

	DIN EN 62351-9 (VDE 0112-351-9)	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
ICS 35.030; 35.240.50 Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 9: Cybersicherheit Schlüsselmanagement für Stromversorgungsanlagen (IEC 62351-9:2017); Deutsche Fassung EN 62351-9:2017 Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment (IEC 62351-9:2017); German version EN 62351-9:2017 Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance (IEC 62351-9:2017); Version allemande EN 62351-9:2017 Gesamtumfang 91 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2017-06-22 angenommene Europäische Norm als DIN-Norm ist 2018-05-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 62351-9 (VDE 0112-351-9):2014-09.

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

Die enthaltene IEC-Publikation wurde vom TC 57 „Power systems management and associated information exchange“ erarbeitet.

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

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

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

Eine Aufstellung aller Teile der internationalen Normenreihe IEC 62351 unter dem allgemeinen Titel *Energiemanagementsysteme und zugehöriger Datenaustausch* kann auf der Internetseite von IEC eingesehen werden.

In dieser Norm werden folgende Drucktypen verwendet:

- ASN.1-Begriffe sind in fett Courier New dargestellt;
- wenn ASN.1-Typen und -Werte im normalen Text referenziert werden, unterscheiden sie sich vom normalen Text, indem sie in Courier New dargestellt werden.

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 (1 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 62351-3	IEC 62351-3	DIN EN 62351-3	–
EN 62351-11	IEC 62351-11	DIN EN 62351-11	–
–	IEC TR 62351-12	–	–
–	IEC TS 62351-1:2007	–	–
–	IEC TS 62351-2	–	–
–	IEC TS 62351-3	–	–
–	IEC TS 62351-4:2007	–	–
–	IEC TS 62351-5:2013	–	–
–	IEC TS 62351-6	–	–
–	IEC TS 62351-8	–	–
–	IEEE 1588:2008	–	–
–	IEEE 686	–	–
–	ISO/IEC 8802-3-2000:2006	–	–
–	ISO/IEC 9834-1:2012 Rec. ITU-T X.660 (2011)	–	–
–	ISO/IEC 9594-8:2017 Rec. ITU-T X.509 (2016)	–	–
–	ISO/IEC 11770-1:2009	–	–
–	ISO/IEC 11770-2:2008	–	–
–	ISO/IEC 11770-3:2008	–	–
–	ISO/IEC 19790:2012	–	–
–	NIST SP 800-133	–	–
–	NIST SP 800-130	–	–
–	NIST SP 800-97	–	–
–	NIST SP 800-90 A	–	–
–	NIST SP 800-90 B	–	–
–	NIST SP 800-90 C	–	–
–	NIST SP 800-57	–	–
–	RFC 2407	–	–
–	RFC 2631	–	–
–	RFC 2818	–	–
–	RFC 2986	–	–
–	RFC 3447	–	–
–	RFC 3647	–	–

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
–	RFC 3740	–	–
–	RFC 4082	–	–
–	RFC 4120	–	–
–	RFC 4210	–	–
–	RFC 4211	–	–
–	RFC 4476	–	–
–	RFC 4949	–	–
–	RFC 5055	–	–
–	RFC 5246	–	–
–	RFC 5272	–	–
–	RFC 5273	–	–
–	RFC 5280	–	–
–	RFC 5652	–	–
–	RFC 5755	–	–
–	RFC 5905	–	–
–	RFC 5996	–	–
–	RFC 5998	–	–
–	RFC 6066	–	–
–	RFC 6407	–	–
–	RFC 6407	–	–
–	RFC 6712	–	–
–	RFC 6960	–	–
–	RFC 6960	–	–
–	RFC 7030	–	–
–	RFC 7030	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 62351-3, *Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen – Daten- und Kommunikationssicherheit – Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich TCP/IP (IEC 62351-3); Deutsche Fassung EN 62351-3*

DIN EN 62351-11, *Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 11: Sicherheit für XML-Dateien (IEC 62351-11); Englische Fassung EN 62351-11*

Energiemanagementsysteme und zugehöriger Datenaustausch –
IT-Sicherheit für Daten und Kommunikation –
Teil 9: Cybersicherheit Schlüsselmanagement für Stromversorgungsanlagen
(IEC 62351-9:2017)

Power systems management and associated
information exchange –
Data and communications security –
Part 9: Cyber security key management for power
system equipment
(IEC 62351-9:2017)

Gestion des systèmes de puissance et
échanges d'informations associés –
Sécurité des communications et des données –
Partie 9: Gestion de clé de cybersécurité des
équipements de système de puissance
(IEC 62351-9:2017)

Diese Europäische Norm wurde von CENELEC am 2017-06-22 angenommen. 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 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, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, 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: Avenue Marnix 17, B-1000 Brüssel

© 2017 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 62351-9:2017 D

Europäisches Vorwort

Der Text des Dokuments 57/1838/FDIS, zukünftige 1. Ausgabe der IEC 62351-9, erarbeitet vom IEC/TC 57 „Power systems management and associated information exchange“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 62351-9:2017 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2018-03-22
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-06-22

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.

Dieses Dokument wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62351-9:2017 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 62351-3 ANMERKUNG Harmonisiert als EN 62351-3.

Inhalt

Seite

Europäisches Vorwort	2
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Abkürzungen und Akronyme	14
5 Kryptografische Anwendungen für die praktische Umsetzung von Systemen der Energietechnik	16
5.1 Kryptografie, kryptografische Schlüssel und Sicherheitsziele	16
5.2 Kryptografietypen	16
5.3 Verwendungsmöglichkeiten der Kryptografie	17
5.3.1 Ziele der Cybersicherheit	17
5.3.2 Vertraulichkeit	17
5.3.3 Datenintegrität	18
5.3.4 Authentifizierung	18
5.3.5 Unleugbarkeit	18
5.3.6 Vertrauen	18
6 Konzepte zum Schlüsselmanagement und Verfahren beim Betrieb von Systemen der Energietechnik	19
6.1 Sicherheitspolitik für das Schlüsselmanagementsystem	19
6.2 Entwurfsprinzipien des Schlüsselmanagements beim Betrieb von Systemen der Energietechnik	19
6.3 Verwendung von Transportschicht-Sicherheit (TLS)	20
6.4 Gebrauch kryptografischer Schlüssel	20
6.5 Vertrauen durch eine Öffentliche-Schlüssel-Infrastruktur (PKI)	20
6.5.1 Registrierungsstellen (RA)	20
6.5.2 Zertifizierungsstelle (CA)	21
6.5.3 Zertifikate mit öffentlichem Schlüssel	21
6.5.4 Attribut-Zertifikate	21
6.5.5 Erweiterungen in Zertifikaten mit öffentlichem Schlüssel und Attribut-Zertifikaten	22
6.6 Vertrauen durch selbstsignierte Nicht-PKI-Zertifikate	22
6.7 Autorisierungs- und Validierungslisten	23
6.7.1 Allgemeines	23
6.7.2 AVLs in unbeschränkten Umgebungen	23
6.7.3 AVLs in beschränkten Umgebungen	24
6.7.4 Verwendung selbstsignierter Zertifikate mit öffentlichem Schlüssel in AVLs	24
6.8 Vertrauen durch vorher vereinbarte Schlüssel	24
6.9 Sitzungsschlüssel	24
6.10 Protokolle, die beim Vertrauensaufbau verwendet werden	25

6.10.1	Zertifizierungsanforderung	25
6.10.2	Vertrauensanker-Verwaltungsprotokoll (TAMP).....	25
6.10.3	Einfaches Zertifikatanmeldungsprotokoll (SCEP)	25
6.10.4	Internet-Zertifikat-Verwaltungsprotokoll für X.509-Zertifikate in einer PKI	25
6.10.5	Zertifikatmanagement über CMS (CMC).....	26
6.10.6	Anmeldung über sicheren Transport (EST)	26
6.10.7	Übersicht über die verschiedenen Protokolle.....	26
6.11	Gruppenschlüssel.....	26
6.11.1	Zweck von Gruppenschlüsseln	26
6.11.2	Gruppendomäne der Interpretation (GDOI)	27
6.12	Lebenszyklus des Schlüsselmanagements.....	32
6.12.1	Schlüsselmanagement im Lebenszyklus einer Einheit	32
6.12.2	Lebenszyklus des kryptografischen Schlüssels	33
6.13	Zertifikatmanagement-Vorgänge.....	35
6.13.1	Zertifikatmanagement-Vorgang.....	35
6.13.2	Initiale Zertifikaterzeugung	35
6.13.3	Anmeldung einer Einheit	35
6.13.4	Vorgang der Zertifikatsignierungsanforderung (CSR).....	37
6.13.5	Zertifikatsperrlisten (CRLs).....	38
6.13.6	Online-Zertifikat-Status-Protokoll (OCSP).....	39
6.13.7	Serverbasiertes Zertifikatvalidierungs-Protokoll (SCVP)	42
6.13.8	Kurzlebige Zertifikate.....	42
6.13.9	Zertifikaterneuerung	43
6.14	Alternativer Vorgang für außerhalb der Einheit erzeugte asymmetrische Schlüssel	44
6.15	Schlüsselverteilung symmetrischer Schlüssel mit unterschiedlichem Zeitrahmen	45
7	Allgemeine Schlüsselmanagementanforderungen.....	45
7.1	Asymmetrische und symmetrische Schlüsselmanagementanforderungen	45
7.2	Benötigte kryptografische Materialien	45
7.3	Anforderungen an Zertifikate mit öffentlichem Schlüssel	46
7.4	Schutz mit kryptografischem Schlüssel	46
7.5	Verwendung bestehender Sicherheits-Schlüsselmanagement-Infrastruktur	46
7.6	Verwendung von Objektbezeichnern	46
8	Asymmetrisches Schlüsselmanagement.....	47
8.1	Zertifikaterzeugung und -installation	47
8.1.1	Erzeugung und Installation privater und öffentlicher Schlüssel	47
8.1.2	Erneuerung privater und öffentlicher Schlüssel	47
8.1.3	Zufallszahlenerzeugung	47
8.1.4	Zertifikatrichtlinie.....	47
8.1.5	Einheitenregistrierung zur Identitätseinrichtung	47

