

	DIN EN IEC 62351-8 (VDE 0112-351-8)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
<p>ICS 33.200; 35.030</p> <p>Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 8: Rollenbasierte Zugriffskontrolle für Energiemanagementsysteme (IEC 62351-8:2020); Deutsche Fassung EN IEC 62351-8:2020</p> <p>Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management (IEC 62351-8:2020); German version EN IEC 62351-8:2020</p> <p>Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 8: Contrôle d'accès basé sur les rôles pour la gestion de systèmes de puissance (IEC 62351-8:2020); Version allemande EN IEC 62351-8:2020</p> <p>Gesamtumfang 84 Seiten</p> <p>DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE</p>		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2020-06-02 angenommene Europäische Norm als DIN-Norm ist 2021-07-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN IEC 62351-8 (VDE 0112-351-8):2020-01.

Für dieses Dokument ist das nationale Arbeitsgremium K 952 „Netzleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

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

Die enthaltene IEC-Publikation wurde vom IEC/TC 57 „Power systems management and associated information exchange“ erarbeitet und unterliegt dem Copyright der IEC .

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Dieses Dokument enthält Code-Elemente, d. h. Elemente, die für die direkte Verarbeitung durch einen Computer vorgesehen sind. Dieser Inhalt ist jeder Text zwischen den Markierern <CODE BEGINS> und <CODE ENDS> oder jeder Inhalt, der in dieser Norm eindeutig als Code-Element gekennzeichnet ist.

Mit dem Erwerb dieses Dokuments ist eine Urheberrechtslizenz verbunden, die es dem Käufer erlaubt, Software, die Code-Elemente aus diesem Dokument enthält, direkt an den Endnutzer oder über Vertriebs Händler an Endnutzer zu verkaufen und vorbehaltlich der IEC-Softwarelizenzbedingungen, die verfügbar sind unter: <http://www.iec.ch/CCv1>.

Im Fall von Abweichungen zwischen dem Dokument und den Code-Elementen gelten die Code-Elemente.

In diesem Dokument werden die folgenden Schriftarten verwendet:

Codierung in ASN.1 oder XACML: `couriernew`

Das Original-Dokument enthält Bilder und Schrift in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 60870-5-104 + A1	IEC 60870-5-104 + A1	DIN EN 60870-5-104	–
EN IEC 61784 (alle Teile)	IEC 61784 (alle Teile)	DIN (EN)IEC 61784 (alle Teile)	(VDE 0803-500)
EN 61850-7-2	IEC 61850-7-2	DIN EN 61850-7-2	–
EN 61850-8-1	IEC 61850-8-1	DIN EN 61850-8-1	–
EN IEC 61850-8-2	IEC 61850-8-2	DIN EN IEC 61850-8-2 (VDE 0160-850-8-2)	VDE 0160-850-8-2
–	IEC TR 61850-90-19 ^a	–	–
EN 61968 (alle Teile)	IEC 61968 (alle Teile)	DIN EN 61968 (alle Teile)	–
EN (IEC) 61970 (alle Teile)	IEC 61970 (alle Teile)	DIN EN (IEC) 61970 (alle Teile)	–
–	IEC TS 62351-1	–	–
–	IEC TS 62351-2	–	–
EN 62351-3:2014 + A2:2020	IEC 62351-3:2014 + A2:2020	DIN EN 62351-3 (VDE 0112-351-3):2019-06 + A2 ^a	VDE 0112-351-3
EN IEC 62351-4:2018 + A1 ^a	IEC 62351-4:2018 + A1:2020	DIN EN IEC 62351-4 (VDE 0112-351-4):2020-04 + A1 ^a	VDE 0112-351-4
–	IEC TS 62351-5	–	–
EN 62351-7:2017	IEC 62351-7:2017	DIN EN 62351-7 (VDE 0112-351-7):2019-09	VDE 0112-351-7
–	IEC TS 62351-8:2011	–	–
EN 62351-9	IEC 62351-9	DIN EN 62351-9 (VDE 0112-351-9)	VDE 0112-351-9
EN IEC 62351-14 ^a	IEC 62351-14 ^a	DIN EN IEC 62351-14 (VDE 0112-351-14) ^a	VDE 0112-351-14 ^a

DIN EN IEC 62351-8 (VDE 0112-351-8):2021-07

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
–	IEC TR 62351-90-1	–	–
EN IEC 62443 (alle Teile)	IEC 62443 (alle Teile)	DIN EN IEC 62443 (VDE 0802) (alle Teile)	VDE 0802
–	IEC/ISO 9798-2	–	–
–	IEEE 802.1X-2010	–	–
–	IEEE 1686	–	–
–	IEEE P1689	–	–
–	ISO 9506-1	–	–
–	ISO 9506-2	–	–
–	ISO/IEC 8802-3 <i>ersetzt durch:</i> ISO/IEC/IEEE 8802-3	–	–
–	ISO/IEC 9594-8:2017	–	–
–	ANSI INCITS 359-2004	–	–
–	ANSI X.9.69-2006	–	–
–	ANSI X.9.73-2002	–	–
–	NIST SP 800-82r2	–	–
–	PKCS#10	–	–
–	PKCS#12	–	–
–	RFC 1035	–	–
–	RFC 2798	–	–
–	RFC 2865	–	–
–	RFC 2904	–	–
–	RFC 2905	–	–
–	RFC 4513	–	–
–	RFC 4524	–	–
–	RFC 5246	–	–
–	RFC 5280	–	–
–	RFC 5288	–	–
–	RFC 5289	–	–
–	RFC 5755	–	–
–	RFC 5878	–	–
–	RFC 6614	–	–
–	RFC 6749	–	–
–	RFC 7519	–	–
–	XACML	–	–
–	XACML-RBAC	–	–
^a In Vorbereitung.			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60870-5-104, *Fernwirkleinrichtungen und -systeme – Teil 5-104: Übertragungsprotokolle – Zugriff für IEC 60870-5-101 auf Netze mit genormten Transportprofilen*

DIN EN 61850-7-2, *Kommunikationsnetze und -systeme für die Automatisierung in der elektrischen Energieversorgung – Teil 7-2: Grundlegende Informations- und Kommunikationsstruktur – Abstrakte Schnittstelle für Kommunikationsdienste (ACSI)*

DIN EN 61850-8-1, *Kommunikationsnetze und -systeme für die Automatisierung der elektrischen Energieversorgung – Teil 8-1: Spezifische Abbildung von Kommunikationsdiensten (SCSM) – Abbildungen auf MMS (nach ISO 9506-1 und ISO 9506-2) und ISO/IEC 8802-3*

DIN EN 61968 (alle Teile), *Integration von Anwendungen in Anlagen der Elektrizitätsversorgung – System-schnittstellen für Netzführung*

DIN EN 62351-3 (VDE 0112-351-3):2019-06, *Management von Systemen der Energietechnik und zugehöriger Datenaustausch – Daten- und Kommunikationssicherheit – Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich TCP/IP (IEC 62351-3:2014 + A1:2018); Deutsche Fassung EN 62351-3:2014 + A1:2018*

DIN EN 62351-3/A2 (VDE 0112-351-3/A2)^a, *Management von Systemen der Energietechnik und zugehöriger Datenaustausch – Daten- und Kommunikationssicherheit – Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich TCP/IP (IEC 57/2149/FDIS:2019); Deutsche und Englische Fassung EN 62351-3:2014/FprA2:2019*

DIN EN 62351-7 (VDE 0112-351-7):2019-09, *Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen – Daten- und Kommunikationssicherheit – Teil 7: Datenobjektmodelle für Netzwerk- und Systemmanagement (NSM) (IEC 62351-7:2017); Deutsche Fassung EN 62351-7:2017*

DIN EN 62351-9 (VDE 0112-351-9), *Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 9: Cybersicherheit Schlüsselmanagement für Stromversorgungsanlagen*

DIN EN IEC 61784 (alle Teile), *Industrielle Kommunikationsnetze – Profile*

DIN EN IEC 61850-8-2 (VDE 0160-850-8-2), *Kommunikationsnetze und -systeme für die Automatisierung der elektrischen Energieversorgung – Teil 8-2: Spezifische Abbildung von Kommunikationsdiensten (SCSM) – Abbildungen auf erweiterbares Messaging Presence Protocol (XMPP)*

DIN EN (IEC) 61970 (alle Teile), *Schnittstelle für Anwendungsprogramme für Energiemanagementsysteme (EMS-API)*

DIN EN IEC 62351-4 (VDE 0112-351-4):2020-04, *Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 4: Profile einschließlich MMS und Ableitungen (IEC 62351-4:2018); Deutsche Fassung EN IEC 62351-4:2018*

