policy decision point

Dienst, der eine Zugangssteuerungsrichtlinie implementiert, um über Anfragen von Entitäten zum Zugriff auf *Ressourcen* (3.14) zu urteilen und Autorisierungsentscheidungen für die Verwendung durch einen *Richtliniendurchsetzungspunkt* (3.11) bereitzustellen

Anmerkung 1 zum Begriff: Autorisierungsentscheidungen werden von einem Richtliniendurchsetzungspunkt verwendet, um den Zugang zu einer Ressource zu steuern. Eine Autorisierungsentscheidung darf mithilfe eines *Zugangstokens* (3.3) kommuniziert werden.

Anmerkung 2 zum Begriff: Ein PDP protokolliert auch die Entscheidungen in einem Zugriffsprotokoll und ist in der Lage, Alarme auszulösen.

Anmerkung 3 zum Begriff: Der Begriff entspricht der Zugangsentscheidungsfunktion (ADF, en: Access Decision Function) in ISO 10181-3. Es wird vorausgesetzt, dass diese Funktion in einem Netzwerk des *Subjekts* (3.15) lokalisiert ist und über ein Netzwerk des entsprechenden *PEP* (3.11) lokalisiert sein darf.

3.11

Richtliniendurchsetzungspunkt

PEP, en: policy enforcement point

Dienst, der die Zugangsentscheidung des *Richtlinienentscheidungspunkts* (3.10) durchsetzt

Anmerkung 1 zum Begriff: Der PEP erhält die vom PDP getroffenen Autorisierungsentscheidungen und implementiert sie, um den Zugriff von Entitäten auf *Ressourcen* (3.14) zu steuern. Eine Autorisierungsentscheidung darf in Form eines von einem *Subjekt* (3.15) beim Stellen der Anfrage präsentierten *Zugangstokens* (3.3) empfangen werden.

Anmerkung 2 zum Begriff: Der Begriff entspricht der Zugangsdurchsetzungsfunktion (AEF, en: Access Enforcement Function) in ISO 10181-3. Es wird vorausgesetzt, dass diese Funktion in einem Netzwerk des Subjekts lokalisiert ist und über ein Netzwerk des entsprechenden *PDP* (3.10) lokalisiert sein darf.

3.12

Richtlinienverwaltungspunkt

PAP, en: policy administration point

Dienst, der die Zugangsautorisierungsrichtlinie verwaltet

3.13

Richtlinieninformationspunkt

PIP, en: policy information point

Dienst, der als Quelle von *Attributen* (3.4) dient, die von einem *Richtlinienentscheidungspunkt* (3.10) verwendet werden, um Autorisierungsentscheidungen zu treffen

Anmerkung 1 zum Begriff: Attribute können Ressourcen-, Subjekt- und Umgebungsrechte (*Ressource*, 3.14, *Subjekt*, 3.15, *Rechte*, 3.8) umfassen

3.14

Ressource

Objekt

physischer, Netzwerk- oder sonstiger Informationsgegenstand, auf den ein *Subjekt* (3.15) zur Nutzung zugreifen kann.

3.15

Subjekt

Entität, die den Zugriff auf eine von einem Zugangssteuerungssystem (*Zugangssteuerung*, 3.1) kontrollierten *Ressource* (3.14) anfragt

3.16

Sicherheitstokendienst

STS, en: security token service

Dienst, der auf Grundlage von Entscheidungen eines *Richtlinienentscheidungspunkts* (3.10) *Zugangstoken* (3.3) erstellt, austauscht und ausgibt

Anmerkung 1 zum Begriff: Dieser Dienst kann in separate Komponenten unterteilt sein.

3.17

subjektzentrierte Implementation

Zugangsverwaltung (3.2), die als von einem *Subjekt* (3.15) für die Erlangung der vom *Richtliniendurchsetzungspunkt* (3.11) für den Zugriff auf eine *Ressource* (3.14) anerkannten Mittel aufgerufener Komponentendienst implementiert ist

Anmerkung 1 zum Begriff: Komponentendienste dürfen einen Richtlinienentscheidungspunktdienst, einen Richtliniendurchsetzungspunktdienst und zugehörige Suchdienste umfassen, die es dem Subjekt ermöglichen, die Zugangssteuerungsdienste (*Zugangssteuerung*, 3.1) zu finden und zu kontaktieren.

4 Abkürzungen

AA	Attributautorität
ABAC	attributbasierte Zugangssteuerung (en: attribute-based access control)
ACL	Zugriffskontrollliste (en: access control list)
AM	Zugangsverwaltung (en: access management)
AMS	Zugangsverwaltungssystem (en: access management system)
CBAC	fähigkeitsbasierte Zugangssteuerung (en: capabilities-based access control)
DAC	benutzerbestimmbare Zugangssteuerung (en: discretionary access control)
IBAC	identitätsbasierte Zugangssteuerung (en: identity-based access control)
IKT	Informations- und Kommunikationstechnik
IMS	Identitätsmanagementsystem
IT	Informationstechnologie
MAC	systembestimmte Zugangssteuerung (en: mandatory access control)
PBAC	pseudonymbasierte Zugangssteuerung (en: pseudonym-based access control)
PAP	Richtlinienverwaltungspunkt (en: policy administration point)
PEP	Richtliniendurchsetzungspunkt (en: policy enforcement point)
PDP	Richtlinienentscheidungspunkt (en: policy decision point)
pbD	personenbezogene Daten
PIP	Richtlinieninformationspunkt (en: policy information point)
RBAC	rollenbasierte Zugangssteuerung (en: role-based access control)
REDS	Ressourcen-Endpunkt-Suchdienst (en: resource endpoint discovery service)
STS	Sicherheitstokendienst (en: security token service)
TLS	Transportschichtsicherheit (en: transport layer security)
XACML	erweiterbare Zugangssteuerungs-Auszeichnungssprache (en: extensible access control markup language)

5 Konzepte

5.1 Ein Modell für die Steuerung des Zugriffs auf Ressourcen

5.1.1 Überblick

Die konzeptuelle Abfolge für die Gewährung des Zugriffs auf eine Ressource sieht wie folgt aus:

- Bevor der Zugriff auf eine Ressource gewährt wird, ist die Authentisierung des Subjekts erforderlich. Die Authentisierung ist jedoch eine separate Funktion, die üblicherweise auf Sitzungsbasis implementiert wird statt für jede Zugangsanfrage.
- Die Autorisierungsentscheidung, den Zugriff auf die Ressource zu gewähren oder zu verweigern, wird auf Grundlage einer Richtlinie getroffen, und es wird ein Zugangstoken ausgegeben, um das Ergebnis der Entscheidung zu übermitteln.
- Die Durchsetzung der Autorisierung bei der Ressource erfolgt auf Grundlage der Entscheidung, und der Zugriff auf die Ressource wird gewährt.

