

	DIN EN IEC 62351-4 (VDE 0112-351-4)	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; 35.240.50</p> <p>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</p> <p>Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives (IEC 62351-4:2018); German version EN IEC 62351-4:2018</p> <p>Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 4: Profils comprenant MMS (IEC 62351-4:2018); Version allemande EN IEC 62351-4:2018</p> <p style="text-align: right;">Gesamtumfang 115 Seiten</p> <p style="text-align: center;">DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE</p>		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2018-12-20 angenommene Europäische Norm als DIN-Norm ist 2020-04-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62351-4:2018-10.

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 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.

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.

In diesem Dokument werden folgende Schriftarten verwendet:

- Abstract Syntax Notation One (ASN.1) und W3C XML Schema Definition (W3C XSD) werden in **bold Courier New** dargestellt;
- wenn ASN.1-Typen und -Werte im normalen Text referenziert werden, werden sie vom normalen Text unterschieden, indem sie in **bold 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

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 60870-6-503:2014	IEC 60870-6-503:2014	DIN EN 60870-6-503:2015-04	–
EN 60870-6-702:2014	IEC 60870-6-702:2014	DIN EN 60870-6-702:2015-03	–
EN 60870-6-802:2014	IEC 60870-6-802:2014	DIN EN 60870-6-802:2015-04	–
EN 62351-3:2014 + A1:2018	IEC 62351-3:2014 + A1:2018	DIN EN 62351-3 (VDE 0112-351-3):2019-06	VDE 0112-351-3
EN 62351-9:2017	IEC 62351-9:2017	DIN EN 62351-9 (VDE 0112-351-9):2018-05	VDE 0112-351-9
–	IEC/TS 62351-1	–	–
–	IEC/TS 62351-2	–	–
–	IEC/TS 62351-4:2007 <i>ersetzt durch:</i> IEC 62351-4:2018	–	–
–	IEC/TS 62351-8:2011	–	–
–	ISO 8601:2004	DIN ISO 8601:2006-09	–
–	ISO 9506-2:2003	–	–
–	ISO/IEC 8073:1997	–	–
–	ISO/IEC 8822:1994	–	–
–	ISO/IEC 8823-1:1994	–	–
–	ISO/IEC 8824-1	–	–
–	ISO/IEC 8825-1	–	–
–	ISO/IEC 8825-4	–	–
–	ISO/IEC 9594-8	–	–
–	ISO/ISP 14226-1:1996 zurückgezogen	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60870-6-503:2015-04, *Fernwirkereinrichtungen und -systeme – Teil 6-503: Fernwirkprotokolle, die mit ISO-Normen und ITU-T-Empfehlungen kompatibel sind – TASE.2-Dienste und -Protokoll* (IEC 60870-6-503:2014); Englische Fassung EN 60870-6-503:2014

DIN EN 60870-6-702:2015-03, *Fernwirkereinrichtungen und -systeme – Teil 6-702: Fernwirkprotokolle, die mit ISO-Normen und ITU-T-Empfehlungen kompatibel sind – Funktionsprofil für den TASE.2-Anwendungsdienst in Endsystemen* (IEC 60870-6-702:2014); Englische Fassung EN 60870-6-702:2014

DIN EN 60870-6-802:2015-04, *Fernwirkereinrichtungen und -systeme – Teil 6-802: Fernwirkprotokolle, die mit ISO-Normen und ITU-T-Empfehlungen kompatibel sind – TASE.2-Objektmodelle* (IEC 60870-6-802:2014); Englische Fassung EN 60870-6-802:2014

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 62351-9 (VDE 0112-351-9):2018-05, *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

DIN ISO 8601:2006-09, *Datenelemente und Austauschformate – Informationsaustausch – Darstellung von Datum und Uhrzeit* (ISO 8601:2004)

Energiemanagementsysteme und zugehöriger Datenaustausch –
IT-Sicherheit für Daten und Kommunikation –
Teil 4: Profile einschließlich MMS und Ableitungen
(IEC 62351-4:2018)

Power systems management and associated
information exchange –
Data and communications security –
Part 4: Profiles including MMS and derivatives
(IEC 62351-4:2018)

Gestion des systèmes de puissance et
échanges d'informations associés –
Sécurité des communications et des données –
Partie 4: Profils comprenant MMS
(IEC 62351-4:2018)

Diese Europäische Norm wurde von CENELEC am 2018-12-20 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: Rue de la Science 23, B-1040 Brüssel

© 2018 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN IEC 62351-4:2018 D

Europäisches Vorwort

Der Text des Dokuments 57/2032/FDIS, zukünftige 1. Ausgabe der IEC 62351-4, 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 62351-4:2018 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): 2019-09-20
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2021-12-20

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 62351-4:2018 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 60870-6-503:2014 ANMERKUNG Harmonisiert als EN 60870-6-503:2014 (nicht modifiziert).