DIN EN IEC 62351-4/A1 (VDE 0112-351-4/A1)^a, *Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 4: Profile einschließlich MMS und Ableitungen (IEC 57/2116/CDV:2019); Deutsche und Englische Fassung EN IEC 62351-4:2018/prA1:2019*

DIN EN IEC 62351-14 (VDE 0112-351-14)^a, *Energiemanagementsysteme und zugehöriger Datenaustausch – Daten- und Kommunikationssicherheit – Teil 14: Protokollierung von IT-Sicherheitsvorfällen*

DIN EN IEC 62351-8 (VDE 0112-351-8):2021-07

DIN EN IEC 62443 (VDE 0802) (alle Teile), *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme*

DIN EN IEC 62443 (VDE 0802) (alle Teile), *IT-Sicherheit für industrielle Automatisierungssysteme*

Energiemanagementsysteme und zugehöriger Datenaustausch –
IT-Sicherheit für Daten und Kommunikation –
Teil 8: Rollenbasierte Zugriffskontrolle für Energiemanagementsysteme
(IEC 62351-8:2020)

Power systems management and associated
information exchange –
Data and communications security –
Part 8: Role-based access control for power
system management
(IEC 62351-8:2020)

Gestion des systèmes de puissance et
échanges d'informations associés –
Sécurité des communications et des données –
Partie 8: Contrôle d'accès basé sur les rôles
pour la gestion de systèmes de puissance
(IEC 62351-8:2020)

Diese Europäische Norm wurde von CENELEC am 2020-06-02 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen definiert 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 Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees 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.



Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

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

© 2020 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN IEC 62351-8:2020 D

Europäisches Vorwort

Der Text des Dokuments 57/2180/FDIS, zukünftige 1. Ausgabe der IEC 62351-8, erarbeitet vom IEC/TC 57 „Power systems management and associated information exchange“ wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN IEC 62351-8:2020 angenommen.

Nachstehende Daten wurden definiert:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2021-03-02
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2023-06-02

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

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62351-8:2020 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 60870-5-104	ANMERKUNG	Harmonisiert als EN 60870-5-104.
IEC 61784 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN IEC 61784.
IEC 61850-8-1	ANMERKUNG	Harmonisiert als EN 61850-8-1.
IEC 61850-8-2	ANMERKUNG	Harmonisiert als EN IEC 61850-8-2 .
IEC 61968 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 61968.
IEC 61970 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 61970.
IEC 62351-7:2017	ANMERKUNG	Harmonisiert als EN 62351-7:2017 (nicht modifiziert).
IEC 62351-9	ANMERKUNG	Harmonisiert als EN 62351-9 .
IEC 62351-14	ANMERKUNG	Harmonisiert als EN IEC 62351-14 ^{Z1} .
IEC 62443 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN IEC 62443.

^{Z1} Wird veröffentlicht. Dokumentstufe zum Zeitpunkt der Veröffentlichung: prEN IEC 62351-14:2019.

Anhang ZA (normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ANMERKUNG Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, durch (mod) gekennzeichnet, dann gilt die entsprechende EN oder das HD.

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
IEC 61850-7-2	–	Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)	EN 61850-7-2	–
IEC/TS 62351-2	–	Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms	–	–
IEC 62351-3 + A2	2014 2020	Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP	EN 62351-3 + A2	2014 2020
IEC 62351-4	–	Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives	EN IEC 62351-4	–
IEC/TS 62351-8	2011	Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control	–	–
RFC 2865	–	Remote Authentication Dial In User Service (RADIUS)	–	–
RFC 5246	–	The Transport Layer Security (TLS) Protocol Version 1.2	–	–
RFC 5288	–	AES Galois Counter Mode (GCM) Cipher Suites for TLS	–	–
RFC 5289	–	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)	–	–
RFC 5755	–	An Internet Attribute Certificate Profile for Authorization	–	–
RFC 5878	–	Transport Layer Security (TLS) Authorization Extensions	–	–
RFC 6749	–	The OAuth 2.0 Authorization Framework	–	–
RFC 7519	–	JSON Web Token (JWT)	–	–
XACML-RBAC	2014	XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0, October 2014	–	–

Inhalt

Seite

Europäisches Vorwort.....	2
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	3
Einleitung	9
1 Anwendungsbereich	10
2 Normative Verweisungen	11
3 Begriffe	12
4 Abkürzungen	14
5 RBAC-Prozessmodell.....	15
5.1 Überblick über das RBAC-Prozessmodell.....	15
5.2 Allgemeine RBAC-Konzepte	16
5.3 Trennung von Subjekten, Rollen und Berechtigungen.....	17
5.3.1 RBAC-Modell.....	17
5.3.2 Zuweisung des Subjekts (Subjekt-Rolle-Zuweisung).....	20
5.3.3 Rollenzuweisung (Rolle-Berechtigung-Zuweisung)	20
5.3.4 Berechtigungszuweisung (Zuweisung von Aktionen zu Objekten)	21
5.4 Kriterien für die Definition von Rollen	21
5.4.1 Richtlinien	21
5.4.2 Subjekte, Rollen und Berechtigungen	21
5.4.3 Die Einführung von Rollen verringert die Komplexität.....	21
6 Definition von Rollen.....	22
6.1 Rolle-Berechtigung-Zuweisung innerhalb der Einheit allgemein	22
6.1.1 Allgemeines	22
6.1.2 Anzahl der von einer Rolle unterstützten Berechtigungen	22
6.1.3 Anzahl von unterstützten Rollen.....	22
6.1.4 Flexibilität der Rolle-Berechtigung-Zuweisung.....	22
6.2 Rolle-Berechtigung-Zuweisung bei Energiesystemen	22
6.2.1 Verbindlich vorgeschriebene Rollen und Berechtigungen für die IED-Zugriffskontrolle	22
6.2.2 Automation von Energieversorgungsanlagen mithilfe von IEC 61850.....	26
6.3 Rolle-Berechtigung-Zuweisung bei spezifischen Rollen	27
6.3.1 Allgemeines	27
6.3.2 Codierung von spezifischen Rollen	28
6.3.3 Bewertungskontext.....	32
6.4 Rolle-Berechtigung-Zuweisung im Hinblick auf andere Domänen außerhalb von Energiesystemen (z. B. Prozesssteuerung in der Industrie)	32
7 Verteilung von RBAC-Erkennungsmerkmalen mithilfe des „PUSH“-Modells.....	32
7.1 Allgemeines	32
7.2 Sicherer Zugriff auf ein LDAP-fähiges Repository	34

7.3	Sicherer Zugriff auf einen Identitätsprovider zur Abfrage eines JWT	34
8	Verteilung von RBAC-Erkennungsmerkmalen mithilfe des „PULL“-Modells	34
8.1	Allgemeines.....	34
8.2	Sicherer Zugriff auf ein LDAP-fähiges Repository	36
8.2.1	Allgemeines.....	36
8.2.2	„PULL“-Modell mit LDAP.....	36
8.2.3	Organisation des LDAP-Verzeichnisses	37
8.3	Sicherer Zugriff auf ein RADIUS-fähiges Repository	38
8.3.1	Allgemeines.....	38
8.3.2	„PULL“-Modell mit RADIUS.....	38
8.3.3	RADIUS-Sicherheit mittels transparentem TLS-Schutz.....	40
8.4	Sicherer Zugriff auf den JWT-Provider	42
9	Allgemeine Anwendung des RBAC-Zugriffs-Token (informativ).....	43
9.1	Allgemeines.....	43
9.2	Sitzungsbasierter Ansatz	43
9.3	Nachrichtenbasierter Ansatz	45
10	Definition von Zugriffs-Token	45
10.1	Allgemeines.....	45
10.2	Unterstützte Profile.....	46
10.3	Identifikation von Zugriffs-Token.....	46
10.4	Allgemeine Struktur von Zugriffs-Token.....	46
10.4.1	Verbindlich vorgeschriebene Felder von Zugriffs-Token	46
10.4.2	Verbindlich vorgeschriebene profilspezifische Felder.....	47
10.4.3	Optionale Felder von Zugriffs-Token	47
10.4.4	Definition der spezifischen Felder.....	47
10.5	Spezifische Struktur von Zugriffs-Token	50
10.5.1	Profil A: X.509-Zertifikat des öffentlichen Schlüssels	50
10.5.2	Profil B: X.509-Attributzertifikat.....	53
10.5.3	Profil C: JSON Web-Token – JWT.....	57
10.5.4	Profil D: RADIUS-Token.....	58
11	Transportprofile	61
11.1	Nutzung in TCP-basierten Protokollen.....	61
11.2	Nutzung in nicht Ethernet-basierten Protokollen.....	61
12	Verifizierung von Zugriffs-Token	61
12.1	Allgemeines.....	61
12.2	Vorkommen mehrerer Zugriffs-Token	62
12.3	Subjektauthentifizierung.....	62
12.4	Verfügbarkeit von Zugriffs-Token.....	62
12.5	Gültigkeitszeitraum.....	62