Bild 1 zeigt diesen Entscheidungsablauf.

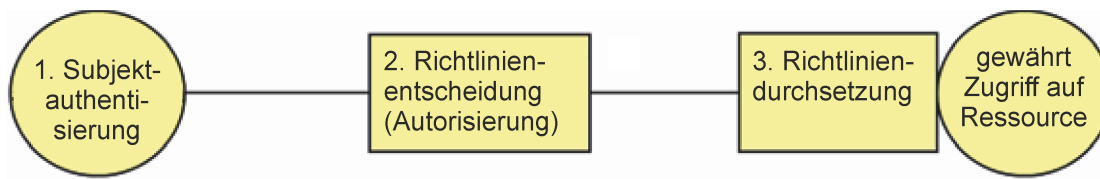


Bild 1 — Modellhafte Abfolge der Zugangssteuerung

Subjekt und Ressource sind als Kreise dargestellt, während konzeptuelle Funktionen als Rechteck dargestellt sind.

Im Hinblick auf den Zugriff auf die Ressource wird diese charakterisiert durch folgende Elemente:

- einen Bezeichner, entweder für eine bestimmte Ressource oder für eine Ressourcenklasse;
- einen oder mehrere Zugriffsmodi;
- einen Satz von mit den Zugriffsmodi und anderen Zugriffskriterien verknüpften Attributen wie in der Zugangssteuerungsrichtlinie angegeben.

Ein Zugangsverwaltungssystem ist für die Verwaltung und die Durchführung von Zugriffsautorisierungen verantwortlich. Autorisierungen werden von administrativen Handlungen unterstützt, die Ressourcenattribute und Subjektrechte in Übereinstimmung mit der Zugangsverwaltungsrichtlinie zuweisen und pflegen.

Ressourcen in IT-Systemen sind üblicherweise dynamisch. Sie durchlaufen einen Lebenszyklus von der Erstellung bis zur Vernichtung, dabei handelt es sich um einen kontinuierlichen Prozess.

- a) Ressourcen haben einen Lebenszyklus, der sich von der Erstellung bis hin zur Vernichtung erstreckt.
- b) Ressourcen werden kontinuierlich erstellt, aktualisiert und vernichtet.
- c) Ressourcen müssen (üblicherweise zum Zeitpunkt ihrer Erstellung) Zugangsattribute zugewiesen werden, die das Zugangsverwaltungssystem verwendet, um den Zugang von Subjekten auf die Ressourcen zu steuern. [Üblicherweise geschieht dies durch vorherige Festlegung anerkannter Ressourcentypen mit zugehörigen Zugangsattributvorlagen. Wenn eine Ressource eines bekannten Typs erstellt wird, übernimmt sie die Zugangsattribute der jeweiligen Vorlage.]
- d) Eigentümer einer Ressource könnte entweder eine Person oder eine Organisation sein. Häufig, aber nicht immer ist der Ersteller der Ressource der Eigentümer, der Eigentümer kann sich während des Lebenszyklus der Ressource ändern.

5.1.2 Beziehung zwischen Identitätsverwaltungssystem und Zugangsverwaltungssystem

In dem hier beschriebenen Modell wird das Subjekt mithilfe eines Identitätsmanagementsystems (IMS) wie in ISO/IEC 24760-2 beschrieben authentisiert. Danach fragt das authentisierte Subjekt mithilfe des Zugangsverwaltungssystems (AMS) den Zugang an. Das Zugangsverwaltungssystem bestimmt, ob das Subjekt zum Zugriff auf die Ressource autorisiert wird oder nicht. Die Autorisierung des Subjekts umfasst zwei getrennte Handlungen:

- die vorherige Zuweisung von Rechten für den Zugang zur Ressource an die Subjekte und
- die Gewährung des Zugriffs auf Ressourcen durch Subjekte während der laufenden Nutzung.

Bild 2 zeigt die Beziehung zwischen einem Identitätsverwaltungssystem (IMS) und einem Zugangsverwaltungssystem (AMS).

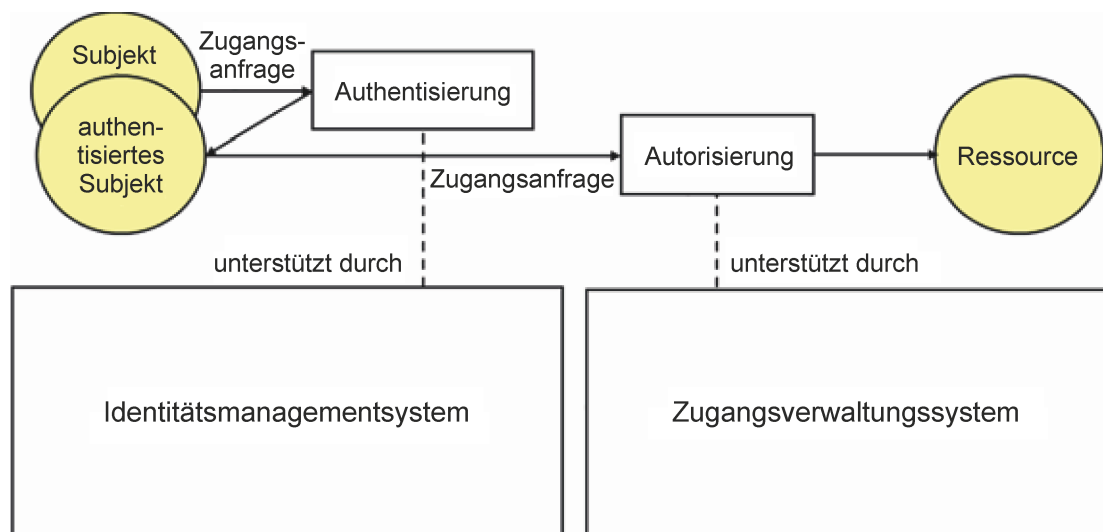


Bild 2 — Beziehung zwischen Identitätsverwaltungssystem und Zugangsverwaltungssystem

Die Authentisierung wird durch ein Identitätsmanagementsystem (IMS) unterstützt. Bei einem Zugangsverwaltungssystem, das eine identitätsbasierte Zugangssteuerung (IBAC) nutzt, ist die Identität die Grundlage für die Zuweisung von Rechten an Subjekte für den Zugang zur Ressource und für die Autorisierung von Anfragen zum Zugang zu Ressourcen durch Subjekte in der laufenden Nutzung.