8.1.6	Einheitenkonfiguration.....	48
8.1.7	Einheitenanmeldung	48
8.1.8	Aktualisierung der Vertrauensankerinformationen.....	50
8.2	Sperrung von Zertifikaten mit öffentlichem Schlüssel	51
8.3	Zertifikatgültigkeit	51
8.3.1	Gültigkeit von Zertifikaten.....	51
8.3.2	Zertifikatssperrung	51
8.3.3	Überprüfung des Zertifikatssperrstatus.....	51
8.3.4	Behandlung von Autorisierungs- und Validierungslisten (AVLs)	52
8.4	Zertifikatablauf und -erneuerung	57
8.5	Sichere Uhrzeitsynchronisation.....	57
9	Symmetrisches Schlüsselmanagement	58
9.1	Gruppenbasiertes Schlüsselmanagement (GDOI)	58
9.1.1	GDOI-Anforderungen	58
9.1.2	Internet-Schlüssel-Austausch Version 1 (IKEv1).....	58
9.1.3	Phase-1-IKEv1-Austausch im Hauptmodus Typ 2	59
9.1.4	Phase 1/2 ISAKMP-Informationsaustausch Typ 5.....	63
9.1.5	Phase-2-GDOI-GROUPKEY-PULL-Austausch Typ 32	64
9.1.6	GROUPKEY-PULL Gruppenschlüssel-Download austausch.....	72
10	Verbindungen zu den Teilen von IEC 62351 und anderen IEC-Dokumenten	73
Anhang A (normativ)	Erklärung zur Konformität der Protokollimplementierung (PICS).....	75
Anhang B (informativ)	Zufallszahlenerzeugung (RNG).....	76
B.1	Typen der Zufallszahlenerzeugung	76
B.2	Deterministische Zufallsbiterzeuger	76
B.3	Nichtdeterministische Zufallsbiterzeuger	77
B.4	Entropiequellen	77
Anhang C (informativ)	Flussdiagramme für Zertifikatanmeldung und -erneuerung	78
C.1	Zertifikatanmeldung.....	78
C.2	Zertifikaterneuerung	78
Anhang D (informativ)	Beispiele für Zertifikatprofile	80
Literaturhinweise		84
Anhang ZA (normativ)	Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	87
Bilder		
Bild 1	– Beziehung zwischen Zertifikaten mit öffentlichem Schlüssel und Attribut-Zertifikaten	22
Bild 2	– Verteilung des Gruppenschlüsselmanagements.....	27
Bild 3	– GDOI IKE Phase 1 – Authentifizierung und Sicherung des Kommunikationskanals.....	28
Bild 4	– GDOI Pull Phase 2	29
Bild 5	– Auslösung der Schlüsselerneuerung durch die Einheiten	31

Bild 6 – Schlüsselmanagement im Produktlebenszyklus	32
Bild 7 – Vereinfachter Lebenszyklus eines Zertifikats	33
Bild 8 – Lebenszyklus des kryptografischen Schlüssels	34
Bild 9 – Beispiel für den SCEP-Einheiten-Anmelde- und CSR-Vorgang.....	36
Bild 10 – Beispiel für den EST-Einheiten-Anmelde- und CSR-Vorgang	37
Bild 11 – CSR-Verarbeitung	38
Bild 12 – Zertifikatssperrliste	39
Bild 13 – Übersicht über das Online-Zertifikat-Status-Protokoll (OCSP).....	40
Bild 14 – Diagramm, das eine Kombination von CRL- und OCSP-Vorgängen verwendet	41
Bild 15 – Anrufabläufe für das Online-Zertifikat-Status-Protokoll (OCSP)	42
Bild 16 – Übersicht über ein serverbasiertes Zertifikatvalidierungs-Protokoll mit Verwendung des OCSP-Backend	42
Bild 17 – SCEP-Zertifikaterneuerung.....	43
Bild 18 – EST-Zertifikaterneuerung/Schlüsselerneuerung	44
Bild 19 – Zentrale Zertifikaterzeugung.....	45
Bild 20 – IKEv1 (RFC 2409)-Austausch im Hauptmodus mit digitalen RSA-Signaturen	59
Bild 21 – IKEv1-Austausch im Hauptmodus und Sicherheitsverbindungsdaten	60
Bild 22 – IKEv1-Austausch im Hauptmodus: Schlüsselaustauschnachrichten	61
Bild 23 – IKEv1-Austausch im Hauptmodus: ID-Authentifizierungsnachrichten	62
Bild 24 – IKEv1-HASH_I-Berechnung	62
Bild 25 – Phase-1-Informationsaustausch	63
Bild 26 – GD004FI GROUPKEY-PULL wie in RFC 6407 definiert.....	64
Bild 27 – GROUPKEY-PULL-Hash-Berechnungen.....	65
Bild 28 – GROUPKEY-PULL: ursprünglicher SA-Anforderungsaustausch	66
Bild 29 – Identifizierungsnutzdatum nach RFC 6407	66
Bild 30 – ID_OID-Identifizierungsdaten	67
Bild 31 – 61850_UDP_ADDR_GOOSE/SV ASN.1 BNF	68
Bild 32 – IPADDRESS ASN.1 BNF	69
Bild 33 – Beispiel für IecUdpAddrPayload ASN.1-Daten mit DER-Kodierung	69
Bild 34 – 61850_UDP_TUNNEL-Nutzdatum ASN.1 BNF	69
Bild 35 – 61850_ETHERNET_GOOSE/SV-Nutzdatum ASN.1 BNF.....	70
Bild 36 – RFC 6407 SA-TEK-Nutzdatum.....	70
Bild 37 – SA-TEK-Nutzdatum nach IEC 61850	71
Bild 38 – GROUPKEY-PULL: Schlüssel-Downloadaustausch.....	72
Bild 39 – Die Beziehung von IEC 62351-9 zu anderen Teilen von IEC 62351	73
Bild C.1 – Zertifikatanmeldung.....	78
Bild C.2 – Zustandsmaschine für die Zertifikaterneuerung.....	79

Tabellen

Tabelle 1 – Von der KDC unterstützte IKEv1-Anforderungen.....58

Tabelle 2 – Objektbezeichner nach IEC 61850: verbindlich (m) oder optional (o).....68

Tabelle D.1 – Beispiele für Betreiberzertifikate mit öffentlichem Schlüssel 81

Tabelle D.2 – Beispiele für OEM-Zertifikate 82

Tabelle D.3 – Beispiel für ein OCSP-Zertifikat 83

1 Anwendungsbereich

Dieser Teil von IEC 62351 legt das Management kryptografischer Schlüssel fest, und zwar wie Zertifikate mit öffentlichem Schlüssel und kryptografische Schlüssel erzeugt, verteilt, gesperrt und verarbeitet werden, um digitale Daten und Kommunikation zu schützen. Im Anwendungsbereich ist sowohl die Behandlung asymmetrischer Schlüssel (z. B. private Schlüssel und Zertifikate mit öffentlichem Schlüssel) als auch symmetrischer Schlüssel (GDOI) enthalten.

Dieser Teil von IEC 62351 geht davon aus, dass andere Normen bereits die Schlüssel- und Kryptografietypen gewählt haben, die verwendet werden, da die gewählten Kryptographie-Algorithmen und Schlüsselmaterialien typischerweise durch die eigenen lokalen Sicherheitsrichtlinien einer Organisation und die Verpflichtung zur Erfüllung anderer Internationaler Normen vorgegeben sind. Dieses Dokument legt daher nur die Managementtechniken für diese ausgewählten Schlüssel- und Kryptografieinfrastrukturen fest. Ziel ist es, Anforderungen und Technologien festzulegen, um Interoperabilität des Schlüsselmanagements zu erreichen.

Dieser Teil von IEC 62351 hat zum Zweck, Interoperabilität zwischen verschiedenen Anbietern sicherzustellen, indem die zu verwendenden Schlüsselmanagement-Optionen festgelegt oder eingeschränkt werden. Dieses Dokument setzt Kenntnisse der Kryptografie und PKI-Prinzipien voraus.

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

ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 9834-1:2012 | Rec. ITU-T X.660 (2011), *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*

SCEP IETF Draft, *Simple Certificate Enrolment Protocol, draft-gutmann-scep-04.txt*

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

RFC 5272, *Certificate Management over CMS (CMC)*

RFC 5934, *Trust Anchor Management Protocol (TAMP)*

RFC 6407, *The Group Domain of Interpretation*

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*

RFC 7030, *Enrolment over Secure Transport*

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

3.1

asymmetrische Schlüssel

zwei zueinander in Beziehung stehende Schlüssel, ein öffentlicher Schlüssel und ein privater Schlüssel, die zur Durchführung von Komplementärfunktionen wie z. B. Verschlüsselung und Entschlüsselung oder Signaturerzeugung und Signaturüberprüfung verwendet werden

3.2

Autorisierungs- und Validierungsliste

AVL

signierte Liste mit Informationen an eine AVL-Einheit über potenzielle Kommunikationsinstanzen und mögliche Einschränkungen der Kommunikationen mit solchen Einheiten

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.9]

3.3

Autorisierungs- und Validierungslisten-Einheit

AVL-Einheit

Einheit, die, wenn sie als vertrauende Partei agiert, abhängig von einer AVL ist, welche von einem festgelegten Autorisierer herausgegeben wird

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.10]

3.4

Autorisierer

Einheit, die von einer oder mehreren als AVL-Einheiten agierenden Einheiten mit der Erzeugung, Verwahrung und Signierung von Autorisierungs- und Validierungslisten betraut wird

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.11]

3.5

Zertifizierungspfad

geordnete Liste von einem oder mehreren Zertifikaten mit öffentlichem Schlüssel, beginnend mit einem vom Vertrauensanker signierten Zertifikat mit öffentlichem Schlüssel und endend mit dem zu validierenden Zertifikat mit öffentlichem Schlüssel der Endeinheit

Anmerkung 1 zum Begriff: Alle zwischengeschalteten Zertifikate mit öffentlichem Schlüssel, falls vorhanden, sind CA-Zertifikate, in denen das betroffene Objekt des vorhergehenden Zertifikats mit öffentlichem Schlüssel der Aussteller des darauffolgenden Zertifikats mit öffentlichem Schlüssel ist.