	Seite
12.6 Integrität von Zugriffs-Token	63
12.7 Herausgeber	63
12.8 RoleID	63
12.9 Revisionsnummer	63
12.10 Verantwortungsbereich	63
12.11 Rollendefinition	63
12.12 Sperrungsstatus	64
12.13 Operation	64
12.14 Sequenznummer	64
12.15 Zurückziehungsverfahren	64
12.15.1 Allgemeines	64
12.15.2 Unterstützte Methode	65
13 Konformität	65
13.1 Allgemeines	65
13.2 Notation	65
13.3 Einhaltung des Zugriffs-Token-Formats	65
13.4 Einhaltung des Zugriffs-Token-Inhalts	66
13.5 Zugriffs-Token-Verteilung	66
13.6 Rolleninformationsaustausch	67
13.7 Zuweisung zu bestehenden Autorisierungsmechanismen	67
13.8 Sicherheitsereignisse	67
14 Repository-Interaktionen für die definierten RBAC-Profile	67
Anhang A (informativ) Informatives Beispiel für die Definition einer spezifischen Rolle	69
A.1 Anwendungsbereich des Anhangs	69
A.2 Beschreibung des Anwendungsfalls	69
A.3 Beispiel für die Definition in XACML	69
A.4 Rollenbezeichnung	70
A.5 Bezeichnung der Berechtigungsgruppen	71
A.6 Bezeichnung der Berechtigungen	72
A.7 Abfragesyntax für PDP	75
Literaturhinweise	76

Bilder

Bild 1 – Allgemeine Umgebung einer Zugriffskontrolle	16
Bild 2 – Diagramm einer RBAC mit statischer und dynamischer Funktionstrennung (erweiterte Version von ANSI INCITS 359-2004)	18
Bild 3 – Subjekte, Rollen, Berechtigungen und Operationen	20
Bild 4 – XACML-Struktur	29
Bild 5 – Schematische Ansicht des auf der RBAC basierenden Autorisierungsmechanismus	33

Bild 6 – Schematische Ansicht des auf dem RBAC „PULL“-Modell basierenden
Autorisierungsmechanismus 36

Bild 7 – RBAC „PULL“-Modell mithilfe von LDAP 37

Bild 8 – RBAC „PULL“-Modell mithilfe von RADIUS 39

Bild 9 – RBAC-Modell mit OAuth 2.0 und JWT 43

Bild 10 – Sitzungsbasierter RBAC-Ansatz (vereinfachte Ende-zu-Ende-Sicherheit aus IEC 62351-4)..... 45

Tabellen

Tabelle 1 – Liste der verbindlich vorgeschriebenen definierten Berechtigungen..... 23

Tabelle 2 – Verbindlich vorgeschriebene vordefinierte Rollen 24

Tabelle 3 – Liste der definierten Rolle-Berechtigung-Zuweisungen 25

Tabelle 4 – Berechtigung LISTOBJECTS und zugehörige ACSI-Dienste 26

Tabelle 5 – Bewertungskontext 32

Tabelle 6 – Kombinationen von Verschlüsselungs-Suites im Kontext dieses Dokuments 41

Tabelle 7 – Verbindlich vorgeschriebene Bestandteile von Zugriffs-Token 46

Tabelle 8 – Verbindlich vorgeschriebene profilspezifische Bestandteile von Zugriffs-Token 47

Tabelle 9 – Optionale Bestandteile von Zugriffs-Token 47

Tabelle 10 – AoR-Felder und Format..... 50

Tabelle 11 – Zuweisung zwischen ID und Attributzertifikat..... 56

Tabelle 12 – Einhaltung des Zugriffs-Token-Formats 66

Tabelle 13 – Einhaltung der Zugriffs-Token-Verteilung..... 66

Tabelle 14 – Vergleich der Profile 68

Tabelle A.1 – Zuweisung der Berechtigung 69

Dokumentenhistorie

Alle Personen, die sich an der Bearbeitung des vorliegenden Dokuments beteiligen, sind aufgefordert, ihre Bearbeitungen in der nachfolgenden Tabelle zu dokumentieren, bevor sie das Dokument weiterleiten. Auf diese Weise können alle Akteure die vorgenommenen Änderungen nachvollziehen und sehen, wer diese vorgenommen hat.

Alle wichtigen Mitteilungen an die IEC-Editoren sollten ebenfalls in der nachfolgenden Tabelle vermerkt werden.

Name der bearbeitenden Person	Dokument erhalten		Kurzbeschreibung der vorgenommenen Änderungen	Dokument versandt	
	Von	Datum		An	Datum
Steffen Fries	WG15	01.03.2017	Erste Version		
Steffen Fries	WG15	30.05.2017	Verbesserung der OID. Weitere Einzelheiten in Bezug auf das RADIUS-Profil. Klärung der Beziehung zu PULL- und PUSH-Modellen, die zu einer Überarbeitung der aktuellen Beschreibung, deren Schwerpunkt ausschließlich auf LDAP liegt, führte		
Steffen Fries	WG15	28.07.2017	Verbesserung des Abschnitts zum Verantwortungsbereich. Standard für profilspezifische Parameter im Zugriffs-Token		
Frances Cleveland	Steffen Fries	31.08.2017	Redaktionelle Aktualisierungen		22.09.2017
Steffen Fries	Frances Cleveland	22.09.2017	Weitere Aktualisierungen des RADIUS-Profiles mit einer Index-Option zur Ermöglichung von mehreren Rollen je Nutzer mit unterschiedlichem AoR oder mit unterschiedlicher Revision Ablehnung von Profil C		
Steffen Fries		22.11.2017	Weitere Beschreibung von Profil D und Beispiele zur Anwendungsintegration. Entfernung des bestehenden Profils C		
Steffen Fries		22.02.2018	Aktualisierung zu RADIUS, Aufnahme speziell angepasster Rollendefinition		
Steffen Fries		30.04.2018	Überarbeitung der speziell angepassten Rollendefinition mittels XACML, wie in IEC 62351-90-1 vorgeschlagen		
Steffen Fries		22.06.2018	Angeglichene Terminologie zu Rechten und Berechtigungen im gesamten Dokument, Überarbeitung verbindlicher Berechtigungen, Aufnahme von JWT (basierend auf dem Beitrag von Arijit Bose) als Profil C. Einführung von Sicherheitsereignissen (Vorfälle und Warnungen), wodurch IEC 62351-14 unterstützt wird.		
Martina Braun	Steffen Fries	28.06.2018	CD-Dokument zur Verteilung	CO	28.06.2018
Steffen Fries		28.11.2018	Aufnahme des Kommentarbeschlusses (57/2056/CC) nach dem WG15-Treffen im Oktober 2018	WG15	23.11.2018
Steffen Fries		17.01.2018	Aufnahme der abschließenden Besprechung offener Punkte nach dem WG15-Treffen im Januar 2019	WG15	
Martina Braun	IEC	17.05.2019	Bearbeiteter CDV an Projektleiter für den nächsten Schritt	Steffen Fries	20.05.2019
Steffen Fries		17.05.2019	Aufnahme des Kommentarbeschlusses für CDV nach der abschließenden Besprechung während des Online-Meetings WG15 am 1. Juli 2019 und der Diskussion mit IETF RADEST WG (Anpassung der Portnummer-Zuweisung)	IEC	
Martina Braun	Steffen Fries	16.08.2019	Hochladen des FDIS-Dokuments an IEC für den Umlauf.	IEC CO	2019-0-23

Einleitung

Dieses Dokument enthält eine Norm für die Zugriffskontrolle in Energiesystemen. Die von diesem Dokument unterstützte Energiesystemumgebung gilt unternehmensweit, geht über die herkömmlichen Grenzen hinaus und umfasst externe Anbieter, Lieferanten und andere Energieversorgungspartner. Treibende Kräfte sind die Liberalisierung des Energiemarkts und damit einhergehend die Einbeziehung einer stark gestiegenen Zahl an betroffenen Parteien, die immer stärkere Dezentralisierung der Energieerzeugung sowie die Notwendigkeit den Zugriff auf sensitive Daten von Ressourcen und Betroffenen zu kontrollieren. Dieses Dokument unterstützt eine verteilte Sicherheitsumgebung, in der die Sicherheit ebenfalls einen verteilten Dienst darstellt.