ANMERKUNG Die Gewährung des Zugangs zu einer Ressource darf ein vorgegebenes Mindestniveau an Vertrauenswürdigkeit der Authentisierung des Subjekts erfordern, das vom Risikoprofil der Ressource abhängt. Das nötige Niveau hängt vom identitätsbezogenen Risiko für die Ressource ab, auf die zugegriffen werden soll. Weitere Informationen zur Vertrauenswürdigkeit der Authentisierung siehe ISO/IEC 29115.

Die Autorisierung wird vom Zugangsverwaltungssystem (AMS) vorgenommen, das die Zugangsinformationsverwaltung unterstützt.

Die Praxis der Implementation von Zugangsverwaltungssystemen darf je nach Architektur und dem verwendeten Zugangssteuerungsmodell variieren, zum Beispiel

- a) darf, wenn ein AMS als Webservicesystem implementiert ist, ein System den Zugriff auf eine Ressource anfragen, ohne zuvor authentisiert zu werden. In diesem Fall veranlasst das AMS das Subjekt dazu, die Authentisierung beim IMS anzufragen, und
- b) wenn ein ABAC-Modell verwendet wird, besteht die Möglichkeit, dass ein Subjekt keinerlei Authentisierung benötigt. In diesem Fall darf es anonymen Entitäten erlaubt werden, direkt an das AMS heranzutreten, und die Autorisierungsentscheidung wird auf Grundlage von Zugangsdaten getroffen, die validiert werden können, um nachzuweisen, dass das Subjekt über die geltend gemachten Attribute verfügt.

5.1.3 Sicherheitsmerkmale des Zugangsverfahrens

Die Sicherheitsaspekte der Implementation und der Prozesse von Zugangssteuerungssystemen sollten Beachtung finden, insbesondere wenn föderierte Architekturen verwendet werden.

Aus Sicherheitsgründen darf zunächst eine Validierung der Integrität der Zugangsanfrage erforderlich sein, bevor sie vom Zugangsverwaltungssystem weiterverarbeitet wird.

Wo Kommunikationskanälen vertraut werden kann, zum Beispiel bei privaten Verbindungen innerhalb einer Organisation, ist ein zusätzlicher Schutz möglicherweise nicht erforderlich. Wo Kommunikationskanäle jedoch über öffentliche Netzwerke oder andere ungeschützte Kanäle laufen, sollten Maßnahmen für den Schutz der Integrität und Vertraulichkeit von Zugangsdaten und zugehörigen Daten sowohl für die Zugangsanfrage

selbst (Rechte, Subjektauthentisierungsdaten, Ressource, angefragte Handlung usw.) als auch die während des Zugriffszeitraums an die Ressource gesendeten oder von der Ressource empfangenen Daten bereitgestellt werden.

Für die Etablierung eines sicheren Kommunikationskanals zwischen dem Subjekt und dem Zugangsverwaltungssystem gibt es zwei Konzepte. Die folgenden Konzepte berücksichtigen den Zeitpunkt, zu dem dieser sichere Kommunikationskanal etabliert wird:

- a) ein sicherer Kommunikationskanal darf vor der Übertragung der Rechte oder der für deren Erlangung verwendeten Daten etabliert werden (z. B. durch den Aufbau einer Transportschichtsicherheitssitzung (TLS-Sitzung) mit dem Server, der die Ressource unterstützt);
- b) ein sicherer Kommunikationskanal darf nach der erfolgreichen Übertragung der Rechte oder der für die Authentisierung eines Bezeichners des Subjekts verwendeten Daten etabliert werden.

Im letzteren Fall wird der sichere Kommunikationskanal entweder nach einem erfolgreichen Authentisierungsaustausch oder nach der erfolgreichen Annahme eines Zugangstokens etabliert; die Integritäts- und Vertraulichkeitsschlüssel werden aus dem Authentisierungsaustausch, von den im Zugangstoken enthaltenen Informationen oder von mit dem Zugangstoken verknüpften Informationen abgeleitet. Danach kann die Übertragung der für die Ressource angefragten Operation über diesen sicheren Kommunikationskanal erfolgen.

5.2 Beziehungen zwischen logischer und physischer Zugangssteuerung

Diese Internationale Norm konzentriert sich hauptsächlich auf die logische Zugangssteuerung. Die logische Zugangssteuerung wird durch die physische Zugangssteuerung unterstützt.

Der logische Zugriff auf eine Ressource in einem Unternehmenssystem sollte durch eine sichere physische Infrastruktur unterstützt werden, die einen Satz an wirksamen Kontrollen und Aktionen zur Verfügung stellt, die nicht korumpiert werden können.

Für den logischen Zugriff auf eine von einem ausgegliederten Dienst gehostete Ressource sollte diese für ihre physische und logische Zugangssteuerung rechenschaftspflichtig sein, um für das Subjekt vertrauenswürdig zu sein.

5.3 Funktionen und Prozesse des Zugangsverwaltungssystems

5.3.1 Überblick

Ein Zugangsverwaltungssystem (AMS) setzt eine Zugangssteuerungsrichtlinie durch und bietet zwei zentrale operative Funktionen:

- a) das Zuweisen von Ressourcenzugriffsrechten zu Subjekten im Vorgiff auf deren operative Nutzung; alternativ die Zuweisung von Zugangsrechten zu Attributen (wie im ABAC-Modell) und die nachfolgende Zuweisung von Attributen zu Subjekten, die die damit verknüpften Zugangsrechte übernehmen;
- b) die Nutzung dieser Rechte (ggf. zusammen mit anderen Informationen) für die Steuerung des Zugriffs auf Systemressourcen durch das Subjekt während der operativen Nutzung.

Zusätzlich bietet ein AMS administrative Funktionen für die Unterstützung dieser Kernfunktionen, zum Beispiel

- Richtlinienverwaltung,
- richtlinienbezogene Zugangsattributverwaltung und
- Verwaltung der Überwachung und Protokollierung.

Ressourcenzugangsrichtlinien sollten den folgenden Grundsätzen folgen:

- a) Zugangsattribute nach dem „Need-to-know-Prinzip“ festlegen;
- b) Datenzugriff minimieren, um den Zugang ausschließlich auf strikt benötigte Daten zu beschränken sowie Datenlecks und das Offenlegungsrisiko zu minimieren;
- c) sensible Daten trennen und schützen;
- d) pbD schützen;
- e) Multifaktorauthentisierung auf Basis der Kritikalität und Sensitivität der Ressource, auf die zugegriffen wird, verwenden.