[QUELLE: ISO/IEC 9594-8:2017, 3.5.18 | Rec. ITU-T X.509 (2016), 3.5.21]

3.6

Zertifikatsignierungsanforderung

CSR

Anforderung, die herausgegeben wird, wenn ein neues Zertifikat oder die Erneuerung eines Zertifikats benötigt wird

Anmerkung 1 zum Begriff: Die CA signiert die CSR unter Verwendung ihres privaten Schlüssels, wenn die erzeugte CSR an die CA übermittelt wird, wodurch die CSR zum Zertifikat wird.

[QUELLE: RFC 2986]

3.7

Controlling

Schnittmenge von rechtlichem Besitz, physikalischer Kontrolle und logischer Kontrolle eines Gerätes oder Systems, bei dem die Art jeglicher vertraglicher Vereinbarungen zwischen Besitz und Kontrolle des Gerätes oder Systems im Kontext nicht wichtig ist

3.8

kryptografische Bindung

Verwendung von einer oder mehreren kryptografischen Techniken durch ein CKMS, um eine vertrauenswürdige Verbindung zwischen einem Schlüssel und ausgewählten Metadaten-Elementen zu erzeugen

[QUELLE: NIST SP 800-130]

3.9

Verwaltungssystem für kryptografische Schlüssel

CKMS

System zur Verwaltung (z. B. Erzeugung, Verteilung, Speicherung, Datensicherung, Archivierung, Wiederherstellung, Benutzung, Sperrung und Zerstörung) von kryptografischen Schlüsseln und ihren Metadaten

[QUELLE: NIST SP 800-130]

3.10

Datensatz

Sammlung von Daten

3.11

digitale Signatur

Ergebnis einer kryptografischen Transformation von Daten, die bei richtiger Implementierung einen Mechanismus zur Überprüfung der Ursprungsauthentifizierung, Datenintegrität und Signaturnachweisbarkeit bietet

[QUELLE: FIPS 186]

3.12

Einheit

Oberbegriff, der menschliche Nutzer, Automatisierungssysteme, Softwareanwendungen, Kommunikationsknoten, Feldgeräte und andere Posten abdeckt

3.13

Gruppencontroller/Schlüsselserver

GCKS

Gerät, das die Gruppenrichtlinie bestimmt und Schlüssel für diese Richtlinie verteilt

[QUELLE: RFC 3740]

3.14

Gruppendomäne der Interpretation

GDOI

Domäne, die Gruppensicherheitsverbindungen verwaltet, die von IPsec und möglicherweise anderen Datensicherheitsprotokollen genutzt werden

Anmerkung 1 zum Begriff: Diese Sicherheitsverbindungen schützen einen oder mehrere Schlüssel zur Schlüsselverschlüsselung (KEK), Schlüssel zur Verkehrsverschlüsselung (TEK) oder Daten, die zwischen Gruppenmitgliedern geteilt werden. GDOI verwendet die Idee eines Gruppencontrollers, der benutzt wird, um den Aufbau von Sicherheitsverbindungen zwischen Mitgliedern einer Gruppe zu unterstützen.

[QUELLE: RFC 6407]

3.15

Gruppenmitglied

GM

autorisiertes Mitglied einer sicheren Gruppe, das gruppenbezogene IP-Pakete versendet und/oder empfängt

3.16

Hash-Funktion

(mathematische) Funktion, die Daten beliebiger Länge auf Daten mit fester Länge (Hashwert) abbildet

Anmerkung 1 zum Begriff: Bewährte Hash-Funktionen erfüllen die folgenden Eigenschaften:

- 1) Einweg. Es ist rechnerisch unmöglich einen Eingabewert zu finden, der auf einen zuvor festgelegten Ausgabewert abgebildet wird.
- 2) Kollisionssicher. Es ist rechnerisch unmöglich, zwei verschiedene Eingabewerte zu finden, die auf denselben Ausgabewert abgebildet werden.

[QUELLE: ISO/IEC 9598-8:2017 | Rec. ITU-T X.509 (2016), 3.5.36]

3.17

Hash-Nachrichtenauthentifizierungscode

HMAC

kryptografischer Code, der zur Authentifizierung mit symmetrischen Schlüsseln und für die Datenintegrität benutzt wird

[QUELLE: RFC 2104]

3.18

Schlüsselverteilungszentrale

KDC

Zentrale, die im Kontext von IEC 62351-9 einen Netzwerkdienst bereitstellt, der nach erfolgreicher Authentifizierung temporäre (symmetrische) Sitzungsschlüssel an eine zuvor festgelegte Reihe von Peers liefert

Anmerkung 1 zum Begriff: Auch als Gruppencontroller/Schlüsselserver (GCKS) bekannt (siehe GDOI).

3.19

Nachrichtenauthentifizierungscode

MAC

kryptografische Prüfsumme aus Daten, die einen symmetrischen Schlüssel zur Erkennung von zufälliger und beabsichtigter Datenveränderung verwendet

[QUELLE: SP 800-63; FIPS 201]

3.20

Objektbezeichner

sortierte Liste primärer ganzzahliger Werte von der Wurzel des internationalen Objektbezeichnerbaums zu einem Knoten, die diesen Knoten eindeutig identifiziert

[QUELLE: ISO/IEC 9834-1:2012 | Rec. ITU-T X.660 (2011), 3.5.11]

3.21

Online-Zertifikat-Status-Protokoll

OCSP

Protokoll, das es Anwendungen ermöglicht, den (Sperr-) Status eines identifizierten Zertifikats zu bestimmen

Anmerkung 1 zum Begriff: Das OCSP darf verwendet werden, um einige der betrieblichen Anforderungen zu erfüllen, indem es Sperrinformationen rechtzeitig als dies mit CRLs möglich ist zur Verfügung stellt, und es darf verwendet werden, um zusätzliche Statusinformationen zu erhalten. Ein OCSP-Client gibt eine Statusanforderung an einen OCSP-Antwortsender heraus und verschiebt die Annahme des fraglichen Zertifikats, bis der Antwortsender eine Antwort bereitstellt.

[QUELLE: RFC 6960]

3.22

vorher vereinbarter Schlüssel

PSK

Geheimnis, das zuvor zwischen zwei Einheiten, wie zum Beispiel Softwareanwendungen oder Geräten, vereinbart wurde, um diese in die Lage zu versetzen, sich nach Aufbau einer sicheren Verbindung selbst zu authentifizieren

3.23

privater Schlüssel

(in einem Kryptosystem mit öffentlichem Schlüssel) derjenige Schlüssel des Schlüsselpaares einer Einheit, der nur dieser Einheit bekannt ist

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.49]

3.24

Zertifikat mit öffentlichem Schlüssel

öffentlicher Schlüssel einer Einheit, der zusammen mit anderen Informationen durch eine digitale Signatur mit dem privaten Schlüssel der CA, die das Zertifikat ausgestellt hat, unfälschbar gemacht wird

Anmerkung 1 zum Begriff: Ein Zertifikat mit öffentlichem Schlüssel wird häufig als X.509-Zertifikat oder digitales Zertifikat bezeichnet. Solche Begriffe sind jedoch mehrdeutig, da sie auch Attribut-Zertifikate bezeichnen könnten, die ebenfalls in ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016) beschrieben sind.

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.57]

3.25

Kryptografienormen für öffentliche Schlüssel

PKCS

Festlegungen, die von den RSA Laboratories in Zusammenarbeit mit weltweiten Entwicklern sicherer Systeme erzeugt werden mit dem Ziel, die Verbreitung der Kryptografie mit öffentlichem Schlüssel zu beschleunigen

[QUELLE: www.rsa.com]

3.26

Zufallszahlenerzeugung

RNG

Prozess, der zur Erzeugung einer unvorhersagbaren Reihe von Zahlen verwendet wird

Anmerkung 1 zum Begriff: Jeder individuelle Wert wird zufällig genannt, falls jeder der Werte aus der Gesamtpopulation der Werte eine gleiche Auswahlwahrscheinlichkeit aufweist.

[QUELLE: NIST SP 800-57]

3.27

Registrierungsstelle

diejenigen Aspekte der Verantwortlichkeiten einer Zertifizierungsstelle, die in Bezug zur Identifizierung und Authentifizierung des betroffenen Objekts eines Zertifikats mit öffentlichem Schlüssel stehen, welches von dieser Zertifizierungsstelle ausgestellt wird

Anmerkung 1 zum Begriff: Eine Registrierungsstelle darf entweder eine eigenständige Einheit sein oder integrierter Bestandteil einer Zertifizierungsstelle.

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T Rec. X.509 (2016), 3.5.60]

3.28

vertrauende Partei

Einheit, die sich bei der Entscheidungsfindung auf die Daten in einem Zertifikat mit öffentlichem Schlüssel verlässt

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.61]

3.29

geheimer Schlüssel

kryptografischer Schlüssel, der in einem kryptografischen Algorithmus für geheime Schlüssel verwendet wird, der eindeutig mit einer oder mehreren Einheiten verbunden ist und nicht öffentlich gemacht werden sollte

[QUELLE: FIPS 140-2]

3.30

Sicherheitsverbindung

SA

Beziehung, die zwischen zwei oder mehr Einheiten aufgebaut wurde, um ihnen den Schutz der ausgetauschten Daten zu ermöglichen

[QUELLE: NIST IR 7298 Rev.1]

3.31

Sicherheitsstärke

Fähigkeit der Sicherheitstechnologien, die für einen potenziellen Angreifer unmöglich zu umgehen oder zu untergraben sind

Anmerkung 1 zum Begriff: Wird oftmals in Bits der Sicherheit [en: bits of security] gemessen.