Der Energiesektor verbessert beständig die Bereitstellung von Energie durch die Nutzung technischer Fortschritte bei computerbasierten Anwendungen. Betreiber von Versorgungseinrichtungen, Energie-Broker und Endbenutzer greifen verstärkt auf eine Vielzahl von Anwendungen zu, um Energie personalisiert bereitzustellen, zu übertragen und zu nutzen. Diese uneinheitlichen Anwendungen sind ihrer Natur gemäß mit einer gemeinsamen Netz-Infrastruktur verbunden, die üblicherweise Schutzeinrichtungen, Automatisierungsprotokolle von Stationen, stationsinterne Protokolle, Fernzugänge und B2B-Dienste (business-to-business service) unterstützen. Folglich ist der sichere Zugriff zu diesen verteilten und häufig nur lose verbundenen Anwendungen sogar noch wichtiger als der Zugriff auf eine Anwendung, die auf einem eigenständigen Gerät ausgeführt wird.

Zu der Bereitstellung eines sicheren Zugriffs zu computerbasierten Anwendungen gehört auch die Authentifizierung der Nutzer dieser Anwendung. Nach der Authentifizierung werden dann die Arten von Interaktionen bestimmt, die dieser Benutzer mit der Anwendung durchführen kann. Die Nutzung lokaler Autorisierungsmechanismen schafft einen Flickenteppich aus Ansätzen, die über die Bandbreite der Energieversorgungsunternehmen hinweg nur schwer zu verwalten sind. Jede Anwendung entscheidet mit ihrer eigenen Logik über den Autorisierungsprozess. Wenn die Anwendungen allerdings den Zugriff über ein gemeinsames Netzwerk verwalten können, so kann eine Datenbank als vertrauenswürdige Quelle der Zugehörigkeit zu einer Benutzergruppe oder einer Rolle dienen. Damit kann der Zugriff zu einer gemeinsamen Benutzerbasis zentral kontrolliert werden. Jede Anwendung kann dann die für ein Subjekt und die entsprechende Rolle aufzeichneten Berechtigungen abfragen und die betreffende Autorisierungsstufe bestimmen.

Dieses Dokument legt die rollenbasierte Zugriffskontrolle (RBAC, en: role-based access control) für die unternehmensweite Nutzung in Energiesystemen fest. Sie unterstützt eine verteilte oder dienstorientierte Architektur, bei der die Sicherheit ein verteilter Dienst ist und die Anwendungen Nutzer dieser verteilten Dienste sind.

In diesem Dokument wird die Rolle eines Benutzers in einem als Zugriffs-Token bezeichneten Container dieses Benutzers zum betreffenden Objekt transportiert. Zugriffs-Token werden mithilfe eines (möglicherweise föderierten) Identitätsmanagement-Tools erstellt und verwaltet. Alle Zugriffs-Token weisen eine Lebensdauer auf und laufen zu einem bestimmten Zeitpunkt ab. Vor der Verifizierung des Zugriffs-Token selbst wird der dieses übermittelnde Benutzer vom betreffenden Objekt authentisiert. Das Objekt vertraut darauf, dass das Management-Tool die Zugriffs-Token mit einer geeigneten Lebensdauer herausgibt. Dies ermöglicht die lokale Verifizierung der Gültigkeit des Zugriffs-Token an entfernten Standorten, ohne dass auf ein zentrales Repository (z. B. eine zentrale Zurückziehungsliste) zugegriffen werden muss.

Vier unterschiedliche Formate für Zugriffs-Token werden in Form von vier unterschiedlichen Profilen unterstützt. Zwei von ihnen basieren auf X.509-Zertifikaten und wurden bereits in IEC TS 62351-8 definiert. Zwei neue Profile werden im Rahmen dieses Dokuments definiert. Das erste neue Profil nutzt JSON zur Codierung des Zugriffs-Token und das zweite neue Profil verwendet ein anbieterspezifisches Attribut in RADIUS, um eine Migrationsoption für Umgebungen bereitzustellen, die bereits einen RADIUS-Server zur Unterstützung der Zugriffskontrolle verwenden. Diese Zugriffs-Token können mit einem spezifischen Transport oder einer spezifischen Anwendung verbunden sein. Allen Zugriffs-Token ist die enthaltene Information gemein, damit eine Migration von einem Profil zum anderen möglich ist.

1 Anwendungsbereich

Der Anwendungsbereich dieses Teils von IEC 62351 besteht in der Unterstützung einer rollenbasierten Zugriffskontrolle (RBAC) für Energiemanagementsysteme. Im Rahmen einer RBAC werden Menschen als Benutzer, automatisierten Systeme und Software-Anwendungen (in diesem Dokument zusammenfassend als „Subjekte“ bezeichnet) definierte „Rollen“ zugewiesen. Dabei wird ihr Zugriff auf genau diejenigen Ressourcen beschränkt, die nach den Sicherheitsrichtlinien für ihre Rollen erforderlich sind.

In dem Maß, in dem Energieversorgungssysteme immer stärker automatisiert und Bedrohungen der IT-Sicherheit immer deutlicher hervortreten, gewinnt eine zuverlässige Einschränkung des Datenzugriffs (Lesen, Schreiben, Kontrolle usw.) an Bedeutung. Wie bei zahlreichen anderen Sicherheitsaspekten ist RBAC nicht nur eine Technologie, sondern vielmehr ein Geschäftsmodell. Dabei ist RBAC kein neues Konzept. Es wird vielmehr von vielen Betriebssystemen genutzt, um den Zugriff auf die Systemressourcen zu steuern. Im Wesentlichen stellt RBAC eine Alternative zum Alles-oder-Nichts-Modell der Super-User dar, bei dem alle Subjekte Zugriff auf alle Daten erhalten, einschließlich der Steuerbefehle.

RBAC ist ein primäres Verfahren zur Einhaltung des Sicherheitsprinzips der minimal erforderlichen Rechte, das darauf beruht, dass kein Subjekt mehr Rechte erhalten sollte als für die Durchführung seiner Aufgabe notwendig ist. Im Rahmen der RBAC wird die Autorisierung von der Authentifizierung getrennt. Außerdem ermöglicht RBAC einer Organisation die Unterteilung und Einhüllung von Super-User-Befähigungen in bestimmten Benutzerkonten, die nach den betreffenden Pflichten definierten Einzelpersonen als Rollen zugewiesen werden. Anhand dieser Unterteilung und den unterstützten Sicherheitsrichtlinien kann bestimmt werden, wer oder welches System auf welche Daten in anderen Systemen zugreifen darf. Auf diese Weise schafft RBAC eine Möglichkeit zur Neuordnung der Systemsteuerungen nach der Definition in der Organisationsrichtlinie. Insbesondere kann RBAC sensible Systemvorgänge vor unbeabsichtigten (oder vorsätzlichen) Aktionen durch nicht autorisierte Benutzer schützen. Natürlich ist RBAC nicht auf menschliche Benutzer limitiert. Das System eignet sich ebenso gut für automatisierte Systeme und Softwareanwendungen, d. h. für Softwareteile, die unabhängig von einer Benutzerinteraktion bestimmte Aktionen ausführen.

In den Anwendungsbereich dieser Norm fallen die folgenden Interaktionen:

- lokaler Zugriff (über lokale, direkt drahtverbundene Systeme) auf Objekte durch einen menschlichen Benutzer, einen lokalen, automatisierten Agenten eines Computersystems, einen integrierten HMI oder einer Anzeige;
- Fernzugriff (über eine Einwählverbindung oder ein drahtloses Medium) auf ein Objekt durch einen menschlichen Benutzer;
- Fernzugriff (über eine Einwählverbindung oder ein drahtloses Medium) auf ein Objekt durch einen automatisierten Agenten eines Computersystems an einem anderen Standort, z. B. ein anderes Objekt an einer anderen Station, eine verteilte Energieressource an der Einrichtung eines Endbenutzers oder eine Anwendung einer Netzleitstelle.

Zum Einen legt dieses Dokument einen Satz von verbindlichen zu unterstützenden Regeln fest, zum anderen ist aber auch das Austauschformat für bestimmte spezifische oder benutzerdefinierte Rollen Bestandteil des Anwendungsbereichs dieses Dokuments.