IEC 60870-6-702:2014 ANMERKUNG Harmonisiert als EN 60870-6-702:2014 (nicht modifiziert).

IEC 60870-6-802:2014 ANMERKUNG Harmonisiert als EN 60870-6-802:2014 (nicht modifiziert).

Anhang ZA (normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

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).

ANMERKUNG 1 Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod.), dann gilt die entsprechende EN oder das HD.

ANMERKUNG 2 Aktualisierte Informationen über die in diesem Anhang aufgeführten aktuellen Fassungen der Europäischen Normen sind hier verfügbar: www.cenelec.eu.

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
IEC/TS 62351-1	–	Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues	–	–
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	EN 62351-3	2014
+ A1	2018		+ A1	2018
IEC/TS 62351-8	2011	Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control	–	–
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	EN 62351-9	2017
ISO/IEC 8073	1997	Information technology – Open Systems Interconnection – Protocol for providing the connection-mode transport service	–	–
ISO/IEC 8823-1	1994	Information technology – Open Systems Interconnection – Connection-oriented presentation protocol: Protocol specification	–	–
ISO/IEC 8824-1	–	Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation	–	–
ISO/IEC 8825-1	–	Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	–	–
ISO/IEC 8825-4	–	Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)	–	–

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
ISO 8601	2004	Data elements and interchange formats – Information interchange – Representation of dates and times	–	–
ISO 9506-2	2003	Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification	–	–
ISO/IEC 9594-8	–	Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks	–	–
ITU-T Recommendation X.227	–	Information technology – Open Systems Interconnection – Connection-oriented protocol for the Association Control Service Element: Protocol specification	–	–
+ A1	1995		–	–
IETF RFC 1006	1987	ISO Transport Service on top of the TCP, Version: 3	–	–
IETF RFC 3526	2003	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)	–	–
IETF RFC 5246	2008	The Transport Layer Security (TLS) Protocol Version 1.2	–	–
IETF RFC 5480	2009	Elliptic Curve Cryptography Subject Public Key Information	–	–
IETF RFC 5639	2010	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation	–	–
IETF RFC 5869	2010	HMAC-based Extract-and-Expand Key Derivation Function	–	–
IETF RFC 6120	2011	Extensible Messaging and Presence Protocol (XMPP): Core	–	–
IETF RFC 6122	2011	Extensible Messaging and Presence Protocol (XMPP): Address Format	–	–

Inhalt

Seite

Europäisches Vorwort	2
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	3
1 Anwendungsbereich.....	12
1.1 Allgemeines.....	12
1.2 Code-Komponenten	13
2 Normative Verweisungen	13
3 Begriffe und Abkürzungen.....	14
3.1 Allgemeines.....	14
3.2 Begriffe	14
3.3 Abkürzungen	18
4 In diesem Teil von IEC 62351 behandelte Sicherheitsfragen.....	19
4.1 Kommunikations-Referenzmodelle	19
4.2 Sicherheit von Anwendungs- und Transportprofilen	20
4.3 Kompatibilitätsmodus und nativer Modus	21
4.4 Sicherheitsbedrohungen, denen entgegengewirkt wird.....	21
4.4.1 Allgemeines.....	21
4.4.2 Sicherheitsbedrohungen, denen im Kompatibilitätsmodus entgegengewirkt wird.....	21
4.4.3 Sicherheitsbedrohungen, denen im nativen Modus entgegengewirkt wird	21
4.5 Angriffsverfahren, denen entgegengewirkt wird.....	22
4.5.1 Allgemeines.....	22
4.5.2 Angriffe, denen im Kompatibilitätsmodus entgegengewirkt wird	22
4.5.3 Angriffe, denen im nativen Modus entgegengewirkt wird	22
4.6 Protokollierung	23
5 Spezifische Anforderungen	23
5.1 Spezifische Anforderungen an den Kommunikationsstapel nach ICCP/IEC 60870-6-x.....	23
5.2 Spezifische Anforderungen an IEC 61850.....	24
6 Transportsicherheit	24
6.1 Allgemeines.....	24
6.2 Anwendung der Transportschicht-Sicherheit (TLS).....	24
6.2.1 Allgemeines.....	24
6.2.2 Der Begriff der TLS-Chiffrensammlung.....	24
6.2.3 Wiederaufnahme von TLS-Sitzungen	24
6.2.4 Neuaushandlung von TLS-Sitzungen	25
6.2.5 Unterstützte Anzahl von Vertrauensankern	25
6.2.6 Größe von Zertifikaten mit öffentlichem Schlüssel	25
6.2.7 Bewertungsdauer für den Sperrstatus von Zertifikaten mit öffentlichem Schlüssel.....	25