[QUELLE: NIST SP 800-130]

3.32

Sitzungsschlüssel

im Kontext der symmetrischen Verschlüsselung ein Schlüssel, der temporär ist oder für einen relativ kurzen Zeitraum verwendet wird

[QUELLE: RFC 2828]

3.33

einfaches Zertifikatanmeldungsprotokoll

SCEP

Protokoll, das die sichere Zertifikatausstellung für Netzwerkgeräte auf skalierbare Weise unterstützt und möglichst bestehende Technologien verwendet

Anmerkung 1 zum Begriff: Das Protokoll unterstützt die folgenden Funktionen:

Verteilung des öffentlichen Schlüssels durch CA und RA;

Zertifikatanmeldung;

Zertifikatsperrung;

Zertifikatanfrage;

CRL-Anfrage.

[QUELLE: IETF Draft SCEP]

3.34

symmetrischer Schlüssel

kryptografischer Schlüssel, der verwendet wird, um die kryptografische Funktion und ihre Umkehrfunktion durchzuführen, z. B. die Verschlüsselung und Entschlüsselung oder die Erzeugung eines Nachrichtenauthentifizierungscodes und die Überprüfung des Codes

[QUELLE: NIST SP 800-63]

3.35

Vertrauen

fester Glaube an die Zuverlässigkeit und Wahrheit von Informationen oder an die Fähigkeit und Bereitschaft einer Einheit, in einem bestimmten Kontext angemessen zu handeln

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.2.1]

3.36

Vertrauensanker

Einheit, die von einer vertrauenden Partei als vertrauenswürdig erachtet und für die Validierung von Zertifikaten mit öffentlichem Schlüssel in Zertifizierungspfaden verwendet wird

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.71]

3.37

Vertrauensankerinformationen

mindestens: ausgezeichneter Name des Vertrauensankers, zugehöriger öffentlicher Schlüssel, Bezeichner des Algorithmus, Parameter des öffentlichen Schlüssels (falls zutreffend) und alle Einschränkungen bezüglich seiner Verwendung, einschließlich der Gültigkeitsdauer

Anmerkung zum 1 Begriff: Die Vertrauensankerinformationen dürfen als selbstsigniertes CA-Zertifikat oder als normales CA-Zertifikat (d. h. Cross-Zertifikat) zur Verfügung gestellt werden.

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.72]

3.38

Vertrauensanker-Verwaltungsprotokoll

TAMP

Protokoll zur Verwaltung eines Vertrauensankerspeichers

[QUELLE: RFC 5934]

3.39

Vertrauensankerspeicher

Vertrauensanker-Informationssammlung bei einer vertrauenden Partei für einen oder mehrere Vertrauensanker

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.73]

4 Abkürzungen und Akronyme

Zusätzliche Abkürzungen und Akronyme sind in IEC TS 62351-2 aufgeführt.

ASN.1	abstrakte Syntax-Notation Eins (en: Abstract Syntax Notation One)
AVL	Autorisierungs- und Validierungsliste (en: Authorization and Validation List)
AVMP	Autorisierungs- und Validierungs-Verwaltungsprotokoll (en: Authorization and Validation Management Protocol)
CA	Zertifizierungsstelle (en: Certification Authority)
CASP	Subskriptionsprotokoll der Zertifizierungsstelle (en: Certification Authority Subscription Protocol)
CKMS	Verwaltungssystem für kryptografische Schlüssel (en: Cryptographic Key Management System)
CIA	Vertraulichkeit, Integrität und Verfügbarkeit (en: Confidentiality, Integrity, and Availability)
CMC	Zertifikatmanagement über CMS (en: Certificate Management over CMS)

CMS	kryptografische Nachrichtensyntax (en: Cryptographic Message Syntax)
CSR	Zertifikatsignierungsanforderung (en: Certificate Signing Request)
DER	Distinguished Encoding Rules
DOI	Domäne von Interesse (en: Domain of Interest)
DSA	digitaler Signaturalgorithmus (en: Digital Signature Algorithm)
EST	Anmeldung über sicheren Transport (en: Enrolment over Secure Transport)
GCKS	Gruppencontroller/Schlüsselserver (en: Group Controller/Key Server)
GDOI	Gruppendomäne der Interpretation (en: Group Domain of Interpretation)
GKDC	Gruppen-KDC (en: Group KDC)
GM	Gruppenmitglied (en: Group Member)
GMAC	Galois-Nachrichtenauthentifizierungscode (en: Galois Message Authentication Code)
GOOSE	generisches objektorientiertes Schaltanlagen-Ereignis (en: Generic Object Oriented Substation Event)
HMAC	Hash-Nachrichtenauthentifizierungscode (en: Hash-based Message Authentication Code)
HTTP	Hypertext-Übertragungsprotokoll (en: Hypertext Transfer Protocol)
ID	Identität (en: Identity)
IKE	Internet-Schlüssel-Austausch (en: Internet Key Exchange)
ISAKMP	Internet-Sicherheitsverbindungs- und Schlüsselmanagement-Protokoll (en: Internet Security Association and Key Management Protocol)
KD	Schlüsseldownload (en: Key Download)
KDC	Schlüsselverteilungszentrale (en: Key Distribution Centre), auch GKDC
KEK	Schlüssel zur Schlüsselverschlüsselung (en: Key Encryption Key)
MAC	Nachrichtenauthentifizierungscode ^{N1)} (en: Message Authentication Code)
OCSP	Online-Zertifikat-Status-Protokoll (en: Online Certificate Status Protocol)
PDU	Protokolldateneinheit (en: Protocol Data Unit)
PEM	Privacy-enhanced Electronic Mail
PKCS	Kryptografienorm für öffentliche Schlüssel (en: Public-Key Cryptography Standard)
PKI	öffentlicher-Schlüssel-Infrastruktur (en: Public-Key Infrastructure)
PSK	vorher vereinbarter Schlüssel ^{N1)} (en: Pre-shared Key)
RA	Registrierungsstelle (en: Registration Authority)
RNG	Zufallszahlenerzeugung (en: Random Number Generation)
RSA	Rivest-Shamir-Adleman, kryptografisches Verfahren mit öffentlichem Schlüssel
SA	Sicherheitsverbindung (en: Security Association)
SCEP	einfaches Zertifikatanmeldungsprotokoll (en: Simple Certificate Enrolment Protocol)
SV	Stichprobenwerte (en: Sample Values)
TAMP	Vertrauensanker-Verwaltungsprotokoll (en: Trust Anchor Management Protocol)
TEK	Schlüssel zur Verkehrsverschlüsselung (en: Traffic Encryption Key)

^{N1)} Nationale Fußnote: Abkürzung fehlt im IEC-Original.

5 Kryptografische Anwendungen für die praktische Umsetzung von Systemen der Energietechnik

5.1 Kryptografie, kryptografische Schlüssel und Sicherheitsziele

Der Begriff Kryptografie bezieht sich auf die Verwendung einer Familie von Datentransformations-Algorithmen, um spezifische sicherheitsorientierte Ziele zu erreichen, wie zum Beispiel das Verschleiern der Inhalte einer Nachricht vor unerwünschten Empfängern (Vertraulichkeit), die Absicherung, dass niemand die Nachrichteninhalte während der Übertragung gefälscht hat (Integrität), und die Bestätigung der behaupteten Identität des Absenders (Authentizität). Um Vertraulichkeit, Integrität und Authentizität sicherzustellen, verwenden moderne Implementierungen von Verschlüsselungsverfahren kryptografische Schlüssel als veränderbaren Teil der Datentransformation, wodurch die Sensibilität der Daten auf den Schlüssel statt auf die Nutzdaten verlagert wird. Dieser Teil von IEC 62351 handelt vom Management dieser kryptografischen Schlüssel, um sicherzustellen, dass die Sicherheitsziele im Kontext der praktischen Umsetzung von Systemen der Energietechnik erreicht werden.

5.2 Kryptografietypen

Dieser Teil von IEC 62351 fokussiert auf das Management von Schlüsseln für zwei Basis-Kryptografietypen: asymmetrisch und symmetrisch. Diese beiden Kryptografietypen vertrauen auf Verschlüsselungs-Suiten und zahlreiche allgemein akzeptierte kryptografische Algorithmen. Die Spezifikation von Verschlüsselungsalgorithmen und Konfigurationen für bestimmte Implementierungen wird nicht von diesem Dokument adressiert, die charakteristischen Anforderungen, die mit dem Management beider kryptografischer Schlüsseltypen bei der praktischen Umsetzung von Systemen der Energietechnik verbunden sind, werden jedoch adressiert.

Für die symmetrische Kryptografie wird derselbe Schlüssel verwendet, um die Daten zu verschlüsseln und zu entschlüsseln; daher muss dieser Schlüssel beiden Parteien, die eine symmetrisch verschlüsselte Nachricht austauschen, bekannt sein und geheim gehalten werden. Die verschiedenen symmetrischen Schlüsselalgorithmen werden jeweils durch einen Objektbezeichner identifiziert (siehe 7.6).

Asymmetrische Kryptografie verwendet ein Paar mathematisch miteinander im Zusammenhang stehender Schlüssel. Einer dieser Schlüssel ist der private Schlüssel, der vom Besitzer geheim gehalten werden muss, und der andere ist der öffentliche Schlüssel, der öffentlich bekannt sein darf. Der öffentliche Schlüssel wird üblicherweise in einem Zertifikat mit öffentlichem Schlüssel bereitgestellt, das den öffentlichen Schlüssel an die Identität des Besitzers des Zertifikats mit öffentlichem Schlüssel und damit an den korrespondierenden privaten Schlüssel bindet. Ein solches Zertifikat mit öffentlichem Schlüssel wird durch eine Zertifizierungsstelle verifiziert und digital signiert.