5.3.2 Zugangssteuerungsrichtlinie

Ein Zugangsverwaltungssystem (AMS) setzt eine Zugangssteuerungsrichtlinie durch. Es gibt mehrere Zugangssteuerungsmodelle (siehe Anhang A). Diese Internationale Norm konzentriert sich auf die folgenden Modelle, die ausreichend flexibel für die Verwendung sowohl in zentralisierten als auch in verteilten Netzwerkumgebungen sind;

- identitätsbasierte Zugangssteuerung (IBAC);
- rollenbasierte Zugangssteuerung (RBAC);
- attributbasierte Zugangssteuerung (ABAC).

Die Zugangssteuerungsrichtlinie sollte in natürlicher Sprache oder einer anderen geeigneten Darstellungsweise, z. B. einer formalen Sprache, beschrieben werden, um die Ziele der Steuerung des Zugriffs auf Ressourcen, die Methoden und Prozesse für die Ausübung der Steuerung und alle Anforderungen für die Überwachung, das Auditing und andere nicht zentrale Funktionen auszudrücken.

Innerhalb einer Organisation darf es mehrere Zugangssteuerungsrichtlinien geben. Üblicherweise darf auf eine Gruppe von Ressourcen mit einer Technologie unter der Kontrolle eines Entscheidungspunkts zugegriffen werden, der auf eine Richtlinie reagiert, während der Zugriff auf eine andere Gruppe von Ressourcen, die mit einer anderen Technologie entwickelt wurde, unter einem anderen Entscheidungspunkt verwaltet wird, der auf eine zweite Zugangssteuerungsrichtlinie reagiert. Beide Entscheidungspunkte dürfen auch auf dieselbe Zugangssteuerungsrichtlinie reagieren, und dies wird empfohlen.

Wo mehrere Zugangssteuerungssysteme innerhalb einer Organisation operieren und in ein einziges System integriert werden sollen, sollten Unterschiede bei den Richtlinien beseitigt und eine gemeinsame Zugangssteuerungsrichtlinie entwickelt und dokumentiert werden. Ein alternatives Konzept könnte die Integration des Systems als eine organisationsinterne Föderation sein, wobei die in 5.3.8 beschriebenen Abwägungen und Anforderungen Geltung haben müssen.

Die Zugangssteuerung erfolgt durch Mechanismen für die Gewährung oder Verweigerung von an Ressourcen durchzuführenden Operationen auf Grundlage einer Zugangssteuerungsrichtlinie.

Autorisierungsentscheidungen werden auf Grundlage der Beurteilung von Subjektrechten und Attributen anhand von für die jeweilige Ressource vorgegebenen Zugangsregeln getroffen. Regeln können auch Umgebungsattribute umfassen, zum Beispiel die Uhrzeit und den Standort, von dem aus die Anfrage erfolgt. So können zum Beispiel Operationen an der Ressource zwischen 21.00 Uhr und 7.00 Uhr verhindert werden.

Bei einer systembestimmten Zugriffskontrolle gilt eine Regel notwendigerweise global für einen Satz von Ressourcen. So sollten zum Beispiel Subjekte für Operationen, die sie an einem gegebenen Satz von Ressourcen ausführen möchten, eine „Top-Secret-Freigabe“ haben.

ANMERKUNG Da mehrere Regeln nacheinander angewendet werden dürfen, könnte die Reihenfolge der Anwendung die Effizienz des Entscheidungsprozesses beeinträchtigen. Die optimale Rangordnung hängt jedoch von der relativen Wahrscheinlichkeit der Gewährung/Verweigerung des Zugriffs im operativen Betrieb ab.

Im Allgemeinen dürfen individuelle Regeln mithilfe einer mit jeder Ressource verknüpften Zugangssteuerungsmatrix implementiert werden, die einen oder mehrere Einträge enthält.

Jeder Eintrag gibt die Bedingung(en) an, die ein Subjekt erfüllen muss, um eine oder mehrere Operationen an der Ressource auszuführen. Die wichtigste zu erfüllende Bedingung ist, dass das Subjekt über ein bestimmtes oder mehrere bestimmte Rechte verfügen muss.

ABAC ist der allgemeinste Fall, bei dem die Zugangssteuerung auf per AMS definierten Attributen von Subjekten beruht. IBAC, PBAC und RBAC sind Sonderfälle von ABAC, bei denen die Attribute die Identität, die pseudonyme Identität bzw. die Rolle sind. Diese vier Modelle dürfen mithilfe von ACLs implementiert werden.

Wenn das Subjekt (im CBAC-Modell) zur Autorisierung ein Capability-Ticket präsentiert, muss überprüft werden, dass dieses als Zugangstoken für die betreffende Operation gültig ist.

Bei Zugangsverwaltungssystemen, die mehr als ein Zugangsmodell umfassen, sollte darauf geachtet werden, dass Richtlinien, die den Zugriff auf Ressourcen durch Subjekte spezifizieren, nicht über verschiedene Pfade zu konfligierenden Zugangsentscheidungen für dasselbe Subjekt führen. Ein Richtlinienverwaltungspunkt sollte in der Lage sein, verschiedene Modelle (PBAC, IBAC, RBAC, ABAC oder CBAC) zu verwalten.

Eine Zugangssteuerungsrichtlinie sollte:

- a) auf Richtlinienanforderungen basieren, die den erforderlichen verwendeten Modellen gemein sind, um Informationen zu schützen, geschäftliche Anforderungen zu erfüllen und um rechtlichen und behördlichen Vorschriften zu entsprechen und geistige Eigentumsrechte zu schützen;
- b) eine Richtlinienhierarchie beinhalten, die auf der allgemeinen Richtlinie basiert, aus der Zugangssteuerungsregeln für Einzelpersonen mit denselben Merkmalen abgeleitet werden dürfen;
- c) die Attribute für eine definierte Klassifizierung beschreiben. Diese Kategorisierung ermöglicht eine organisationsübergreifende Richtlinieninteroperabilität und Compliance;
- d) Verfahren für die Vergabe und Verwaltung von Rechten, den Zugangssteuerungsprozess und den Umgang mit Ausnahmen beschreiben.

5.3.3 Rechteverwaltung

Die Anforderungen an die Rechteverwaltung werden durch die in 5.3.2 erwähnte Zugangssteuerungsrichtlinie definiert.

Bei einer identitätsbasierten Zugangssteuerungsrichtlinie wird die Rechteverwaltung auf Grundlage der Subjektidentität durchgeführt. IBAC-Richtlinien setzen Mechanismen wie Zugriffskontrolllisten (ACL, en: access control lists) ein, um die Identitäten, denen der Zugriff auf eine Ressource gewährt wird, und die Arten von Operationen, die sie an der Ressource ausführen dürfen, zu spezifizieren. Im IBAC-Modell erfolgt die Gewährung der Rechte für den Zugang auf eine Ressource an ein Subjekt, bevor der/den relevante(n) ACL(s) der Ressource die Zugangsanfrage des Subjekts sowie seine Identität und Zugangsrechte hinzugefügt werden.