	Seite
6.2.8 Validierung von Zertifikaten mit öffentlichem Schlüssel	25
6.2.9 Umgang mit Sicherheitsereignissen	26
6.3 T-Sicherheit in einer OSI-Betriebsumgebung	26
6.3.1 Allgemeines	26
6.3.2 TCP-Ports	26
6.3.3 Deaktivierung der TLS	26
6.3.4 Unterstützung von TLS-Chiffrensammlungen	27
6.4 T-Sicherheit in einer XMPP-Betriebsumgebung	28
7 Überblick über die Sicherheit der Anwendungsschicht (informativ)	28
7.1 Allgemeines	28
7.2 Beschreibungstechniken	29
7.2.1 Allgemeines	29
7.2.2 ASN.1 als XML-Schema-Definition	29
7.2.3 W3C XML Schema Definition (W3C XSD)	30
7.2.4 XML-Namensraum	30
8 Verwendung von kryptografischen Algorithmen	30
8.1 Allgemeines	30
8.2 Grundlegende kryptografische Definitionen	30
8.3 Algorithmen mit öffentlichem Schlüssel	31
8.4 Hash-Algorithmen	31
8.5 Signaturalgorithmen	32
8.6 Symmetrische Verschlüsselungsalgorithmen, die nur zur Verschlüsselung verwendet werden	32
8.7 Algorithmen zur authentifizierten Verschlüsselung	33
8.8 Integritätsprüfwert-Algorithmen	33
9 Objektbezeichnervergabe (normativ)	33
10 Allgemeine Anforderungen an die oberen OSI-Schichten (normativ)	34
10.1 Überblick	34
10.2 Allgemeines zu den Anforderungen an die oberen OSI-Schichten	35
10.3 Anforderungen an das Sitzungsprotokoll	35
10.4 Anforderungen an das Darstellungsprotokoll	35
10.4.1 Kontextliste	35
10.4.2 Abstrakte Syntaxen	36
10.4.3 Darstellungs-Benutzerdaten	36
10.4.4 ASN.1-Codierungsanforderungen	37
10.5 Anforderungen an das Assoziationssteuerungsdienstelement(ACSE)-Protokoll	37
10.5.1 Allgemeines	37
10.5.2 Protokollversion	37
10.5.3 Titel	37

	Seite
10.5.4 Verwendung des ASN.1-Datentyps EXTERNAL	38
11 A-Sicherheitsprofil (normativ).....	39
11.1 Spezifische OSI-Anforderungen an das A-Sicherheitsprofil	39
11.1.1 Allgemeines.....	39
11.1.2 Zusätzliche Anforderungen an das Sitzungsprotokoll.....	39
11.1.3 Zusätzliche Anforderung an das Darstellungsprotokoll	39
11.1.4 Zusätzliche ACSE-Anforderungen	39
11.2 MMS-Authentifizierungswert	40
11.2.1 Allgemeines.....	40
11.2.2 MMS-Authentifizierungswert-Datentyp	41
11.2.3 Behandlung der Assoziationsanforderung (AARQ-apdu)	41
11.2.4 Behandlung des Assoziationsergebnisses (AARE-apdu).....	42
12 Modell für Ende-zu-Ende-Anwendungssicherheit.....	42
12.1 Einleitung und allgemeine Architektur.....	42
12.2 Spezifikationen für abstrakte Syntax.....	44
12.2.1 Allgemeines.....	44
13 Ende-zu-Ende-Anwendungssicherheit (normativ)	45
13.1 Assoziationsmanagement.....	45
13.1.1 Allgemeines Konzept	45
13.1.2 UTC-Zeitspezifikation.....	45
13.1.3 Anforderung des Quittungsbetriebs	45
13.1.4 Annahme des Quittungsbetriebs.....	46
13.1.5 Zurückweisung der Assoziation durch das geschützte Protokoll.....	46
13.1.6 Assoziationszurückweisung aufgrund von Sicherheitsproblemen	47
13.1.7 Sicherheitsabbruch des Quittungsbetriebs	47
13.1.8 Sicherheitsabbruch der Datenübertragung.....	47
13.1.9 Abbruch durch geschütztes Protokoll	48
13.1.10 Anforderung der Auflösung einer Assoziation	48
13.1.11 Antwort auf die Anforderung der Auflösung einer Assoziation	49
13.2 Datenübertragungsphase.....	49
13.2.1 Allgemeines.....	49
13.2.2 Unverschlüsselte Datenübertragung.....	49
13.2.3 Verschlüsselte Datenübertragung.....	49
13.3 ClearToken-Datentypen	50
13.3.1 Der Datentyp ClearToken1	50
13.3.2 Der Datentyp ClearToken2	55
13.3.3 Der Datentyp ClearToken3	56
13.4 Festlegungen zur Authentifizierung und zur Integrität	57
13.4.1 Der Datentyp Signature.....	57