Asymmetrische Kryptografie dient hauptsächlich der Erzeugung digitaler Signaturen, bei der der private Schlüssel in Verbindung mit einem Hash-Algorithmus verwendet wird, um eine digitale Signatur zu erstellen. Der korrespondierende öffentliche Schlüssel in Verbindung mit dem gleichen Hash-Algorithmus wird verwendet, um die digitale Signatur zu validieren. Digitale Signaturen bieten Datenintegrität (siehe 5.3.3), Authentifizierung (siehe 5.3.4) und Unleugbarkeit (siehe 5.3.5). Asymmetrische Kryptografie darf auch zur Schlüsselvereinbarung verwendet werden. Dabei können zwei oder mehr Einheiten einen Schlüssel in einer Weise vereinbaren, dass beide Einfluss auf das Ergebnis haben, zum Beispiel unter Einsatz des Diffie-Hellman-Verfahrens ([1]). Diese verschiedenen Algorithmen mit öffentlichem Schlüssel werden durch einen Objektbezeichner identifiziert.

Bestimmte Algorithmen mit öffentlichem Schlüssel, die auf der RSA-Technologie basieren (siehe z. B. [25]), dürfen zur Verschlüsselung und Entschlüsselung eingesetzt werden. Daten, die mit dem privaten Schlüssel verschlüsselt wurden, dürfen mit dem öffentlichen Schlüssel entschlüsselt werden und umgekehrt.

Während grundlegende funktionale Unterschiede zwischen asymmetrischer RSA-Kryptografie und symmetrischer Kryptografie bestehen, ist kein Kryptografietyp grundsätzlich stärker als der andere. Ihre unterschiedlichen Eigenschaften bewirken, dass sie für verschiedene Zwecke verwendet werden, und sie können sich oft gegenseitig ergänzen. Jedoch weist jeder eine ausgeprägte Reihe an Eigenschaften auf, einschließlich der Berechnungskomplexität und der Schlüssellänge, die bei spezifischen Anwendungen Erwägungen bezüglich der Leistungsfähigkeit hervorrufen. Die asymmetrische Kryptografie, die bei der

praktischen Umsetzung von Systemen der Energietechnik verwendet wird, tendiert dazu, rechenintensiver als vergleichbar starke symmetrische Kryptografie zu sein. Diese verschiedenen Eigenschaften der Leistungsfähigkeit führen also zur Verwendungsauswahl, obwohl der spezifische Algorithmus, die Konfiguration und die Plattformwahl die Gesamt-Leistungsfähigkeit ebenfalls stark beeinflussen können. Aus diesem Grund wird die rechenintensive RSA-Kryptografie mit asymmetrischem Schlüssel oftmals nur zum Austausch der symmetrischen geheimen „Sitzungs“-Schlüssel eingesetzt, die dann während einer „Sitzung“ zur schnellen Verschlüsselung und Entschlüsselung aller Nachrichten verwendet werden können.

Die Robustheit eines kryptografischen Algorithmus wird in seiner Sicherheitsstärke ausgedrückt, gemessen in einer Bit-Anzahl, die den erwarteten Aufwand zum Brechen des Algorithmus widerspiegelt.

5.3 Verwendungsmöglichkeiten der Kryptografie

5.3.1 Ziele der Cybersicherheit

Cybersicherheit fokussiert darauf, Hauptbedrohungen entgegenzuwirken. Dazu gehören die folgenden Funktionalitäten:

- Sicherstellen, dass die Befehls- und Datenquelle authentifiziert ist.
- Sicherstellen, dass der Zugriff auf Ressourcen und Daten autorisiert ist.
- Sicherstellen der Datenintegrität.
- Sicherstellen, dass Systemsteuerung und Änderungen authentifiziert und autorisiert sind.
- Verhindern, dass vertrauliche Daten offengelegt werden.
- Verhindern von Unleugbarkeit (Verlust der Verantwortlichkeit).
- Verhindern von Dienstverweigerung (Verfügbarkeit).

Traditionellerweise adressiert Cybersicherheit die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) (en: confidentiality, integrity, availability). Für den Betrieb von Systemen der Energietechnik jedoch hat der kontinuierliche sichere und zuverlässige Betrieb des Systems oberste Priorität. Die höchste Priorität liegt daher auf den ersten drei Punkten: Authentifizierung der Datenquelle, Zugriffsautorisierung und Schutz der Integrität, während Vertraulichkeit und Unleugbarkeit für bestimmte Interaktionen wichtig sein können.

Kryptografie kann dabei helfen, die meisten dieser Bedrohungen zu adressieren, hauptsächlich aber die ersten fünf. Zur Verhinderung von Dienstverweigerung sind normalerweise Konstruktionsauslegungen und -strategien notwendig. Daher werden bei der praktischen Umsetzung von Systemen der Energietechnik fünf Hauptziele bei der Verwendung von Kryptografie berücksichtigt:

- Bestätigung der vom Absender der Nachricht behaupteten Identität (Authentifizierung).
- Überprüfung, dass der Absender das Recht hat, auf die angeforderten Daten zuzugreifen (Autorisierung).
- Versicherung, dass niemand die Nachricht während der Übermittlung gefälscht hat (Integrität).
- Verdecken der Nachrichteninhalte vor unerwünschten Empfängern (Vertraulichkeit).
- Assoziation spezifischer Aktionen mit der Einheit, die diese durchgeführt hat (Unleugbarkeit).

Diese kryptografischen Maßnahmen werden in 5.3.2 bis 5.3.6 behandelt. Die Reihenfolge dieser Unterabschnitte bedeutet keine Priorität bei Anwendungen für Systeme der Energietechnik: In solchen Umgebungen hat die Vertraulichkeit üblicherweise eine der niedrigeren Prioritäten unter diesen kryptografischen Zielen. Jedoch bauen einige der kryptografischen Mechanismen zur Erreichung dieser Ziele aufeinander auf, und daher sind die Ziele zur Erleichterung der konzeptuellen Erklärung in der folgenden Reihenfolge dargestellt.

5.3.2 Vertraulichkeit

Das kryptografische Ziel der Datenvertraulichkeit bei der praktischen Umsetzung von Systemen der Energietechnik wird typischerweise durch die Verschlüsselung der Nachricht unter Verwendung von Kryptografie mit symmetrischem Schlüssel erreicht. Die Nachricht darf individuell auf Anwendungsebene,

dem zugrunde liegenden Kommunikationskanal oder möglicherweise beidem verschlüsselt werden. Wie zuvor angegeben, hängt die Vertraulichkeit dieser Nachricht vom Absender und Empfänger ab, die die Geheimhaltung des Verschlüsselungsschlüssels aufrechterhalten. Zusätzlich wird die asymmetrische Kryptografie oftmals verwendet, um symmetrische Sitzungsschlüssel auszuhandeln und auszutauschen, die für eine bestimmte Zeitspanne gültig sind, wodurch das mit der Geheimhaltung eines spezifischen Sitzungsschlüssels verbundene Risiko verringert wird.

5.3.3 Datenintegrität

Die Datenintegrität beinhaltet die Erkennung unautorisierter Datenveränderung. Jegliche Veränderungen der Daten bei der Durchquerung der Kommunikationsnetze sollten vom Empfänger erkannt werden. Um Verletzungen der Integrität der empfangenen Daten zu erkennen, werden kryptografische Hash-Funktionen (z. B. SHA256) eingesetzt.

Das kryptografische Ziel der Nachrichtenintegrität bei der praktischen Umsetzung von Systemen der Energietechnik wird typischerweise durch Verwendung einer anderen Art kryptografischer Algorithmen erreicht, dem HMAC (verschlüsselter Hash-Nachrichtenauthentifizierungscode), einer kryptografischen Hash-Funktion in Verbindung mit einem geheimen symmetrischen kryptografischen Schlüssel. Das Ergebnis ist eine verschlüsselte Hash-Funktion, z. B. HMAC, die nicht nur die Datenintegrität sicherstellt, sondern auch die Datenquelle validiert.

Anstelle von symmetrischer Kryptografie darf der Absender alternativ eine digitale Signatur an die Nachricht anhängen, die zusätzliche kryptografische Bindungsinformationen zur Datenquelle enthält (siehe 5.3.5).

5.3.4 Authentifizierung

Wenn Einheiten, namentlich Feldgeräte, Softwareanwendungen, Automatisierungssysteme und die Nutzer, die mit diesen interagieren, Daten austauschen müssen, ist es von wesentlicher Bedeutung, dass die Quelle dieser Daten authentifiziert wird. Um eine zuverlässige Authentifizierung zu erreichen, werden Datenquellen mit kryptografischen Schlüsseln ausgestattet, die es ihnen gestatten, ihre Identität gegenüber den Empfängern der Daten zu beweisen. Zur Authentifizierung dieser Einheiten als Datenquellen können Zertifikate mit öffentlichem Schlüssel und asymmetrische kryptografische Verfahren eingesetzt werden.

5.3.5 Unleugbarkeit

Unleugbarkeit bezeichnet die Fähigkeit, eine Aktion (z. B. einen Befehl oder eine Nachricht) unwiderlegbar an eine ausgebende Einheit zu binden. Sie darf einen Absender an den Versand einer bestimmten Nachricht oder einen Empfänger an den Empfang einer bestimmten Nachricht binden. Dies wird durch den Einsatz von Zertifikaten mit öffentlichem Schlüssel und asymmetrischer Kryptografie erreicht. Ein Zertifikat mit öffentlichem Schlüssel ist eine digital signierte Bescheinigung, die behauptet, dass ein öffentlich-privates Schlüsselpaar mit einer eindeutigen Einheit verbunden ist. Empfänger einer signierten Nachricht können nachweisen, dass eine Nachricht von ihrem Urheber versendet wurde, da angenommen wird, dass sich nur der Urheber im Besitz des privaten Schlüssels zur Erzeugung der Signatur befindet. Wird die Unleugbarkeit des Empfangs gefordert, muss der Empfänger eine Kopie der empfangenen Nachricht signieren und an die Einheiten, die einen Nachweis benötigen, zurücksenden. Typischerweise wird solchen signierten Nachrichten ein Zeitstempel hinzugefügt, da ein Signierer anderenfalls die Nachricht anfechten könnte, indem er einfach behauptet, dass der geheime Schlüssel nicht länger geheim ist.