Wenn die Identität eines authentisierten Subjekts mit einer in der relevanten ACL eingetragenen Identität übereinstimmt, wird in Übereinstimmung mit seinen Zugangsrechten der Zugriff auf die Ressource gewährt. Jede Ressource hat eine zugehörige ACL, in der die Zugangsrechte für die zum Zugriff auf die Ressource autorisierten Subjekte eingetragen sind. Im IBAC-Modell werden die Autorisierungsentscheidungen getroffen, bevor der/den relevante(n) ACL(s) der Ressource die Zugangsanfrage des Subjekts, die Entscheidung darüber und die Zugangsrechte des Subjekts hinzugefügt werden.

Bei rollenbasierter Zugangssteuerung (RBAC) wird (oder werden) jedem Subjekt eine (oder mehrere) Rollen zugewiesen, die im Konto für das Subjekt eingetragen werden. Autorisierungsentscheidungen werden auf Grundlage der der jeweiligen Rolle innerhalb des Zugangsverwaltungssystems (AMS) zugewiesenen Zugangsrechte getroffen. In einem RBAC-Modell werden die Rechte nicht Subjekten zugewiesen, sondern Rollen. Eine separate Aktivität weist den Subjekten Rollen zu. Dies beeinflusst bei Anfragen auf Ressourcen, was in einem RBAC-Modell ein zweistufiger Prozess ist, auch den Autorisierungsprozess:

- Autorisierung der Zugangsanfrage für die Rolle;
- Authentisierung des Subjekts als Mitglied einer Rollengruppe.

Bei attributbasierter Zugangssteuerung (ABAC) werden Subjekten richtlinienbezogene Zugangsattribute zugewiesen. Autorisierungsentscheidungen basieren auf den Attributen der Subjekte.

Ein Subjekt darf als Mitglied einer Gruppe, als Inhaber von Attributen oder als Einzelperson auf Ressourcen zugreifen, und rollenbasierte, attributbasierte und identitätsbasierte Zugangssteuerungsschemata können gleichzeitig in einem Zugangssteuerungssystem existieren.

Die Rechteverwaltung umfasst die folgenden Aktivitäten:

- a) die Erstellung eines Satzes von Rechten für die Bezeichnung und Begrenzung der Typen von Operationen, die an Ressourcen vorgenommen werden dürfen;
- b) die Etablierung von Regeln, die die Zuweisung von Rechten in Übereinstimmung mit der Zugangssteuerungsrichtlinie und dem verwendeten Zugangssteuerungsmodell spezifizieren, z. B. die Zuweisung von Identitäten, Rollen, Fähigkeiten oder sonstigen festgelegten Attributen;
- c) die Aktualisierung und der Widerruf von Rechten und Identitätsattributen.

Die Implementation einer Zugangssteuerungsrichtlinie resultiert aus der Zuweisung von Ressourcenzugriffsrechten an Subjekte, Rollen, Gruppen usw. Rechte sollten auf Grundlage des „Need-to-know-Prinzips“ zugewiesen werden und das geringste Recht gewähren, mit dem das Subjekt die relevante Aktivität ausführen kann.

ANMERKUNG Rechte dürfen sowohl menschlichen als auch nicht-menschlichen Subjekten zugewiesen werden. So dürfen zum Beispiel einem Gerät oder Dienst Ressourcenzugriffsrechte zugewiesen werden, wenn sie einem Netzwerk hinzugefügt werden.

5.3.4 Verwaltung richtlinienbezogener Attributinformationen

Die Verwaltung von Informationen für das Festlegen von Rechten anhand von Attributen ist eine administrative Tätigkeit wie in Bild 5 dargestellt.

Informationen dieser Art werden:

- a) aus verschiedenen Quellen beschafft, darunter Attributautoritäten, Ressourcen und die Umgebung,
- b) vom Richtlinienverwaltungspunkt (PAP) verwaltet und
- c) im Richtlinieninformationspunkt (PIP) gespeichert.

Die resultierenden Informationen werden dem Richtlinienentscheidungspunkt (PDP) zur Verfügung gestellt, um den Zugang zu Ressourcen zu steuern.

Attributinformationen werden innerhalb eines AMS in Übereinstimmung mit der zuvor beschriebenen Zugangssteuerungsrichtlinie verwaltet.

Im Falle eines ABAC-Modells wird die Richtlinie anhand der Attribute formuliert, die verwendet werden, um den Zugriff auf die Ressource zu regeln, und anhand der Art und Weise, wie die Attribute den Ressourcenzugriffsrechten zugeordnet werden. In einem RBAC-Modell legt die Richtlinie fest, wie die Ressourcenzugriffsrechte den verschiedenen Rollen zugeordnet werden.

Bei einer DAC-Richtlinie werden die Attribute von den Eigentümern der Ressource verwaltet, während bei einer MAC-Richtlinie zusätzliche Attribute von Richtlinienbeauftragten verwaltet werden.

Das PBAC-Modell setzt Mechanismen wie Zugriffskontrolllisten (ACL) ein, die die Pseudonyme der Subjekte, denen der Zugriff auf eine Ressource gewährt wird, zusammen mit den Zugriffsrechten der Subjekte für die Ressource enthalten. Wenn ein Subjekt ein Pseudonym präsentiert, das mit einem in der ACL gespeicherten übereinstimmt, darf dem Subjekt das Recht gewährt werden, die Operation an der Ressource vorzunehmen, sofern es über eine ausreichende Erlaubnis verfügt und weitere ggf. geltende Überprüfungen besteht.

Das IBAC-Modell verwendet einen ähnlichen Mechanismus, bei dem Identitäten statt Pseudonyme verwendet werden.

Das RBAC-Modell verwendet einen ähnlichen Mechanismus, bei dem Rollen statt Pseudonyme verwendet werden.

Das ABAC-Modell verwendet einen ähnlichen Mechanismus, bei dem Attribute (z. B. Gruppenmitgliedschaften) statt Pseudonyme verwendet werden.

PBAC-, IBAC-, RBAC- und ABAC-Modell dürfen gleichzeitig innerhalb eines Zugangssteuerungssystems existieren.

Das CBAC-Modell setzt Mechanismen ein, bei denen die vom Subjekt präsentierte Fähigkeit zunächst mit dem Bezeichner der Ressource und mit der an der Ressource vorzunehmenden Operation übereinstimmen muss. Ferner muss der Inhalt der Fähigkeit auch mit dem Bezeichner einer anerkannten Stelle und mit den zugehörigen, für diese Stelle gewährten Operationen übereinstimmen. Wenn dies der Fall ist, darf dem Subjekt vorbehaltlich etwaiger weiterer Prüfungen das Recht gewährt werden, die Operation an der Ressource auszuführen.