	Seite
13.4.2 Der Datentyp Authenticator	57
14 Umgang mit E2E-Sicherheitsfehlern (normativ)	57
14.1 Allgemeines	57
14.2 Festlegung der Diagnose	58
14.2.1 Quittungsbetriebdiagnose	58
14.2.2 Datenübertragungsdiagnose	59
14.3 Überprüfung der Anforderung und Annahme des E2E-Sicherheits-Quittungsbetriebs	60
14.3.1 Allgemeines	60
14.3.2 Überprüfung der Signatur	60
14.3.3 Überprüfung der Identität des geschützten Protokolls	60
14.3.4 Überprüfung von ClearToken1	60
14.4 Überprüfung der Sicherheitsprotokoll-Steuerinformationen während der Datenübertragung	62
14.4.1 Allgemeines	62
14.4.2 Überprüfung des Authentifizierers	62
14.4.3 Überprüfungen des Wertes von ClearToken2	62
15 E2E-Sicherheit in einer OSI-Betriebsumgebung	63
15.1 Allgemeines	63
15.2 Zusätzliche Anforderungen an die oberen Schichten	63
15.2.1 Zusätzliche Anforderungen an die Darstellungsschicht	63
15.2.2 Zusätzliche ACSE-Anforderungen	63
15.3 Assoziationsmanagement in einer OSI-Betriebsumgebung	63
15.3.1 Allgemeines	63
15.3.2 Zuordnung zur ACSE-Assoziationsanforderung	64
15.3.3 Zuordnung zur ACSE-Assoziationsantwort	64
15.3.4 Zuordnung zum ACSE-Abbruch	65
15.3.5 Zuordnung zur ACSE-Auflösungsanforderung	66
15.3.6 Zuordnung zur ACSE-Auflösungsantwort	66
15.4 Datenübertragung in einer OSI-Betriebsumgebung	66
15.4.1 Allgemeines	66
15.4.2 Zuordnung der SecPDU für die unverschlüsselte Datenübertragung	66
15.4.3 Zuordnung der SecPDU für die verschlüsselte Datenübertragung	66
15.5 Routing auf den oberen OSI-Schichten	66
15.6 Überprüfung der OSI-Betriebsumgebung	68
15.6.1 Allgemeine Überprüfung	68
15.6.2 Überprüfung der Umgebungszuordnung	68
15.6.3 Diagnosen in der OSI-Betriebsumgebung	69
16 E2E-Sicherheit in einer XMPP-Betriebsumgebung	69
16.1 Allgemeine Informationen zum Wrapping in einer XMPP-Betriebsumgebung	69
16.2 Zuordnung der SecPDUs zu „iq“-Stanzas	70