Außerhalb des Anwendungsbereichs dieses Dokuments sind alle Themen, die nicht unmittelbar mit der Definition von Rollen und Zugriffs-Token für lokale und Fernzugriffe im Zusammenhang stehen. Hierzu zählen insbesondere administrative oder organisatorische Aufgaben, wie:

- Definition bzw. Richtlinien zu Benutzernamen und Passwörtern;
- Verwaltung von Schlüsseln und/oder dem Austausch von Schlüsseln;
- Verfahrenstechnik für die Rollendefinition;
- Rollenzuweisung;
- Auswahl vertrauenswürdiger Zertifizierungsstellen, die Zugriffsdaten (Zugriffs-Token) herausgeben;
- Definition der Aufgaben von Sicherheitsmitarbeitern;
- Integration örtlicher Richtlinien in das RBAC-System.

ANMERKUNG Insbesondere die Verwaltung von Zertifikaten wird in IEC 62351-9 behandelt.

Derzeit vorhandene Normen (siehe ANSI INCITS 359-2004, IEC 62443 (alle Teile) und IEEE 802.1X-2004) der Prozesssteuerungsbranche und der Zugriffskontrolle (RFC 2904 und RFC 2905) sind nicht ausreichend, da diese weder den genauen Rollennamen und die zugehörigen Berechtigungen noch das Format der Zugriffs-Token oder den genauen Mechanismus festlegen, mit dem die Zugriffs-Token zum Zielsystem transportiert und dort authentisiert werden. Für die Interoperabilität sind diese Angaben aber alle erforderlich.

Auf der anderen Seite legt IEEE 1686 bereits eine Mindestanzahl von zu unterstützenden Rollen und die Berechtigungen fest, die mithilfe der Rollen definiert werden müssen. Es ist zu beachten, dass IEEE 1686 derzeit überarbeitet wird.

Im Rahmen dieses Dokuments werden Sicherheitsereignisse als Warnungen und Alarmer definiert. Diese Sicherheitsereignisse sollen die Fehlerbehandlung unterstützen und somit die Ausfallsicherheit des Systems steigern. Es ist wichtig, da Implementierungen einen Mechanismus zum Melden von Sicherheitsereignissen enthalten.

Zu beachten ist, dass für Prozesse der Sicherheitswarnungen und -alarmer, die aus der Protokollierung von Sicherheitsereignissen und Überwachungsinformationen resultieren, separate Dokumente existieren, die die Handhabung festlegen. Noch genauer, die Handhabung von Sicherheitsereignissen ist in IEC 62351-14¹ definiert, während die Handhabung von Überwachungsinformationen in IEC 62351-7 definiert ist.

Es ist zu beachten, dass Warnungen und Alarmer zur Angabe des Schärfegrads eines Ereignisses aus Sicht der Sicherheit dienen. Die folgenden Konzepte werden verwendet:

- eine Warnung wird die Aufmerksamkeit auf etwas richten, aber auch anzeigen, dass es unter Umständen sicher sein kann, fortzufahren;
- ein Alarm zeigt an, dass nicht fortgefahren werden soll.

In jedem Fall wird erwartet, dass die Sicherheitsrichtlinie des Betreibers die abschließende Handhabung basierend auf der Einsatzumgebung festlegt.

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).

IEC 61850-7-2, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
IEC 62351-3:2014/AMD2:2019²

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC TS 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

¹ In Vorbereitung. Stand zum Zeitpunkt der Veröffentlichung: IEC/CD 62351-14:2019.

² In Vorbereitung. Stand zum Zeitpunkt der Veröffentlichung: IEC BPUB 62351-3/AMD2:2019.

RFC 5246, *Transport Layer Security (TLS) Protocol version 1.2*

RFC 5288, *AES Galois Counter Mode (GCM) Cipher Suites for TLS*

RFC 5289, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

RFC 5755, *An Internet Attribute Certificate Profile for Authorization*

RFC 5878, *Transport Layer Security (TLS) Authorization Extensions*

RFC 6749, *The OAuth 2.0 Authorization Framework*

RFC 7519, *JSON Web Token (JWT)*

XACML-RBAC, *XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0, October 2014* [viewed 2019-11-15]. Available at:
<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-en.html>

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC TS 62351-2 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Zugriffs-Token

Nachweis oder Bezeugung(en) der Glaubwürdigkeit, Vertrauenswürdigkeit der Autorität eines Benutzers

3.2

Verantwortungsbereich

Reichweite der Autorität eines Benutzers (beispielsweise auf der Grundlage einer Netzwerkisolierung)

3.3

automatisierter Agent

Rechnerprogramm, das auf einem einzelnen Computer ausgeführt wird und unabhängig von Benutzereingaben Operationen auf lokalen oder entfernten Systemen ausführt

3.4

dynamische Funktionstrennung

DSD; en: dynamic separation of duty

Begrenzung der Verfügbarkeit von Berechtigungen durch Einrichtung von Rollenbeschränkungen, die innerhalb einer Benutzersitzung oder darüber hinaus aktiviert werden können

Anmerkung 1 zum Begriff: DSD bietet die Möglichkeit potenzielle Interessenkonflikte bei der Zuweisung eines Benutzers zu einer Rolle zu beseitigen und erlaubt einen Benutzer für Rollen zu autorisieren, die zwar bei unabhängiger Wahrnehmung keine Interessenkonflikte hervorrufen aber bei gleichzeitiger Wahrnehmung Richtlinienverletzungen herbeiführen. Diese Funktionstrennung könnte zwar auch durch eine statische Trennung der Funktionsbeziehung erreicht werden, aber DSD-Beziehungen bieten einem Unternehmen im Allgemeinen eine größere Betriebsflexibilität.

3.5

Halter

Benutzer, der ein Zugriffs-Token besitzt oder innehat

3.6

Einheit

mit einer Rolle-Berechtigung-Zuweisung versehene Instanz, die Zugriffs-Token akzeptiert

3.7

Identitätsprovider

Instanz, die Identitätsdaten erstellt, speichert und verwaltet; wird üblicherweise in Single-Sign-on-Szenarien verwendet

3.8

Herausgeber

Instanz, die ein Zugriffs-Token herausgibt

3.9

Objekt

der Zugriffskontrolle unterliegende Systemressource, wie Dateien, Drucker, Bildschirmarbeitsplätze, Datenbankdaten usw.

3.10

Operation

ausführbares Bild eines Programms, das bei Aufruf eine Funktion oder Aktivität für das Subjekt ausführt

3.11

band-externe Kommunikation

Kommunikation, die außerhalb des zuvor definierten Kommunikationsverfahrens oder -kanals stattfindet

3.12

Berechtigung

Recht zur Ausführung einer Aktion bei einem Systemobjekt (z. B. Berechtigung = FILEWRITE: Aktion = Schreiben [en: write], Objekt = Datei [en: FILE])

Anmerkung 1 zum Begriff: Berechtigungen werden im Rahmen dieses Dokuments definiert, können aber auch bei der Definition spezifischer Rollen von einem Betreiber vorgegeben werden. Da Berechtigungen mit spezifischen Objekten zusammenhängen, kann die entsprechende Aktion nur durchgeführt werden, wenn sie vom Zielgerät unterstützt wird.

3.13

Privileg

Attribut oder Eigenschaft, die eine verantwortliche Stelle einem Subjekt zuweist

3.14

Rechteverwaltungs-Infrastruktur

PMI; en: privilege management infrastructure

Infrastruktur, mit der Rechte verwaltet werden können, um im Zusammenhang mit einer Public-Key-Infrastruktur umfassende Autorisierungsdienste zu unterstützen

3.15

Recht

kleinste unabhängige Aktionseinheiten (z. B. Lesen, Schreiben)

3.16

Rolle

Funktion im Arbeitsumfeld einer Organisation mit einer bestimmten Semantik hinsichtlich der Autorität und Verantwortlichkeit, die einem Benutzer mit der Rolle übertragen wird

Anmerkung 1 zum Begriff: Eine Rolle fasst einen Satz von Berechtigungen zusammen.

Definierte Rolle: Rolle, die in diesem Dokument definiert wird.

Vorgegebene Rolle: Rolle, die vom Anbieter einer Schutzeinrichtung (nicht durch deren Norm) definiert wird und im Allgemeinen für alle Objekte dieses Anbieters gilt

Spezifische Rolle: Rolle, die vom Netzbetreiber für seine besonderen Anforderungen definiert wird

3.17

Dienst

Berechtigung im Zusammenhang mit IEC 61850

3.18

Dienstanbieter

Objekt, das Dienste bereitstellt, welches der Zugriffskontrolle unterliegt

3.19

Sitzung

Zuweisung eines Benutzers zu einer Anwendung oder einem Computer

Anmerkung 1 zum Begriff: Eine Benutzersitzung ist die Zeit von der Öffnung eines Kommunikationskanals (lokal oder von einem Fernstandort) bis zu dessen Schließung (durch den Benutzer oder durch das System).