5.3.6 Vertrauen

Ein wichtiger Teil der Sicherung digitaler Kommunikation ist der Bedarf nach Vertrauen. Einheiten (Systeme oder Geräte) sollten nur Daten von Einheiten annehmen (kommunizieren), die sie authentifizieren und denen sie vertrauen können (siehe 5.3.4). Zertifikate mit öffentlichem Schlüssel bieten eine solche Vertrauensbasis, indem sie die Verbindung eines Zertifikats mit öffentlichem Schlüssel mit einer eindeutigen Einheit bestätigen. Vertrauen in ein bestimmtes Zertifikat mit öffentlichem Schlüssel wird durch Validierung eines sogenannten Zertifizierungspfads hergestellt. Dieser hat seinen Ursprung in einem Vertrauensanker, dem die validierende Einheit, auch vertrauende Partei genannt, vertraut. Ein Zertifizierungspfad ist eine Kette von Zertifikaten mit öffentlichem Schlüssel, die mit dem vom Vertrauensanker signierten Zertifikat beginnt und mit dem zu

validierenden Zertifikat endet. Die Begriffe vertrauende Partei, Vertrauensanker und Zertifizierungspfad werden in Abschnitte 6, 7.5 und 7.7 von ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016) näher beschrieben.

In manchen Fällen darf das Vertrauen direkt zwischen einem Vertrauensanker und der vertrauenden Partei hergestellt werden. Es kann jedoch eine Vertrauenskette hergestellt werden. Wenn eine vertrauende Partei ein Zertifikat mit öffentlichem Schlüssel von einer Einheit erhält, mit der sie ein Vertrauensverhältnis aufgebaut hat, darf dieses Zertifikat mit öffentlichem Schlüssel validiert werden, ohne den kompletten Zertifizierungspfad zu durchlaufen. Das Vertrauen wird stattdessen durch die Vertrauenskette hergestellt. In diesem Fall ist es zulässig, dass das Zertifikat mit öffentlichem Schlüssel nicht durch den Vertrauensanker ausgestellt und signiert wird, sondern durch eine Zertifizierungsstelle signiert wird, die eine Vertrauenskette zum Vertrauensanker hergestellt hat.

Bei praktischen Umsetzungen von Systemen der Energietechnik könnten Zertifizierungsstellen die entsprechende organisatorische Einheit innerhalb einer Firma, die Firma selbst, eine Regierungseinheit oder ein akzeptierter Dritter sein.

Digitale Zertifikate mit öffentlichem Schlüssel haben eine endliche Gültigkeitsdauer, nach der sie verfallen. Das Vertrauen kann auch im Fall einer Kompromittierung entzogen werden. Das Management von Zertifikaten mit öffentlichem Schlüssel ist mit dem Management kryptografischer Schlüssel eng verwandt und ist daher in dieser Norm enthalten. Siehe 6.5

6 Konzepte zum Schlüsselmanagement und Verfahren beim Betrieb von Systemen der Energietechnik

6.1 Sicherheitspolitik für das Schlüsselmanagementsystem

Kryptografische Schlüssel müssen geschützt werden. Jede Organisation sollte daher eine Sicherheitspolitik für ihr Schlüsselmanagementsystem entwickeln, die alle Anforderungen aufstellt und festlegt, die dem Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Quellauthentifizierung aller von der Organisation verwendeten kryptografischen Schlüssel und Metadaten dienen. Diese Schutzanforderungen sollten den gesamten Lebenszyklus der Schlüssel abdecken und beinhalten, wann sie im Betrieb sind, gespeichert und transportiert werden. Eine Sicherheitspolitik für das Schlüsselmanagement sollte ebenfalls die Auswahl aller kryptografischen Mechanismen und Protokolle enthalten, die überall in den Systemen der Organisation verwendet werden.

Schlüsselmanagementsysteme benötigen ebenfalls administrative Sicherheitsunterstützung, um sicherzustellen, dass die Sicherheitsrichtlinien befolgt und die Abläufe aufrechterhalten werden. Die Spezifikation dieser Unterstützung liegt nicht im Anwendungsbereich dieses Dokumentes, kann aber in anderen Dokumenten wie zum Beispiel ISO/IEC 11770 ([8]) oder NIST SP 800-130 ([13]) gefunden werden.

6.2 Entwurfsprinzipien des Schlüsselmanagements beim Betrieb von Systemen der Energietechnik

Kryptografische Schlüssel mit ausgewählten kryptografischen Funktionen können zur Sicherung von Nachrichten zwischen verschiedenen Einheiten eingesetzt werden, wie zum Beispiel Nutzern, Systemen, Softwareanwendungen, Kommunikationsknoten und der potenziell großen Anzahl von Einheiten und Geräten, die sich oft an entfernten und oftmals nicht vertrauenswürdigen Stellen befinden.

Diese kryptografischen Schlüssel sollten verwaltet werden, so dass sie den Einheiten, die einen sicheren Datenaustausch erfordern, effektiv und sicher bereitgestellt werden können. Dieses Schlüsselmanagement muss viele Themen berücksichtigen, von den Möglichkeiten der Einheiten, über die verschiedenen Ortstypen dieser Einheiten, dem Timing zur Bereitstellung und Sperrung von Schlüsseln bis hin zum Schutz der Vorgänge des Schlüsselmanagements selbst vor Angriffen.

Viele kleinere Geräte sind beispielsweise in ihrer Rechenleistung und Speicherkapazität beschränkt, während die Kommunikationsnetze ebenfalls in ihrer verfügbaren Bandbreite beschränkt sein können. Daher sind einige Schlüsselmanagementtechniken, die in traditionellen Systemen der Informationstechnologie in Unternehmen mit leistungsstarken Systemen und Kommunikation mit hoher Bandbreite verwendet werden,

nicht gut geeignet für die Automatisierungs- und Kommunikationsumgebungen von Systemen der Energietechnik.

Um diese Nebenbedingungen zu adressieren, legt dieses Dokument verschiedene Schlüsselmanagement-techniken fest, die bei unterschiedlichen Anforderungen und Einschränkungen verwendet werden könnten. Insbesondere legt es fest, wie die Schlüssel für die in den anderen Teilen von IEC 62351 festgelegten kryptografischen Funktionen zu verwalten sind. Beratungsquellen zu den Entwurfsprinzipien des Schlüsselmanagements enthalten:

- Verweisung [8] ISO/IEC 11770-1:2010, *Information technology – Security techniques – Key management – Part 1: Framework*, 6.1.2, D-3.4.
- Verweisung [10] ISO/IEC 11770-3:2008, *Information technology – Security techniques – Key management – Part 3: Mechanisms Using Asymmetric Techniques*.
- Verweisung [15] NIST 800-57, Part 1, 8.1.4 und 8.1.5.

6.3 Verwendung von Transportschicht-Sicherheit (TLS)

Dieser Teil von IEC 62351 verwendet die Definition von Transportschicht-Sicherheit aus RFC 5246. Einzelheiten zur Verwendung von TLS in Systemen der Energietechnik sind in IEC 62351-3 festgelegt.

6.4 Gebrauch kryptografischer Schlüssel

Kryptografische Schlüssel werden für verschiedene Zwecke und in unterschiedlichen Phasen des Produktlebenszyklus verwendet und wie folgt angewandt:

- Digitale Zertifikate und korrespondierende private Schlüssel: werden verwendet, um Einheiten in einer Öffentlichen-Schlüssel-Infrastruktur(PKI)-Umgebung zu authentifizieren.
- Vorher vereinbarte Schlüssel (z. B. zur Echtzeitkommunikation): werden als gemeinsames Geheimnis zwischen Einheiten verwendet, um gegenseitige Authentifizierung zwischen ihnen aufzubauen. Dies kann in Nicht-PKI-Umgebungen von Nutzen sein. Dieses Schema darf außerdem während der PKI-Anmeldung verwendet werden, um es einer Einheit zu gestatten, sich gegenüber der Zertifizierungsstelle (CA) zu authentifizieren, wenn zum Beispiel eine Zertifikatsignierungsanforderung (CSR) durchgeführt wird. *Konstruktions-Werkzeuge könnten die Erzeugung des Registrierungspasswortes der Einheit automatisieren. Optionen zur Passwortkomplexität sind durch die Sicherheitspolitik und die von der CA unterstützten Möglichkeiten gegeben.*
- Geheime Sitzungsschlüssel (paarweise oder gruppenbasiert): werden zur effizienten Verschlüsselung oder für Integritätsprüfungen von Kommunikationsnachrichten verwendet.
- Sitzungsparameter (dedizierte kryptografische Algorithmen): werden zur Unterstützung von Sitzungen verwendet (Schlüssel, Lebensdauer usw.).
- Kryptografische Zugangs-Token: werden zumeist verwendet, um Autorisierung/Zugang von Ressourcen auf Einheiten für eine begrenzte Dauer zu übertragen/bereitzustellen.
- Andere relevante Referenzen der Einheiten oder Organisationen.

6.5 Vertrauen durch eine Öffentliche-Schlüssel-Infrastruktur (PKI)

6.5.1 Registrierungsstellen (RA)

In PKI-basierten Systemen müssen die Einheiten zuerst ihre Identität durch eine Registrierungsstelle (RA) nachweisen. RAs dürfen die individuelle Identität von Personen anhand von Geburtsurkunden, Pässen oder anderen offiziellen Dokumenten feststellen. Bei Systemen und Geräten dürfen RAs die Identität einer Einheit anhand eines vom Hersteller ausgestellten digitalen Zertifikats oder eines eindeutigen Einmal-Passworts (OTP) (en: one-time password) feststellen.