16.3	Zuordnung der SecPDUs zu „message“-Stanzas.....	71
16.4	Umgang mit XMPP-Stanza-Fehlern.....	71
16.5	XML-Namensräume	72
16.6	Codierung von EnvPDUs in XMPP-Stanzas.....	72
16.7	Mehrfachassoziationen	72
16.8	Überlegungen zur Kollision von Auflösungen	72
17	Konformität mit diesem Dokument.....	72
17.1	Allgemeines.....	72
17.2	Notation	73
17.3	Konformität mit der Betriebsumgebung	73
17.4	Konformität mit den Betriebsmodi.....	73
17.5	Konformität mit dem Kompatibilitätsmodus.....	74
17.6	Konformität mit dem nativen Modus.....	74
Anhang A (normativ)	Formale ASN.1-Spezifikation für das A-Sicherheitsprofil.....	77
Anhang B (normativ)	Formale ASN.1-Spezifikation für Ende-zu-Ende-Sicherheit	78
Anhang C (normativ)	Formale W3C-XSD-Spezifikation für Ende-zu-Ende-Sicherheit.....	84
Anhang D (normativ)	ASN.1-Modul für die OSI-Betriebsumgebung	92
D.1	Anwendungsbereich des Anhangs	92
D.2	ASN.1-Modul.....	92
Anhang E (normativ)	ASN.1-Module und W3C XSDs für eine XMPP-Betriebsumgebung.....	94
E.1	Anwendungsbereich des Anhangs	94
E.2	ASN.1-Module für die XMPP-Betriebsumgebung	94
E.2.1	ASN.1-Modul für den XML-Namensraum urn:ietf:params:xml:ns:xmpp-stanzas	94
E.2.2	ASN.1-Modul für den XML-Namensraum http://www.ietf.org/62351/2018/ENV_4	94
E.3	W3C XSDs für die XMPP-Betriebsumgebung	96
E.3.1	W3C XSD für den XML-Namensraum urn:ietf:params:xml:ns:xmpp-stanzas	96
E.3.2	W3C XSD für den XML-Namensraum http://www.ietf.org/62351/2018/ENV_4	97
Anhang F (normativ)	Vorlage für Spezifikationen einer virtuellen API	99
F.1	Allgemeines.....	99
F.2	ASN.1-Spezifikation für eine virtuelle API.....	100
F.3	W3C-XSD-Spezifikation für eine virtuelle API.....	100
Anhang G (normativ)	Spezifikation des Zertifikats mit öffentlichem Schlüssel der Endeinheit.....	101
G.1	Anwendungsbereich des Anhangs	101
G.2	Allgemeine Anforderung.....	101
G.3	Überlegungen zur Länge.....	101
G.4	Grundlegende Anforderungen und Empfehlungen zur Struktur	101
G.4.1	Komponente für die Version.....	101
G.4.2	Komponente für die Seriennummer	101
G.4.3	Komponente für den Signaturalgorithmus des Ausstellers	102

	Seite
G.4.4 Komponente für den Aussteller	102
G.4.5 Komponente für die Gültigkeit	102
G.4.6 Komponente für das betroffene Objekt	102
G.4.7 Komponente für die Informationen zum öffentlichen Schlüssel des betroffenen Objekts.....	102
G.4.8 Komponenten für die eindeutige ID des Ausstellers und die eindeutige ID des betroffenen Objekts.....	103
G.5 Erweiterungen	103
G.5.1 Allgemeines	103
G.5.2 Erweiterung für den Schlüsselgebrauch.....	103
G.5.3 Überprüfung der Sperre.....	103
G.5.3.1 Allgemeines	103
G.5.3.2 Erweiterung für CRL-Verteilungspunkte.....	103
G.5.3.3 Erweiterung für den Zugriff auf Informationen für zuständige Stellen.....	104
G.5.4 IEC-Erweiterung für Informationen zu Benutzerrollen.....	104
G.6 Spezifische Anforderungen an Betriebsumgebungen.....	104
G.6.1 Allgemeines	104
G.6.2 OSI-Betriebsumgebung	104
G.6.3 XMPP-Betriebsumgebung	104
Anhang H (normativ) Anforderungen an die unteren Schichten der OSI-Betriebsumgebung.....	105
H.1 Anwendungsbereich des Anhangs.....	105
H.2 Transportprotokollklasse 0	105
H.2.1 Vorgabe von zwingenden Längenbeschränkungen	105
H.2.2 Antwort auf TPDU's ohne Unterstützung der Klasse 0	105
H.2.3 Transportselektoren.....	105
H.3 IETF RFC 1006	106
H.3.1 Allgemeines	106
H.3.2 Versionsnummer	106
H.3.3 Länge.....	106
H.3.4 Keep-alive.....	106
Anhang I (informativ) ASN.1-Definition von ACSE	107
Literaturhinweise.....	111
Bilder	
Bild 1 – Anwendungs- und Transportprofile (informativ)	19
Bild 2 – T-Profil mit und ohne TLS-Schutz	26
Bild 3 – Assoziationsaufbau.....	34
Bild 4 – Aufnahme von User-data in die Sitzungs-DATA-TRANSFER-SPDU	37
Bild 5 – E2E-Sicherheitsbausteine	43
Bild 6 – Zusammenhänge zwischen Umgebung, E2E-Sicherheit und geschütztem Protokoll	43
Bild 7 – Beziehungen zwischen APDU's	43