3.20

statische Funktionstrennung

SSD; en: static separation of duty

Durchsetzung von Einschränkungen der Zuweisung von Benutzern zu Rollen

Anmerkung 1 zum Begriff: Die Mitgliedschaft in einer Rolle kann den Benutzer in Abhängigkeit von durchgesetzten SSD-Regeln daran hindern, Mitglied einer anderen Rolle oder mehrerer anderer Rollen zu werden.

3.21

Subjekt

Benutzer oder automatisierter Agent

Anmerkung 1 zum Begriff: Ein Subjekt ist der Halter (Inhaber) einer Berechtigung; er muss ein Namensattribut mit einem verbindlich vorgeschriebenen Wert aufweisen, mit dem das Subjekt einer bestimmten Rolle zugewiesen werden muss.

3.22

Token

physische Instanz eines Zugriffs-Token

3.23

Benutzer

Mensch oder Systemanwendung

4 Abkürzungen

AC	Attributzertifikat (en: attribute certificate)
ACL	Zugriffskontrollliste (en: access control list)
ACRL	Attributzertifikatsperrliste (en: attribute certificate revocation list)
ACSI	abstrakte Kommunikationsdienst-Schnittstelle (en: abstract communication system interface)
AMI	erweiterte Infrastruktur für die Zählwerterfassung (en: advanced metering infrastructure)
AoR	Verantwortungsbereich (en: area of responsibility)
CIM	allgemeines Informationsmodell (en: common information model)
CRL	Zertifikatsperrliste (en: certificate revocation list)
DER	unterschiedene Codierregeln (en: distinguished encoding rules)
HMAC	Keyed-Hash-Nachrichtenauthentifizierungscode (en: keyed-hash message authentication code)

HMI	Mensch-Maschine-Schnittstelle (en: human machine interface)
IED	intelligentes elektronisches Gerät (en: intelligent electronic device), steht für ein Feldgerät, ein Gateway oder einen PC in der Netzleitstelle.
ID	Bezeichnung (en: identity)
IS	Internationale Norm (en: international standard)
LDAP	leichtgewichtiges Verzeichniszugriffsprotokoll (en: lightweight directory access protocol)
LD	logisches Gerät (en: logical device) (IEC 61850)
LN	logischer Knoten (en: logical node) (IEC 61850)
OASIS	Organisation für die Weiterentwicklung strukturierter Informationsstandards (en: Organization for the Advancement of Structured Information Standards)
OCSP	Online-Zertifikat Status-Protokoll (en: online certificate status protocol)
OID	Objekt-Identifizierer
OSI	Kommunikation offener Systeme (en: open systems interconnection)
PDP	Richtlinienentscheidungspunkt (en: policy decision point), (RFC 2904): Der Punkt, an dem Entscheidungen zu Richtlinien getroffen werden.
PEP	Richtlinienumsetzungspunkt (en: policy enforcement point), (RFC 2904): Der Punkt, an dem Entscheidungen zu Richtlinien tatsächlich umgesetzt werden.
PKI	Public-Key-Infrastruktur; umfassender Satz von Prozessen, die für die Bereitstellung von Verschlüsselungs- und digitalen Signatordiensten erforderlich sind
PMI	Rechteverwaltungs-Infrastruktur (en: privilege management infrastructure); umfassender Satz von Prozessen, die für die Bereitstellung von Autorisierungsdiensten erforderlich sind
RADIUS	Authentifizierungsdienst für sich einwählende Benutzer (en: remote authentication dial in user service)
RBAC	rollenbasierte Zugriffskontrolle (en: role-based access control)
SCL	Sprache für die Beschreibung der Konfiguration für die Kommunikation in Stationen (IEC 61850) (en: substation configuration description language)
SSL	Secure Socket Layer
SW	Software
TCP	Übertragungssteuerungsprotokoll (en: transport/transmission control protocol)
TLS	Transportschichtsicherheit (en: transport layer security)
UID	allgemeiner Bezeichner (en: universal identifier)
VSA	anbieterspezifische Attribute (in RADIUS) (en: vendor-specific attributes)

5 RBAC-Prozessmodell

5.1 Überblick über das RBAC-Prozessmodell

Zweck eines Zugriffskontrollmechanismus ist der Schutz der formal als „Objekte“ bezeichneten Systemressourcen. Die rollenbasierte Zugriffskontrolle (RBAC) ist eine Technik mit dem Potential, die Komplexität und die Kosten der Sicherheitsadministration in Netzwerken mit zahlreichen intelligenten Geräten zu verringern. Bei Nutzung von RBAC wird die Sicherheitsverwaltung durch die Nutzung von Rollen und Einschränkungen bei der Organisation der Zugriffsebenen von Subjekten vereinfacht. RBAC verringert die Kosten innerhalb der Organisation in erster Linie deshalb, weil hierbei akzeptiert wird, dass Mitarbeiter ihre Rollen und Verantwortlichkeiten häufiger wechseln als die Berechtigungen innerhalb dieser Rollen und Verantwortlichkeiten geändert werden müssen. In einem System, das RBAC implementiert, können Systemressourcen Informationscontainer (z. B. Dateien, Verzeichnisse im Betriebssystem und/oder Spalten, Reihen, Tabellen und Sichten innerhalb eines Datenbank-Managementsystems) oder nicht unerschöpfliche Gerätere Ressourcen darstellen, wie Drucker, Speicherplatz auf Festplatten und CPU-Zyklen.

Üblicherweise wird die Anwendung von RBAC in drei Phasen unterteilt:

- Phase 1: Zuweisung
 - von Aktionen zu Objekten, um Berechtigungen aufzubauen (kommt nicht sehr häufig vor);
 - von Berechtigungen zu Rollen (kommt weniger häufig, nur bei der Definition bestimmter Rollen);
 - von Subjekten zu Rollen (kommt je nach Anwendungsfall unter Umständen häufig vor).
- Phase 2: Operation (Durchsetzung)
 - Authentifizierung des Subjekts gegenüber der akzeptierenden Partei (en: relying party);
 - Autorisierung des Subjekts zur Durchführung einer bestimmten Aufgabe auf der Grundlage der übermittelten Rolleninformation und den zugehörigen Berechtigungen.

Im Zusammenhang mit diesem Dokument ist die Rolleninformation in einem Zugriffs-Token enthalten. Phase 1 ist eine Vorbedingung für Phase 2, da die Authentifizierung des Subjekts an das Zugriffs-Token gebunden wird. Außerdem muss beachtet werden, dass die akzeptierenden Parteien die Authentifizierung direkt durchführen oder sie an ein (Zugriffs-Token-)Repository verweisen kann, das die zugehörigen Daten enthält.

5.2 Allgemeine RBAC-Konzepte

Dieses Dokument legt eine Reihe von Methoden zur rollenbasierten Zugriffskontrolle zur Unterstützung der RBAC in Automatisierungssystemen für die Stromversorgung fest. Der Zweck dieses Dokuments ist es daher:

- 1) Subjekt-Rollen-Berechtigungen als Autorisierungskonzept einzuführen;
- 2) alle Ebenen der Energiemanagementsysteme die rollenbasierte Zugriffskontrolle zu fördern; und
- 3) Interoperabilität zwischen den Umgebungen der Automatisierung in den Energieversorgungssystemen mehrerer Anbieter zu ermöglichen.

Da sich die Namen von Subjekten häufiger ändern als die Namen der Rollen, und sich die Namen der Rollen häufiger ändern als die Berechtigungen eines Datenmodells (z. B. IEC 61850), ist es ratsam, die sich häufig ändernden Einheiten (also die Subjektnamen) außerhalb des Objekts zu speichern. Die sich weniger häufig ändernden Rollennamen und Berechtigungen werden im Objekt gespeichert.

Bild 1 enthält ein allgemeines Bild von einer Zugriffskontrolle. Diese besteht aus einem Subjekt, einem Identitätsprovider und einem Objekt.

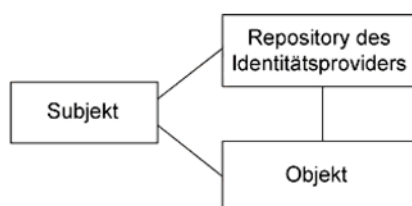


Bild 1 – Allgemeine Umgebung einer Zugriffskontrolle

Das Subjekt möchte mithilfe eines von einem Identitätsprovider bereitgestellten Zugriffs-Token auf die Ressource der Einheit (akzeptierenden Partei) zugreifen. Hierzu gibt es im Allgemeinen zwei Möglichkeiten:

- Das Zugriffs-Token kann von der Einheit aus dem Repository des Identitätsproviders entnommen werden, sobald sich das Subjekt mit der Einheit verbindet. Dieser Fall wird als „PULL“-Vorgang bezeichnet.
- Die andere Möglichkeit besteht darin, dass das Subjekt das Zugriffs-Token aus dem Repository des Identitätsproviders vor dem Zugriff auf die Einheit entnehmen kann. Dieser Fall wird als „PUSH“-Vorgang bezeichnet.