Anhang A enthält weitere Informationen über Modelle.

5.3.5 Autorisierung

5.3.5.1 Basisautorisierung

Die Autorisierung erfolgt während der operativen Phase und wird durch den Richtlinienentscheidungspunkt (PDP) in Übereinstimmung mit der Zugangssteuerungsrichtlinie vermittelt. Diese Aktivität wird durch administrative Handlungen unterstützt.

5.3.5.2 Autorisierung des Zugriffs durch Delegierte

Unter festgelegten Bedingungen darf die Autorisierung einem Delegierten eines Subjekts erteilt werden. Ein Delegierter könnte eine Person, ein Webserver oder eine datenverwendende Anwendung unter Kontrolle des Subjekts sein. Ein Delegierter übernimmt typischerweise die Zugangsrechte des Subjekts und muss auf dieselbe oder eine äquivalente Weise authentisiert werden wie das Subjekt. Das Delegiertenszenario ist in Bild 3 dargestellt.

ANMERKUNG Dies ist ein von der OAuth-Technologie unterstützter Anwendungsfall. Die Autorisierungsentscheidung wird vom Eigentümer der Ressource in Echtzeit oder über eine zuvor von ihm festgelegte Richtlinie getroffen. Wenn das Subjekt bereits ein Delegierter ist, kann das AMS die Autorisierungsentscheidung anhand der Zugangsdaten treffen, die der Delegierte bereits besitzt. Wenn das Subjekt nicht bereits ein Delegierter ist, muss der Eigentümer der Ressource kontaktiert und gefragt werden, ob der nicht autorisierten Person der Zugriff auf die Ressource erlaubt wird.

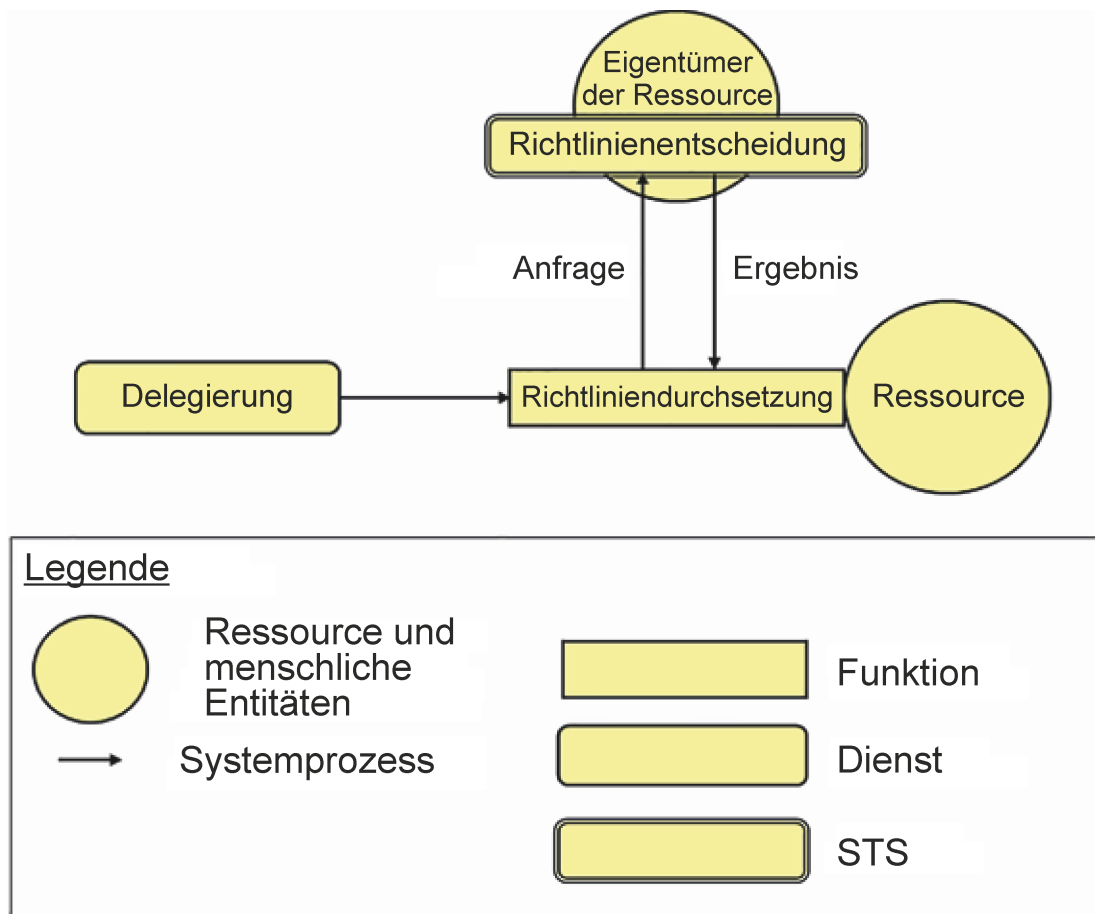


Bild 3 — Autorisierung des Zugriffs durch Delegierte

5.3.6 Überwachungsmanagement

Aktivitäten im Zusammenhang mit der Zugangsverwaltung sollten zu Zwecken der Compliance, der Regulierung und der Untersuchung überwacht werden.

Das Zugangsverwaltungssystem (AMS) sollte nachverfolgbare Überwachungs- und Protokollierungsfähigkeiten zum Zwecke der regulatorischen Compliance, Haftung und Untersuchung bieten.

Ein AMS sollte Fähigkeiten zur Überwachung der von Subjekten versuchten Operationen an den Ressourcen sowie der Gewährung oder Verweigerung dieser Operationen bieten.

Die folgenden Parameter sollten in einer Zugriffsprotokollierung aufgezeichnet werden:

- ein Bezeichner der Ressource;
- die Operation, die das Subjekt an der Ressource ausführen wollte;
- die Entscheidung (d. h. Gewährung oder Verweigerung) unter Angabe eines Grundes;
- der Zeitpunkt der Gewährung bzw. Verweigerung des Zugangs;
- die Rechte bzw. Attribute des Subjekts;
- alle Informationen, die das Subjekt direkt oder indirekt identifizieren können.

Darüber hinaus sollte das AMS Tools für die einfache Erstellung von Auditberichten mithilfe von auf den letzten sechs in der Zugriffsprotokollierung zu findenden Parametern basierenden Filtern bereitstellen.