Bild 8 – Anwendungsbereich der E2E-Sicherheitsspezifikation	44
Bild 9 – Routing auf den oberen Schichten	67
Bild F.1 – Konzept der virtuellen API	99

Tabellen

Tabelle 1 – Zusammenhänge zwischen der Sicherheit und der Kombination von Sicherheitsmaßnahmen	20
Tabelle 2 – Kommentierte empfohlene Chiffrensammlungen aus IEC TS 62351-4:2007	27
Tabelle 3 – Kombinationen von Chiffrensammlungen im Kontext dieses Dokuments	28
Tabelle 4 – Zuordnung der SecPDUs zu den ACSE-APDUs	64
Tabelle 5 – Zuordnung der SecPDUs zu XMPP-Stanzas	69
Tabelle 6 – Konformität mit der Betriebsumgebung	73
Tabelle 7 – Konformität mit den Betriebsmodi	74
Tabelle 8 – Konformität mit dem Kompatibilitätsmodus	74
Tabelle 9 – Konformität mit TLS-Chiffrensammlungen im Kompatibilitätsmodus	74
Tabelle 10 – Konformität mit dem nativen Modus	75
Tabelle 11 – Konformität mit den Verschlüsselungsmodi	75
Tabelle 12 – Konformität mit TLS-Chiffrensammlungen im nativen Modus	75
Tabelle 13 – Konformität mit kryptografischen Algorithmen für E2E-Sicherheit	76
Tabelle H.1 – Maximale Größe der TP-Klasse 0	105

1 Anwendungsbereich

1.1 Allgemeines

Dieser Teil von IEC 62351 erweitert den Anwendungsbereich von IEC TS 62351-4:2007 [1]¹ durch das Festlegen eines Kompatibilitätsmodus, der Interoperabilität mit einer auf IEC TS 62351-4:2007 basierenden Implementierung bietet, und durch das Festlegen eines erweiterten Funktionsumfangs, der als „nativer Modus“ bezeichnet wird.

Dieser Teil von IEC 62351 legt Sicherheitsanforderungen auf der Transportschicht und auf der Anwendungsschicht fest. Während IEC TS 62351-4:2007 in erster Linie eine noch eingeschränkte Unterstützung auf der Anwendungsschicht für die Authentifizierung während des Quittungsbetriebs (en: handshake) von Anwendungen auf Grundlage der Festlegung der Nachrichtenformate für Fertigungszwecke (MMS, en: Manufacturing Message Specification) beinhaltet, stellt dieses Dokument außerdem die Unterstützung einer erweiterten Integrität und Authentifizierung sowohl während der Phase des Quittungsbetriebs als auch während der Datenübertragungsphase bereit. Sie ermöglicht die Verwaltung gemeinsam genutzter Schlüssel sowie die Verschlüsselung der Datenübertragung auf der Anwendungsschicht und stellt eine Ende-zu-Ende(E2E)-Sicherheit mit null oder mehr zwischengeschalteten Einheiten bereit. Während IEC TS 62351-4:2007 nur Unterstützung von Systemen beinhaltet, die auf der MMS basieren, d. h. von Systemen, die einen Open Systems Interworking(OSI)-Protokollstapel nutzen, bietet dieses Dokument auch die Unterstützung von Anwendungsprotokollen, die andere Protokollstapel, z. B. eine Internetprotokoll-Suite (siehe 4.1), verwenden. Diese Unterstützung wird für den Schutz von Anwendungsprotokollen erweitert, die eine XML-Codierung verwenden. Diese erweiterte Sicherheit auf der Anwendungsschicht wird als E2E-Sicherheit bezeichnet.

Zusätzlich zur E2E-Sicherheit legt dieser Teil von IEC 62351 auch die Zuordnung zu Umgebungsprotokollen fest, in denen die sicherheitsrelevanten Informationen enthalten sind. Derzeit werden nur OSI- und XMPP-Umgebungen berücksichtigt.

Es ist vorgesehen, dass dieser Teil von IEC 62351 als ein normativer Teil von Normen angesehen wird, die eine sichere Verwendung von Anwendungsprotokollen wie der MMS erfordern.