6.5.2 Zertifizierungsstelle (CA)

Nachdem seine Identität festgestellt wurde, muss ein System oder Gerät von einer Zertifizierungsstelle (CA) an ein Zertifikat gebunden werden. Der Hersteller erstellt eine Zertifikatsignierungsanforderung (CSR) für die Einheit und signiert sie digital. Die CA überprüft die CSR und stellt anhand der in der CSR enthaltenen Daten ein digitales Zertifikat aus. CAs stellen eine vertrauenswürdige Verbindung zwischen dem öffentlichen Schlüssel der Einheit und den Metadaten des Zertifikats mit öffentlichem Schlüssel her, indem der öffentliche Schlüssel der Einheit kryptografisch an die Metadaten gebunden wird (d. h. die digitale Signatur der CA wird anhand der Kombination von öffentlichem Schlüssel und Metadaten berechnet). Dieses digitale Zertifikat bindet daher die Identität der Einheit an ihren öffentlichen Schlüssel, so dass jetzt eine vertrauenswürdige Kombination von öffentlichem/privatem Schlüssel besteht, die von der Einheit zum Informationsaustausch mit anderen Einheiten verwendet werden kann. Das Vertrauen in den Schlüssel der Einheit beruht daher auf dem Vertrauen in die Gültigkeit des Schlüssels der CA (siehe 6.5.3).

CAs dürfen entweder durch eine Organisation selbst betrieben werden, was eine geschlossene, durch die Organisation kontrollierte Kommunikationsgruppe ermöglicht, oder durch einen Dritten (Dienstanbieter, Systembetreiber oder Netzmanager), der öffentlich akzeptiert wird und somit ein größeres Vertrauen genießt. Dritt-CAs erfordern ein sicheres Verfahren, um die gültige Identität jeder neuen Einheit zu garantieren; diese kann von der persönlichen Bestätigung für Menschen über die Validierung einer Wirtschaftseinheit bis hin zu Sicherheitsketten für digitale Zertifikate reichen, die zuvor überprüfte digitale Zertifikate mit neuen digitalen Zertifikaten verbinden.

6.5.3 Zertifikate mit öffentlichem Schlüssel

Ein Zertifikat mit öffentlichem Schlüssel (auch digitales Zertifikat) ist ein digitales Dokument, das die Identität einer Einheit an das öffentlich-private Schlüsselpaar dieser Einheit bindet. Wie in 6.5.2 vermerkt, wird diese Bindung anhand einer digitalen Signatur der ausstellenden CA verifiziert. Außer dem öffentlichen Schlüssel und der Identität des Besitzers des Zertifikats mit öffentlichem Schlüssel enthält das Zertifikat mit öffentlichem Schlüssel auch verifizierte Informationen zur Gültigkeitsdauer und zur Identität des Ausstellers. Ein Zertifikat mit öffentlichem Schlüssel darf Erweiterungen mit zusätzlichen Informationen enthalten. Eine Erweiterung wird durch einen Objektbezeichner identifiziert, der von der Organisation zugeordnet wird, welche die Erweiterung festlegt. Ein Zertifikat mit öffentlichem Schlüssel darf an eine CA ausgestellt werden und wird dann als CA-Zertifikat bezeichnet, oder an einen Anwender und wird dann als Anwenderzertifikat mit öffentlichem Schlüssel bezeichnet.

In einer PKI-Umgebung dürfen Zertifikate mit öffentlichem Schlüssel durch die CA der Organisation, zu der die Einheit gehört, digital signiert werden. In einigen Fällen werden mehrere Zertifikate mit öffentlichem Schlüssel erzeugt, da die Einheit eine Versorgungskette vom Hersteller, über den Vertreiber, den Abnehmer bis zum Installateur, usw. abdeckt. Wurzel-Zertifikate der ausstellenden CA werden – falls verwendet – zum Vertrauensanker. Typischerweise sollten Organisationen nur Wurzel-Zertifikate von CAs, denen sie vertrauen, installieren; dies beinhaltet Zertifikate mit öffentlichem Schlüssel, die von ihrer eigenen CA ausgestellt wurden.

Zertifikate mit öffentlichem Schlüssel und Attribut-Zertifikate sind durch einen Basissatz plus Erweiterungen zum Basissatz definiert. Erweiterungen werden durch ein internationales Objektbezeichner(OID)-Register identifiziert. Siehe 6.5.4.

OIDS werden von verschiedenen Internationalen Normen zugeordnet, einschließlich ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), und dürfen zum privaten Gebrauch registriert werden. Die OID-Namensraum-(Wurzel-)Werte für IEC 62351 sind 1.0.62351 und 1.2.840.10070. IEC TS 62351-8 verwendet letzteren Ansatz, um Zugangs-Token (Autorisierungen) festzulegen. Dieser Teil von IEC 62351 und jeder neue zukünftige Teil von IEC 62351 sollte den ersten OID (1.0.62351) verwenden.

6.5.4 Attribut-Zertifikate

Attribut-Zertifikate bieten eine effektive Möglichkeit, das Identitätsmanagement vom Management identitätsgebundener Autorisierungen zu trennen. Eine vollständige Trennung kann durch das Management von Zertifikaten mit öffentlichem Schlüssel mit einer PKI und von Attribut-Zertifikaten mit einer „privilegierten Management-Infrastruktur“ (die die gleiche CA-Technologie wie eine PKI verwendet) erreicht werden.

Wie in Bild 1 dargestellt, können Attribut-Zertifikate zur Erweiterung der Informationen in einem Zertifikat mit öffentlichem Schlüssel verwendet werden. Sie ermöglichen zum Beispiel die temporäre Ausweitung der Berechtigungen des Inhabers eines Zertifikats mit öffentlichem Schlüssel durch spezifische, rollenbasierte Zugangsinformationen. Dieser Ansatz wird in IEC TS 62351-8 eingesetzt.

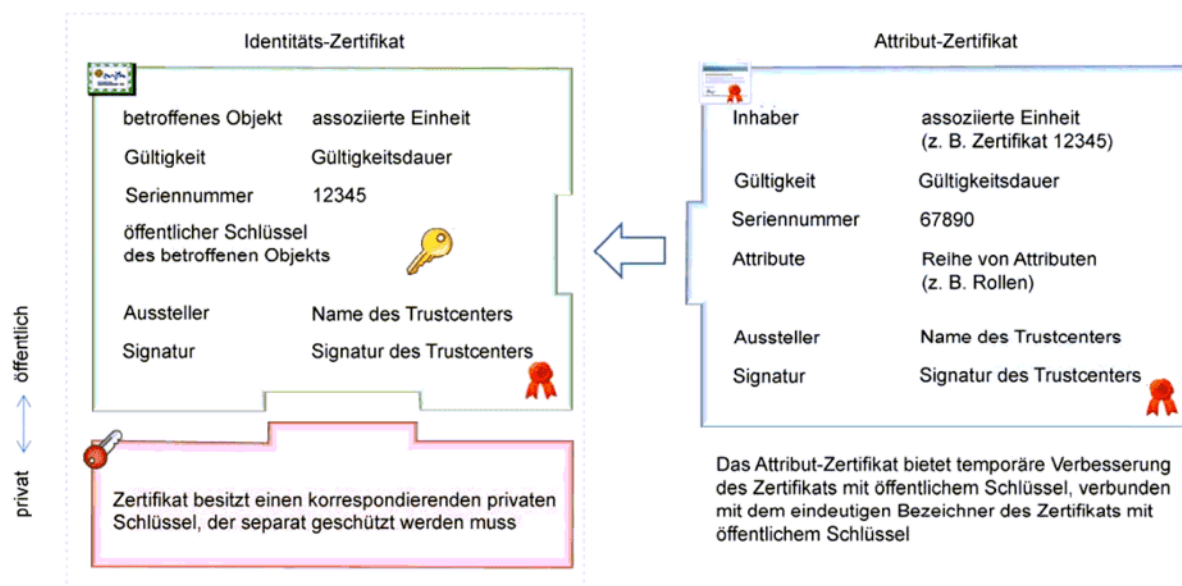


Bild 1 – Beziehung zwischen Zertifikaten mit öffentlichem Schlüssel und Attribut-Zertifikaten

6.5.5 Erweiterungen in Zertifikaten mit öffentlichem Schlüssel und Attribut-Zertifikaten

Sowohl Zertifikate mit öffentlichem Schlüssel als auch Attribut-Zertifikate dürfen optional Erweiterungen enthalten. Solche Erweiterungen liefern zusätzliche Informationen.

Ein Erweiterungstyp besteht aus einem Objektbezeichner (siehe 7.6), der den Typ der Erweiterung identifiziert und die Syntax für die zugehörige Information festlegt. Außerdem enthält er einen Booleschen Wert, der angibt, ob eine bestimmte Erweiterung als kritisch oder nicht kritisch markiert ist. Ist eine Erweiterung als kritisch markiert, kann sie nicht ignoriert werden und das Zertifikat mit öffentlichem Schlüssel oder das Attribut-Zertifikat sollte als ungültig erachtet werden, wenn die vertrauende Partei diesen Erweiterungstyp nicht unterstützt. Ist die Erweiterung als nicht-kritisch markiert, darf die vertrauende Partei die Erweiterung ignorieren, wenn der Erweiterungstyp nicht unterstützt wird. Für detailliertere Informationen siehe 7.3 von ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016).

ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016) legt verschiedene allgemeine nutzbare Erweiterungen fest. IEC TS 62351-8 legt die Erweiterung `IECUserRoles` fest, die für Systeme der Energietechnik definiert wurde, um die rollenbasierte Zugangskontrolle zu ermöglichen.

6.6 Vertrauen durch selbstsignierte Nicht-PKI-Zertifikate

Selbstsignierte Zertifikate spielen in einer PKI eine wichtige Rolle. Vertrauenshierarchien oder Vertrauensketten in PKIs sind durch „Wurzel-Zertifikate“ verwurzelt (siehe 6.5.3). PKI-Wurzel-Zertifikate dürfen selbstsignierte Zertifikate sein, die als Vertrauensanker bekannt sind und von vertrauenswürdigen CAs erstellt wurden, die die Verteilung dieses Vertrauens zulassen.