Der Eigentümer einer Ressource muss die Zugangskriterien angeben, die vom Richtlinienentscheidungspunkt für die Entscheidung, ob einem Subjekt der Zugriff auf die Ressource gewährt wird, verwendet werden.

5.3.7 Alarmverwaltung

Üblicherweise besteht der Zweck von Alarmen darin, Zugangsverwaltungsauditoren auf ungewöhnliche Betriebsbedingungen aufmerksam zu machen. Solche Situationen sollten zusammen mit den Handhabungsverfahren und den beim Überwachungsmanagement implementierten Handhabungsverfahren in der Zugangssteuerungsrichtlinie definiert werden. Ungewöhnliche Situationen könnten zum Beispiel Versuche von nicht autorisierten Subjekten sein, auf die Ressource zuzugreifen.

Alarmbedingungen werden definiert, damit sie im operativen Gebrauch erkannt werden und geeignete Maßnahmen ergriffen werden können. Wenn Alarmbedingungen eintreten, sollten sie für eine spätere Analyse in einer Zugriffsprotokollierung aufgezeichnet werden.

Alarme dürfen von einzelnen oder mehrfachen Bedingungen ausgelöst werden, die sich auf die folgenden Punkte beziehen können:

- a) einen Bezeichner der Ressource;
- b) die Operation, die das Subjekt an der Ressource ausführen wollte;
- c) die Entscheidung (d. h. Gewährung oder Verweigerung) unter Angabe eines Grundes;
- d) den Zeitpunkt der Gewährung bzw. Verweigerung des Zugangs;
- e) Rechte bzw. Attribute;
- f) alle Informationen, die das Subjekt direkt oder indirekt identifizieren können.

Sobald ein Alarm ausgelöst wurde, können weitere Untersuchungen mithilfe der für die Überwachung der Ereignisse erstellten Zugriffsprotokollierung durchgeführt werden.

5.3.8 Föderierte Zugangssteuerung

Ein föderiertes Identitäts- und Zugangsmanagement wird benötigt, wenn ein authentisiertes Subjekt einer Organisation den Zugriff auf eine Ressource in einer anderen Organisation anfragt. Für das föderierte Identitätsmanagement gibt es mehrere Modelle, die in ISO/IEC 24760 beschrieben sind. Bild 4 zeigt ein Beispiel für ein föderiertes Zugangssteuerungssystem. Vorausgesetzt, ein Subjekt kann sich in einem Föderationsmodell authentisieren, werden die Anforderungen der föderierten Zugangssteuerung durch die Mitglieder der Föderation in Übereinstimmung mit einer Beziehung geteilter Vertrauenswürdigkeit und gemeinsamen, von den an der Gemeinschaft teilhabenden Organisation vereinbarten Richtlinien implementiert.

- a) Das zu authentisierende Subjekt der Autoritätsquelle der Organisation, der es angehört.
- b) Die Organisation des Subjekts sichert der Organisation des Eigentümers der Ressource die Zugangssteuerung zu. Die Organisation des Eigentümers der Ressource bestätigt, dass die Authentisierung des Subjekts gültig ist und stellt den Authentisierungskontext und die vereinbarten Zugangsattribute einschließlich der ABAC- oder RBAC-Rechte bereit.
- c) Die Organisation des Eigentümers der Datenressource akzeptiert die Zusicherung und untersucht die Attribute im Hinblick auf die Zugangssteuerungsrichtlinien des Eigentümers der Datenressource.
- d) Der Eigentümer der Datenressource autorisiert das Subjekt zum Zugriff auf die Ressource oder verweigert den Zugriff und benachrichtigt das Subjekt.

e) Alle Autoritäten zeichnen Zugangssteuerungsereignisse auf.

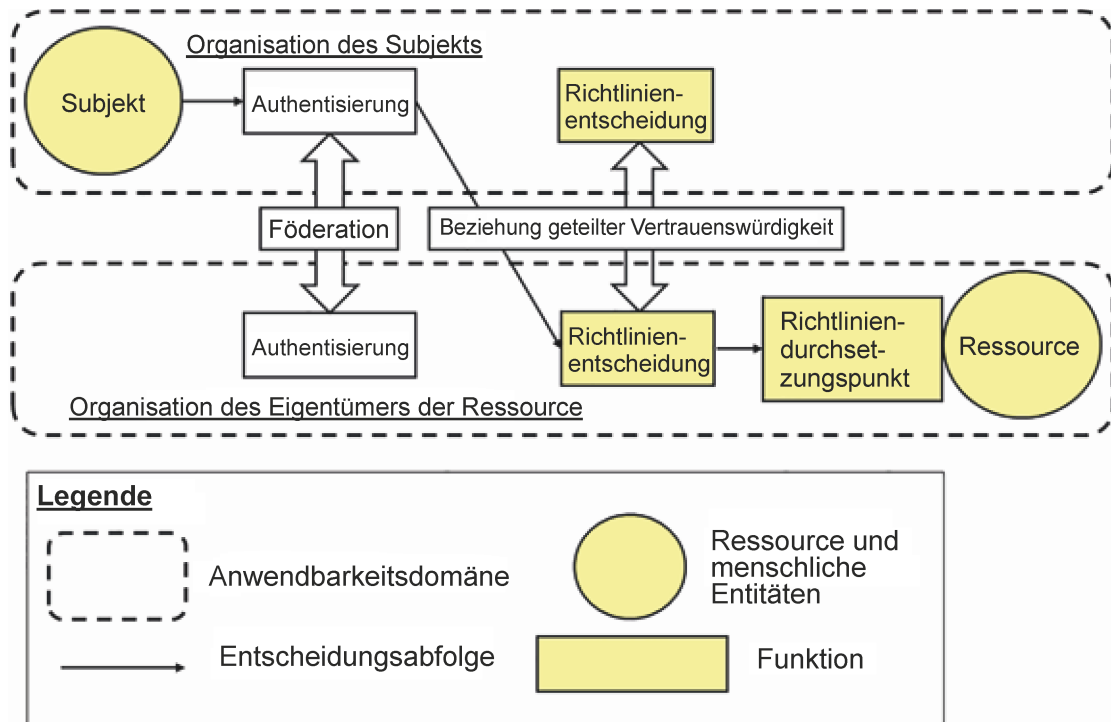


Bild 4 — Föderierte Zugangssteuerung

Eine Beziehung geteilter Vertrauenswürdigkeit für die Zugangssteuerung innerhalb einer Föderation sollte:

- a) auf vereinbarten Föderationsanforderungen für den Schutz von Informationen basieren, um rechtlichen und behördlichen Anforderungen zu genügen sowie geistiges Eigentum zu schützen,
- b) gemeinsame Richtlinienelemente enthalten, anhand derer Zugangssteuerungsregeln und die Implementationskategorisierung abgeleitet werden können und
- c) Zugangsdaten für die Zugangssteuerung (Attribute, Berechtigungen usw.) definieren, die innerhalb einer Föderation verwendet werden können, um die Etablierung von Vertrauensbeziehungen zwischen den Mitgliedern der Föderation zu erleichtern.