Es wird davon ausgegangen, dass es Implementierungen gibt, insbesondere Implementierungen des Inter-Control Centre Communications Protocol (ICCP), die von den Spezifikationen des T-Profiles und des A-Sicherheitsprofils nach IEC TS 62351-4:2007 abhängen. In diesem Teil von IEC 62351 sind daher die Spezifikationen nach IEC TS 62351-4:2007 enthalten. Implementierungen, die diese Spezifikationen unterstützen, arbeiten mit Implementierungen nach IEC TS 62351-4:2007 zusammen.

ANMERKUNG Beim A-Sicherheitsprofil handelt es sich streng genommen nicht um ein Profil, der Begriff wird jedoch aus historischen Gründen hier beibehalten.

Dieses Dokument bildet einen Satz verbindlicher und optionaler Sicherheitsspezifikationen, die für den Schutz von Anwendungsprotokollen zu implementieren sind.

Dieses Dokument richtet sich zunächst an die Mitglieder der Arbeitsgruppen, die Protokolle entwickeln oder nutzen. Damit die in diesem Teil von IEC 62351 beschriebenen Maßnahmen angewandt werden können, müssen sie in den Spezifikationen der Protokolle selbst anerkannt und referenziert werden.

Eine weitere Zielgruppe dieses Dokuments sind die Entwickler von Produkten, die diese Protokolle implementieren, und Endanwender, die Anforderungen für ihre eigene Umgebung festlegen möchten.

Teile dieses Dokuments können auch Managern und Führungskräften dabei helfen, Zweck und Anforderungen der Arbeit zu verstehen.

¹ Nummern in eckigen Klammer beziehen sich auf die Literaturhinweise.

1.2 Code-Komponenten

Mit dem Erwerb dieser IEC-Norm erwirbt der Käufer eine Copyright-Lizenz zum Verkauf von Software, die Code-Komponenten dieser Norm enthält, an Endanwender, entweder direkt oder über Vertreiber, im Rahmen der IEC-Software-Lizenzbedingungen, die unter www.iec.ch/CCv1 abrufbar sind.

Die in dieser IEC-Norm enthaltenen Code-Komponenten sind auch als elektronische maschinenlesbare Dateien erhältlich, unter: www.iec.ch/public/tc57/supportdocuments/IEC_62351-4.ASN.1_XSD.full.zip

In diesem Dokument sind Code-Komponenten in den [Anhängen A, B, C, D](#) und [E](#) enthalten.

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 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

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/AMD1:2018

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

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*

ISO/IEC 8073:1997 | Rec. ITU-T X.224 (1995), *Information technology – open systems interconnection – Protocol for providing the connection-mode transport service*

ISO/IEC 8823-1:1994 | Rec. ITU-T X.226 (1994), *Information technology – open systems interconnection – connection-oriented presentation protocol: Protocol specification*

ISO/IEC 8824-1 | Rec. ITU-T X.680, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1 | Rec. ITU-T X.690, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 8825-4 | Rec. ITU-T X.693, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*

ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*

ISO 9506-2:2003, *Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification*

ISO/IEC 9594-8: | Rec. ITU-T X.509, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

Rec. ITU-T X.227 (1995), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification*

ANMERKUNG 1 Die entsprechende internationale Norm ISO/IEC 8650-1:1996 wurde zurückgezogen.

Rec. ITU-T X.227 (1995)/Amd.1 (1996), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification – Amendment 1: Incorporation of extensibility markers*

ANMERKUNG 2 Die entsprechende Änderung der internationalen Norm ISO/IEC 8650-1:1996/Amd.1:1997 wurde zurückgezogen.

IETF RFC 1006:1987, *ISO Transport Service on top of the TCP, Version: 3*

IETF RFC 2104:1997, *HMAC: Keyed-Hashing for Message Authentication*

IETF RFC 3526:2003, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*

IETF RFC 5114:2008, *Additional Diffie-Hellman Groups for Use with IETF Standards*

IETF RFC 5246:2008, *The Transport Layer Security (TLS) Protocol, Version 1.2*

IETF RFC 5480:2009, *Elliptic Curve Cryptography Subject Public Key Information*

IETF RFC 5639:2010, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*

IETF RFC 5869:2010, *HMAC-based Extract-and-Expand Key Derivation Function*

IETF RFC 6120:2011, *Extensible Messaging and Presence Protocol (XMPP): Core*

IETF RFC 6122:2011, *Extensible Messaging and Presence Protocol (XMPP): Address Format*