Um Vertrauen zu schaffen, dürfen unter bestimmten Umständen selbstsignierte Nicht-PKI-Zertifikate leichter implementiert werden als die komplexeren signierten PKI-Zertifikate. Dies darf insbesondere bei kleineren Entwicklungen mit nur einer begrenzten Zahl an Einheiten der Fall sein. Selbstsignierte Zertifikate sind öffentliche/private Schlüsselpaare, die intern durch eine Einheit erzeugt wurden und bei denen der private Schlüssel zum Signieren des eigenen öffentlichen Schlüssels der Einheit verwendet wird, zusammen mit zusätzlichen Informationen wie zum Beispiel dem Namen des betroffenen Objektes, der Gültigkeitsdauer usw. Um auf dieselbe Weise wie PKI-basierte Zertifikate verwendet werden zu können, z. B. zur

Authentifizierung von Interaktionen bei TLS-Verbindungen, werden selbstsignierte Zertifikate mit öffentlichem Schlüssel benötigt, um der in ISO/IEC 9594-8 beschriebenen Struktur der Zertifikate mit öffentlichem Schlüssel zu entsprechen.

Selbstsignierte Zertifikate können im Allgemeinen nicht als vertrauenswürdig angenommen werden. Somit sollten sie, um die Akzeptanz selbstsignierter Zertifikate durch eine begrenzte Gruppe von Einheiten bei der Authentifizierung zu ermöglichen, nur in Verbindung mit Autorisierungs- und Validierungslisten verwendet werden (siehe 6.7).

Die Komplexitätsstufe der Verwendung von einheitenspezifischen selbstsignierten Zertifikaten und Autorisierungs- und Validierungslisten ist vergleichbar mit der Verwendung von vorher vereinbarten Schlüsseln. Selbstsignierte Zertifikate werden je Einheit ausgestellt, während vorher vereinbarte Schlüssel je Verbindungspaar ausgestellt werden. Die Zahl der selbstsignierten Zertifikate ist daher abhängig von der Zahl der Endpunkte, während die Zahl der vorher vereinbarten Schlüssel von der Zahl der Verbindungen zwischen den Endpunkten abhängt.

Da selbstsignierte Zertifikate Zertifikate mit öffentlichem Schlüssel sein müssen, könnte ihre Anwendung den Migrationspfad zu PKI-basierten Implementierungen von Zertifikaten mit öffentlichem Schlüssel öffnen, so dass selbstsignierte Zertifikate leicht durch PKI-basierte Zertifikate ersetzt werden können, sobald diese verfügbar sind.

6.7 Autorisierungs- und Validierungslisten

6.7.1 Allgemeines

Autorisierungs- und Validierungslisten (AVLs), auch Positiv-Listen (en: white lists) genannt, liefern Informationen zu potenziellen Kommunikationseinheiten und möglichen Einschränkungen der Kommunikationen mit solchen Einheiten in einer bestimmten Umgebung. Sie sind in Abschnitt 11 von ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016) festgelegt.

Eine AVL wird von einer Einheit verwendet, wenn diese Einheit als vertrauende Partei agiert. Eine solche Einheit wird als AVL-Einheit bezeichnet. Eine AVL ist in einem sogenannten Autorisierer enthalten, einer Einheit, die für den Inhalt der AVL verantwortlich ist, d. h. die AVL-Einheit vertraut dem Autorisierer, dass dieser gültige Informationen bereitstellt. Eine AVL wird vom ausstellenden Autorisierer signiert.

Die Kommunikation zwischen dem Autorisierer und der AVL-Einheit ist wie jede andere Kommunikation in Bezug auf Integrität, Authentizität und mögliche Vertraulichkeit zu schützen. Um die Validierung der AVLs zu vereinfachen, wird empfohlen, dass ein Autorisierer mit den AVL-Einheiten, denen er dient, eng verwandt ist, z. B. indem er Teil der gleichen Organisation ist, so dass ein Vertrauensverhältnis zwischen dem Autorisierer und den AVL-Einheiten aufgebaut werden darf (siehe 5.3.6).

AVLs dürfen entweder in unbeschränkten oder in beschränkten Umgebungen verwendet werden, wie in 6.7.2 und 6.7.3 beschrieben.

6.7.2 AVLs in unbeschränkten Umgebungen

Eine unbeschränkte Umgebung ist eine Umgebung, in der AVL-Einheiten in der Lage sind, erhaltene Zertifikate mit öffentlichem Schlüssel auf traditionelle Weise zu validieren.

AVLs werden verwendet, um die Kommunikation innerhalb einer festgelegten Menge anderer Einheiten einzuschränken, und dürfen diesen Einheiten Einschränkungen auferlegen, die über die Pfadlänge, Richtlinie und Namensbeschränkung hinausgehen, wie in ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016) näher beschrieben. In 8.3.4 sind solche zusätzlichen, durch AVLs auferlegten Einschränkungen festgelegt.

Die Einheiten, mit denen eine Kommunikation möglich ist, werden in der AVL entweder durch Verweisung auf ihre Zertifikate mit öffentlichem Schlüssel oder durch die Namensstruktur der Organisation, zu der die Einheit gehört, identifiziert.

6.7.3 AVLs in beschränkten Umgebungen

Eine Einheit darf auf verschiedene Weisen beschränkt sein:

- a) Sie ist batteriebetrieben und muss den Rechenaufwand beschränken, um die Leistungsdauer der Batterie zu verlängern.
- b) Sie verfügt über eine geringe Verarbeitungskapazität.
- c) Ihr Kommunikationskanal hat eine begrenzte Bandbreite.
- d) Ihre Speicherkapazität ist begrenzt.
- e) Sie hat strenge Zeitvorgaben, da sie sehr schnell auf Zwischenfälle reagieren muss, wodurch der externen Kommunikation keine Zeit bleibt, erhaltene Zertifikate mit öffentlichem Schlüssel zu validieren.

Zusätzlich zu den Ausführungen in 6.7.2 ist der Autorisierer verantwortlich für die Überprüfung der Gültigkeit und uneingeschränkten Vertrauenswürdigkeit aller Zertifikate mit öffentlichem Schlüssel, die in der AVL vorhanden sind. Es liegt auch im Verantwortungsbereich des Autorisierers, die Informationen über die Gültigkeit der Zertifikate mit öffentlichem Schlüssel in seinen AVLs aktuell zu halten. Der Autorisierer entscheidet außerdem, wann ein abgelaufenes oder gesperrtes Zertifikat mit öffentlichem Schlüssel verwendet oder nicht verwendet werden sollte, wenn dessen Zurückziehen eine kritische Einheit betreffen könnte. Eine AVL-Einheit geht davon aus, dass ein in der Liste aufgeführtes Zertifikat mit öffentlichem Schlüssel gültig ist.

Diese Funktionsweise erfordert die Kommunikation zwischen dem Autorisierer und den CAs, die die in der AVL aufgeführten Zertifikate mit öffentlichem Schlüssel ausgestellt haben.

6.7.4 Verwendung selbstsignierter Zertifikate mit öffentlichem Schlüssel in AVLs

Die Verwendung selbstsignierter Zertifikate mit öffentlichem Schlüssel ist von ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016) nicht anerkannt, wird hier jedoch als zusätzliche Fähigkeit angegeben.

Durch Aufnehmen der selbstsignierten Zertifikate mit öffentlichem Schlüssel in eine AVL übernimmt der Autorisierer die Verantwortung dafür, dass die Verwendung dieser selbstsignierten Zertifikate mit öffentlichem Schlüssel sicher ist, indem er die AVL digital signiert. Auf welche Weise der Autorisierer die Informationen zur Gültigkeit der selbstsignierten Zertifikate mit öffentlichem Schlüssel pflegt, liegt außerhalb des Anwendungsbereiches dieses Teils von IEC 62351.

6.8 Vertrauen durch vorher vereinbarte Schlüssel

Unter besonderen Bedingungen dürfen vorher vereinbarte Schlüssel manuell in den Einheiten installiert werden. Diese vorher vereinbarten Schlüssel, die zuvor zwischen Kommunikationseinheiten geteilte symmetrische Schlüssel sind, dürfen zur Herstellung von Vertrauen bei Peer-to-Peer-Interaktionen und ebenfalls zur Sicherung weiterer Schritte des Schlüsselmanagements verwendet werden. Die vorher vereinbarten Schlüssel, die geheim gehalten werden müssen, müssen durch eine vertrauenswürdige Einheit mittels vertrauenswürdiger Installationsverfahren installiert werden. Eine Anleitung zur Installation vorher vereinbarter Schlüssel ist in NIST SP 800-133 ([14]) angegeben.

6.9 Sitzungsschlüssel

Sitzungsschlüssel werden für eine relativ kurze Dauer verwendet – angeblich für eine „Sitzung“ zwischen zwei Einheiten –, aber in der Realität werden sie dazu verwendet, um sicherzustellen, dass die kryptografischen Schlüssel rechtzeitig ersetzt werden. Dieser Aktualisierungszeitraum hängt im Allgemeinen von der kryptografischen Stärke der Schlüssel und der Dauer, die ein Angreifer zum Brechen des Schlüssels benötigen würde, ab.

Sitzungsschlüssel werden zum Beispiel oftmals in Verbindung mit geheimen Schlüsseln bei Einheiten, die rechenbeschränkt und/oder kommunikationsbeschränkt sind, verwendet. Asymmetrische Kryptografie, die rechenintensiv sein kann, darf periodisch zur Aktualisierung der Sitzungsschlüssel der Einheiten verwendet werden. Diese Sitzungsschlüssel können dann durch diese Einheiten für ein paar Stunden oder sogar ein paar Tage verwendet werden. Üblicherweise ist eine kurze Überlappungsdauer zwischen dem Verfall des