6 Referenzarchitektur

6.1 Überblick

Die in Abschnitt 5 vorgestellten Komponenten etablieren eine Referenzarchitektur für ein AMS.

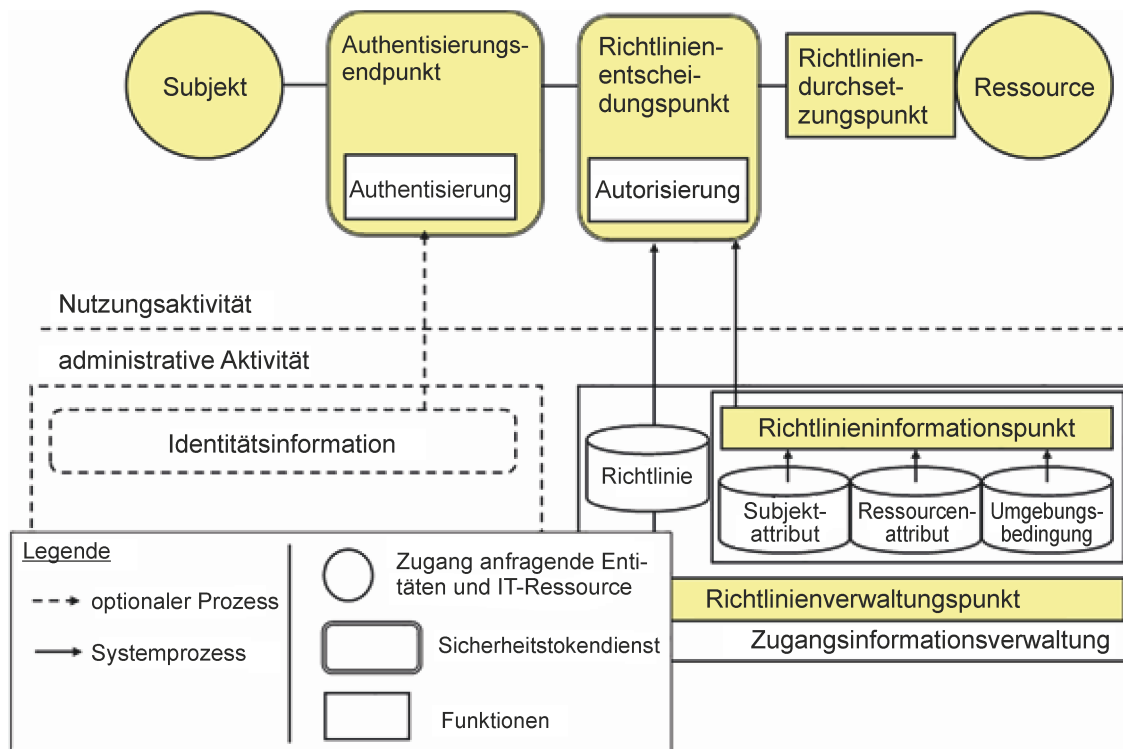


Bild 5 — AMS-Referenzarchitektur

6.2 Grundlegende Komponenten eines Zugangsverwaltungssystems

6.2.1 Authentisierungsendpunkt

Der Authentisierungsendpunkt stellt die Subjektauthentifizierung bereit, die der Richtlinienentscheidungspunkt bei der Entscheidung über den Zugriff auf Ressourcen durch Subjekte verwendet.

6.2.2 Richtlinienentscheidungspunkt (PDP)

Der Richtlinienentscheidungspunkt trifft die Autorisierungsentscheidungen über die Gewährung oder Verweigerung des Zugriffs auf eine Ressource und übermittelt die Entscheidungen zur Umsetzung an den PEP.

Der PDP implementiert die Zugangssteuerungsrichtlinie oder die für die Ressource festgelegte Richtlinie. Der PDP entscheidet auf Grundlage eines festgelegten Satzes an Richtlinien, ob das Subjekt auf die Ressource zugreifen darf.

In einigen Fällen wird die Richtlinie in Echtzeit über eine Schnittstelle zum Eigentümer der Ressource erstellt. In unternehmenszentrierten Implementierungen der Zugangssteuerung wird dieser Dienst häufig als „user authorization endpoint“ („Benutzerautorisierungsendpunkt“) bezeichnet.

Der PDP wird vom Richtlinieninformationspunkt (PIP) unterstützt.

6.2.3 Richtlinieninformationspunkt (PIP)

Diese Komponente agiert als Quelle für Attributwerte (z. B. Ressource, Subjekt, Umgebungsbedingung), die vom PDP benutzt werden, um die Autorisierungsentscheidung zu treffen.

6.2.4 Richtlinienverwaltungspunkt (PAP)

Diese Komponente stellt die Schnittstelle für die Verwaltung des Richtlinienatzes und der zugehörigen Informationen am PIP zur Verfügung. Ihre Verwaltung darf die Konfiguration, das Testen, das Debugging und das Speichern umfassen. Für die Verwaltung eines Zugangssteuerungsrichtlinienatzes wird eine anwendungsprogrammierbare Schnittstelle zum PAP benötigt.

Die Richtlinie oder der Richtlinienatz dürfen auf rollenbasierter Zugangssteuerung (RBAC), attributbasierter Zugangssteuerung (ABAC) oder einem beliebigen anderen Modell oder einer Kombination von Modellen beruhen.

Richtlinien in natürlicher Sprache sollten in äquivalente digitale Repräsentationen übersetzt werden, die der PDP verwendet, um seine Autorisierungsentscheidungen zu treffen.

6.2.5 Richtliniendurchsetzungspunkt (PEP)

Der Richtliniendurchsetzungspunkt (PEP) gewährt autorisierten Zugriff auf Ressourcen und schützt eine Ressource vor nicht autorisiertem Zugriff.

Der PEP fängt die Anfrage des Subjekts zum Zugriff auf die Ressource ab und leitet sie zur Autorisierungsentscheidung um, die vom Richtlinienentscheidungspunkt (PDP) getroffen wird.

6.3 Zusätzliche Dienstekomponenten

6.3.1 Allgemein

Bei der Implementation der logischen Ansicht dürfen verschiedene Dienste zusätzlich eingeführt werden.

6.3.2 Subjektzentrierte Implementation

6.3.2.1 Überblick

Bild 6 zeigt den Fall, in dem das Subjekt eine entscheidende Rolle spielt.