Das Zugriffs-Token enthält die Rolle des Subjekts sowie weitere Informationen zur Gültigkeit des Zugriffs-Token und weitere Parameter. Die RBAC ist ein Bestandteil der allgemeinen Authentifizierung, Autorisierung und Konteninfrastruktur zur Steuerung des Zugriffs auf Daten und Dienste. Im Allgemeinen erhält das Subjekt seine Berechtigungen über die Rollen, die der Einheit gesendet („PUSH“) oder von der Einheit erhalten („PULL“) werden. In jedem Fall wird erwartet, dass die kontrollierte Einheit das Zugriffs-Token validiert, nachdem sie das Subjekt authentifiziert und den Zugriff freigegeben hat.

Bei der Entscheidung, ob ein „PUSH“- oder ein „PULL“-Modell eingesetzt wird, sollten folgende Punkte berücksichtigt werden.

Für das „PUSH“-Modell:

- ist es nicht erforderlich, dass das kontrollierte Objekt auf das Repository zugreifen kann, ein Vertrauensverhältnis zwischen beiden reicht zur Validierung des Zugriffs-Token aus;
- muss das Zugriffs-Token, das die Autorisierungsinformationen enthält, ausreichend sicher sein, während es vom Repository zum Subjekt und weiter zur kontrollierten Einheit gesendet wird. Dies wird üblicherweise durch die Eigenständigkeit des Zugriffs-Token erreicht. Nicht alle in diesem Dokument definierten Profile unterstützen diese Eigenständigkeit. Insbesondere das RADIUS-Profil (D) ist nicht für dieses Einsatzmodell geeignet, da die RBAC-Information an das anbieterspezifische Attribut (VSA, en: vendor specific attribute) gebunden ist, welches keinen Eigenschutz (Eigenständigkeit) bietet;
- das Zugriffs-Token sollte eine nur kurze Lebensdauer haben, um Replay-Angriffe zu verhindern;

Für das „PULL“-Modell:

- der Authentifizierungsdienst auf der Repository-Seite muss für das kontrollierte Objekt erreichbar sein;
- der Token-Austausch muss – insbesondere bei Zugriffs-Token, die nicht über Eigenschutz verfügen – verschlüsselt sein;
- die Authentifizierungsinformationen bei einem „PULL“-Vorgang sind stets aktuell.

5.3 Trennung von Subjekten, Rollen und Berechtigungen

5.3.1 RBAC-Modell

Ein RBAC-Modell enthält Rollen- und Operationsbeschränkungen. Die Funktionstrennung (statisch wie dynamisch) geht aus [Bild 2](#) hervor.

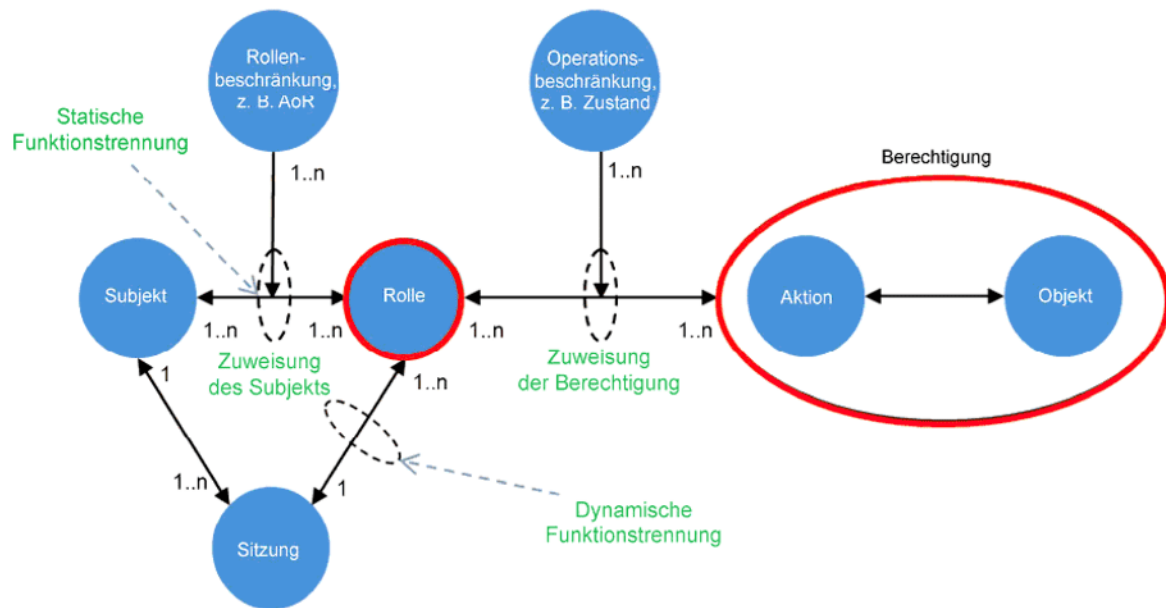


**Bild 2 – Diagramm einer RBAC mit statischer und dynamischer Funktionstrennung
(erweiterte Version von ANSI INCITS 359-2004)**

Die Hauptkomponenten der RBAC sind: Subjekt, Rolle, Sitzung und Berechtigungen als kleinste Aktions-einheiten für Objekte, wie in Bild 2 angegeben.

- Zu den Subjekten zählen Menschen, automatisierte Systeme und Softwareanwendungen. Beispiele aus dem Bereich des Energiemanagements umfassen Max Mustermann, das SCADA-System, ein Ausfallmanagementsystem, eine Stromflussanwendung in einem EMS und eine Anwendung zur Instandhaltungsprüfung auf einem Wartungs-Laptop.
- Rollen sind verbunden mit Funktionen im Arbeitsumfeld einer Organisation mit einer bestimmten Semantik hinsichtlich der Autorität und Verantwortlichkeit, die einem Subjekt mit der Rolle übertragen wird. Beispiele sind ein Übertragungsnetzbetreiber, ein Power Scheduler, Instandhaltung über ein Fernbedienungsmodul sowie Schutztechnik.
- Sitzungen sind die Zuweisung eines Subjekts zu einer Rolle oder möglicherweise zu mehreren Rollen. Auf diese Weise wird angegeben, welche Rollen ein Subjekt übernehmen darf. Jede Sitzung ist mit einem einzelnen Subjekt verbunden, und jedes Subjekt mit einer Rolle oder mehreren Rollen. In einem Beispiel geht es um eine Person, die als Benutzer als Systembetreiber, als Power Scheduler oder als Supervisor tätig sein darf. Ein anderes Beispiel dreht sich um eine Stromflussanwendung, die auf eine Datenbank mit Echtzeitdaten oder einen Satz von historisierten Daten zugreifen darf.
- Aktionen sind Operationen bei Objekten, die zugelassen oder verweigert werden können. Beispiele sind Lese- und Schreibvorgänge bei Datenobjekten.
- Berechtigungen sind Aktionen, die spezifischen Objekten (Ressourcen) zugeordnet werden. Beispiele sind die Anzeige von Daten (Informationen auf einem Bildschirm), das Lesen von Daten (Datenüberwachung, Herunterladen von Dokumenten), das Schreiben von Daten (Einstellen von Parametern, Aktualisierung von Schutzeinstellungen oder von Zuweisungen von Subjekten zu Rollen), die Ausgabe von Steuerbefehlen (Auslösebefehle, Funktionsaktivierungen), die Konfiguration (Aktualisierung von Firmware) und die Dateiverwaltung (Erstellen und Löschen von Dateien).
- Objekte trennen die unterschiedlichen Aktionen, die aufgerufen werden können. Zu Beispielen zählen Schutzrelais, welche die Aktionen (Lesen) beim Lesen und Aktualisieren (Schreiben) von Schutzparametern und beim Konfigurieren der Firmware trennen.

Die Pfeile in [Bild 2](#) zeigen die Beziehungen an (beispielsweise kann ein Subjekt einer Rolle oder mehreren Rollen und eine Rolle einem Subjekt oder mehreren Subjekten zugewiesen werden). Dies bietet bei der Zuweisung von Berechtigungen zu Rollen und von Subjekten zu Rollen im Sinne des Sicherheitsprinzips der minimal erforderlichen Rechte umfassende Flexibilität und Granularität. Ohne diese Optionen besteht die Gefahr, dass ein Subjekt unter Umständen mehr Zugriff auf Ressourcen erhält als erforderlich ist, da die Kontrolle über die Art des möglichen Zugriffs von Subjekten auf Ressourcen eingeschränkt ist. Jede Steigerung der Flexibilität bei der Kontrolle des Zugriffs auf Ressourcen stärkt darüber hinaus die Anwendung des Sicherheitsprinzips der minimal erforderlichen Rechte.

