DIN EN ISO/IEC 29146

DIN

ICS 35.030

Informationstechnologie – Sicherheitstechniken – Ein Rahmenwerk für die Zugangsverwaltung (ISO/IEC 29146:2016 einschließlich Änderung 1:2022); Deutsche Fassung EN ISO/IEC 29146:2023

Information technology –
Security techniques –
A framework for access management (ISO/IEC 29146:2016 including Amendment 1:2022);
German version EN ISO/IEC 29146:2023

Technologies de l'information –
Techniques de sécurité –
Cadre pour la gestion de l'accès (ISO/IEC 29146:2016 compris Amendement 1:2022);
Version allemande EN ISO/IEC 29146:2023

Gesamtumfang 48 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: DIN EN ISO/IEC 29146:2023-12

Nationales Vorwort

Der Text von ISO/IEC 29146:2016 einschließlich Änderung 1:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 29146:2023 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 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

ISO/IEC 24760-1:2019	siehe	DIN EN ISO/IEC 24760-1:2023-03
ISO/IEC 24760-2:2015	siehe	DIN EN ISO/IEC 24760-2:2023-03
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.

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

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 24760-1:2023-03, *IT-Sicherheit und Datenschutz — Rahmenwerk für Identitätsmanagement — Teil 1: Terminologie und Konzept (ISO/IEC 24760-1:2019); Deutsche Fassung EN ISO/IEC 24760-1:2022*

DIN EN ISO/IEC 24760-2:2023-03, *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*

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 29146:2023-12

– Leerseite –

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 29146:2023-12

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 29146

April 2023

ICS 35.030

Deutsche Fassung

Informationstechnologie — Sicherheitstechniken — Ein Rahmen für die Zugangsverwaltung (ISO/IEC 29146:2016 einschließlich Änderung 1:2022)

Information technology — Security techniques — A framework for access management (ISO/IEC 29146:2016 including Amdendment 1:2022)

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'accès (ISO/IEC 29146:2016 compris Amendement 1:2022)

Diese Europäische Norm wurde vom CEN am 24. März 2023 angenommen.

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

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 29146:2023-12

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 Richtliniendurchsetzungspunkt (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 Zugangsverwaltungsrahmenwerks 31
8.3.3 Validierung des Zugangsverwaltungssystems 34
8.3.4 Validierung der Pflege eines implementierten AMS 38
Anhang A (informativ) Übliche Zugangssteuerungsmodelle 41

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12

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 Identifikatorbasierte Zugangssteuerung (IBAC) 42
A.2.5 Rollenbasierte Zugangssteuerung (RBAC) 42
A.2.6 Attributbasierte Zugangssteuerung (ABAC) 43
A.2.7 Pseudonymbasierte Zugangssteuerung (PBAC) 43
Literaturhinweise 44

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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 29146:2023-12

Europäisches Vorwort

Der Text von ISO/IEC 29146:2016 einschließlich Amd1:2022 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 EN ISO/IEC 29146:2023 übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Oktober 2023, und etwaige entgegenstehende nationale Normen müssen bis Oktober 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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.

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

Anerkennungsnotiz

Der Text von ISO/IEC 29146:2016, einschließlich Änderung 1:2022, wurde von CEN-CENELEC als EN ISO/IEC 29146:2023 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12

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\protect\relax\protect\kern+.1667em\relax--Supplementaryinformation.

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12

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 nichtmenschliche 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 Rahmenwerk 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).

Das Rahmenwerk für die Zugangsverwaltung ist ein Teil eines allgemeinen Identitäts- und Zugangsverwaltungsrahmenwerks. Der andere Teil ist das Rahmenwerk 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12

1 Anwendungsbereich

Diese Internationale Norm legt ein Rahmenwerk 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 24760-1:2019, *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)

AVA Documents Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12

3.3
Zugangstoken
vertrauenswürdiges 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 Daten*ressourcen* (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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12

Anmerkung 2 zum Begriff: Das Need-to-have-Prinzip ist die Sicherheitszielsetzung, dass die Ausführung bestimmter Aufgaben durch den Anfragesteller 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 Löschungsrechte 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 29146:2023-12

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, signiert, austauscht und ausgibt

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

3.17
subjektzentrierte Implementation
Zugangsverwaltung (3.2), die als Komponentendienste implementiert ist, die von einem *Subjekt* (3.15) aufgerufen werden zur Erlangung der vom *Richtliniendurchsetzungspunkt* (3.11) für den Zugriff auf eine *Ressource* (3.14) anerkannten Mittel

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.

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12

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:

a) 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.

b) 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.

c) 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 29146:2023-12