Es gibt dabei zwischen diesen Komponenten zwei Zuweisungen, die vom Administrator konfiguriert werden müssen:

- die Zuweisung des Subjekts (Subjekt-Rolle-Zuweisung). Beispiele sind eine Person, die als Supervisor angemeldet ist oder eine Stromflussanwendung, die auf einen historisierten Datensatz zugreift.
- die Zuweisung der Berechtigung: Rolle-Berechtigung-Zuweisung zur Definition, was eine Rolle ausführen darf und was nicht. Wenn eine Berechtigung einer Rolle zugewiesen nicht explizit wird, so ist die Aktion verboten (Sicherheitsprinzips der minimal erforderlichen Rechte). Ein Beispiel ist ein Systembetreiber, der zwar berechtigt ist, Steuerbefehle für Schutzschalter auszugeben aber die Schutzeinstellungen nicht ändern darf. Ein weiteres Beispiel ist ein SCADA-System, das Daten von Stations-RTUs überwachen aber keine Befehle an das Energiespeichersystem ausgeben darf.

Weitere RBAC-Konzepte schließen Folgendes ein.

- Rollenbeschränkungen: dürfen einschränken, was ein Subjekt in seiner Rolle ausführen darf. So können SCADA-Systeme beispielsweise durch Verantwortungsbereiche begrenzt sein (SCADA-Systeme dürfen alle Regionen überwachen aber nur innerhalb der westlichen Region oder während der Nachtschicht Steuerbefehle ausgeben).
- Betriebseinschränkungen: dürfen einschränken, was eine Rolle in einem bestimmten Betriebszustand (z. B. bei einem Notfall) ausführen darf. Der Betriebszustand, in dem sich eine Einheit befindet, darf die mit einer Rolle verknüpften Berechtigungen ändern. Wenn sich beispielsweise ein Energiespeichersystem im normalen Modus befindet, kann der Systembetreiber Änderungen der aktiven Leistungsabgabe einleiten. Im Notfallbetrieb nach einer Störabschaltung darf der Systembetreiber unter Umständen gar keine Befehle mehr ausgeben.

[Bild 3](#) zeigt ein Beispiel von Subjekten, Rollen, Berechtigungen und Aktionen nach IEC 61850 (alle Teile). Gezeigt wird auch die Option zur Definition bestimmter Rollen und ihrer zugehörigen Berechtigungen durch einen Betreiber (im Bild auf der rechten Seite).

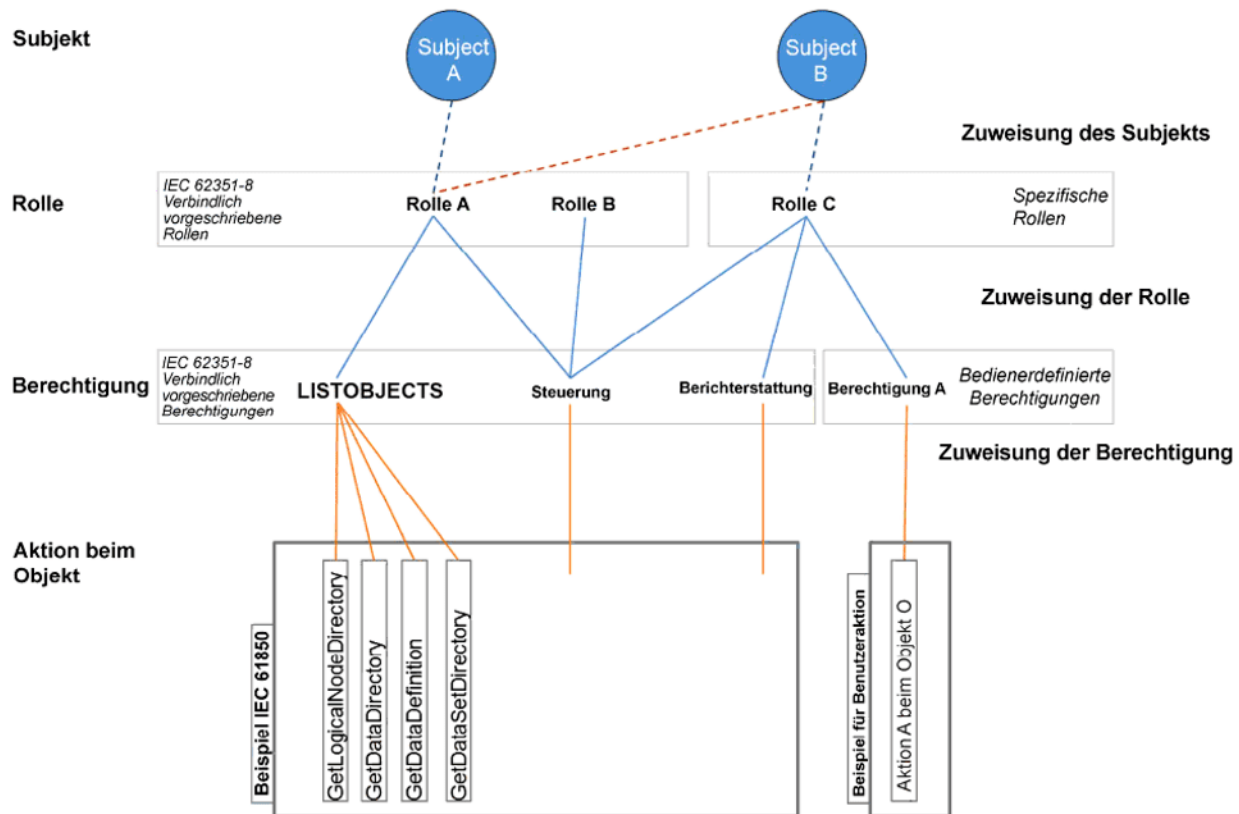


Bild 3 – Subjekte, Rollen, Berechtigungen und Operationen

Aktionen bei Objekten werden durch das gerade verwendete Datenmodell definiert: so darf zum Beispiel ein Schutzsystem ein Datenmodell nach IEC 61850 nutzen. Die Berechtigung bindet diese Aktion an das spezifische Objekt. Dieses Dokument unterstützt Datenmodelle für Energiesysteme nach den Angaben in 6.2.

Um einen ordnungsgemäßen Betrieb zu ermöglichen, müssen ein bestimmter Mindestsatz von Rollen und ihre zugewiesenen Berechtigungen definiert sein. Diese sogenannten definierten Rollen und ihre definierten Berechtigungen sind in Bild 3 durch graue Felder hervorgehoben. Sie sind im Rahmen dieses Dokuments in 6.2 definiert. Die definierten Berechtigungen stellen gegenüber den darunterliegenden Datenmodellen eine Abstraktionsschicht dar. In diesem Dokument ebenfalls definiert ist eine Vorlage zur Definition von spezifischen Rollen und zugehörigen Berechtigungen sowie die Definition von Berechtigungen als auf Objekte angewendete Aktionen in 6.3.

5.3.2 Zuweisung des Subjekts (Subjekt-Rolle-Zuweisung)

Die Zuweisung des Subjekts oder Subjekt-Rolle-Zuweisung wird außerhalb des Systems in einem Repository gespeichert. Der Zugriff auf das Repository wird unter Umständen durch einen LDAP- oder RADIUS-fähigen Dienst ermöglicht, um damit die Zugriffs-Token abzufragen (siehe auch die Abschnitte 7 und 8).

Ein Subjekt oder mehrere Subjekte kann/können einer Rolle oder mehreren Rollen zugewiesen werden.

Der Zeitraum, in dem eine bestimmte Subjekt-Rolle-Zuweisung gültig ist, sollte flexibel gehalten werden.

5.3.3 Rollenzuweisung (Rolle-Berechtigung-Zuweisung)

Die Rollenzuweisung oder Rolle-Berechtigung-Zuweisung wird innerhalb der Einheit gespeichert. Sie stellt die Konfiguration der Einheit dar und hängt vom verwendeten Datenmodell ab.

Diese Zuweisung wird ebenfalls durch Sicherheits- und Schutzbestimmungen definiert und ist der Hauptschwerpunkt dieses Dokuments. Mithilfe von definierten Rollen und definierten Berechtigungen werden solche Richtlinien umgesetzt.