3 Begriffe und Abkürzungen

3.1 Allgemeines

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>

3.2 Begriffe

3.2.1

a-Sicherheitsprofil

Anwendungssicherheitsspezifikation, die eine Peer-to-Peer-Authentifizierung nach der ursprünglichen Definition in IEC TS 62351-4:2007 bietet

3.2.2

abstrakte Syntax

Festlegung von Anwendungsprotokoll-Dateneinheiten durch Anwendung von Notationsregeln, die von den zu ihrer Darstellung verwendeten Codierungsverfahren unabhängig sind

[QUELLE: ISO/IEC 7498-1:1994 | Rec. ITU-T X.200:1994, 7.1.1.2]

3.2.3

Anwendungskontext

Menge von Regeln, die von zwei Anwendungseinheiten gemeinsam benutzt werden, um eine Assoziation (in einer OSI-Betriebsumgebung) zu betreiben

3.2.4

Anwendungsinstanz

Menge von Fähigkeiten verkörperndes aktives Element, das für Kommunikationssysteme geeignet ist und für die Anwendungsschicht definiert wird

3.2.5

Anwendungsprofil

Anwendungsprofil, das die Protokolle und Vereinbarungen über die oberen drei Schichten des OSI-Referenzmodells repräsentiert

3.2.6

Anwendungsprotokoll-Steuerinformationen

zwischen den Anwendungsinstanzen zur Koordination ihres gemeinsamen Betriebs ausgetauschte Informationen

3.2.7

Assoziation

kooperierende Beziehung zwischen Anwendungsinstanz-Aufrufen, die die Informationskommunikation und die Koordination ihres gemeinsamen Betriebs für einen Zeitpunkt der Kommunikation ermöglicht

Anmerkung 1 zum Begriff: Diese Beziehung kann mittels der Übertragung von Anwendungsprotokoll-Steuerinformationen über einen zugrunde liegenden Dienst hergestellt werden.

[QUELLE: Rec. ITU T X.217:1995, 3.5.1]

3.2.8

Assoziationssteuerungsdienstelement

Anwendungs-Dienstelement, das die alleinigen Mittel für den Aufbau und die Beendigung von Anwendungsassoziationen in einer OSI-Umgebung bereitstellt

3.2.9

bilaterale Vereinbarung

Vereinbarung zwischen zwei Netzleitstellen, die die Datenelemente, auf die zugegriffen wird, und die Mittel für den Zugriff betrifft

[QUELLE: IEC 60870-6-503:2014, 3.3]

3.2.10

bilaterale Tabelle

rechentechnische Darstellung der bilateralen Vereinbarung

Anmerkung 1 zum Begriff: Die verwendete Darstellung ist lokal festzulegen.

[QUELLE: IEC 60870-6-503:2014, 3.4]

3.2.11

CA-Zertifikat

Zertifikat mit öffentlichem Schlüssel, das einer Zertifizierungsstelle (CA) von einer anderen CA oder derselben CA ausgestellt wird

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.14]

3.2.12

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 | Rec. ITU-T X.509:2016, 3.5.21]

3.2.13

Client

Anwendungsinstanz, die den Aufbau einer Assoziation mit einem Server initialisiert

Anmerkung 1 zum Begriff: Der Begriff legt die Rolle einer Instanz für eine bestimmte Assoziation fest. Die Instanz darf eine weitere Rolle für eine andere Assoziation einnehmen.

Anmerkung 2 zum Begriff: XMPP verfolgt einen etwas anderen Client/Server-Ansatz.

3.2.14

Kompatibilitätsmodus

Betriebsmodus, in dem die Partner in einer Assoziation oder beim Aufbau einer Assoziation unter Anwendung derjenigen in diesem Teil von IEC 62351 festgelegten Einrichtungen kommunizieren, welche den Einrichtungen entsprechen, die in IEC TS 62351-4:2007 festgelegt sind

3.2.15

koordinierte Weltzeit

UTC

vom Internationalen Büro für Maß und Gewicht (BIPM, Bureau international des poids et mesures) geführte Zeitskala, die die Grundlage einer koordinierten Verbreitung von Standardfrequenzen und Zeitsignalen bildet

Anmerkung 1 zum Begriff: UTC und GMT (Greenwich Mean Time) sind zwei alternative Zeitstandards, die für die meisten praktischen Zwecke die gleiche Zeit festlegen.

Anmerkung 2 zum Begriff: Festgelegt in Rec. ITU-R TF.460-6.

Anmerkung 3 zum Begriff: ASN.1 hat zwei integrierte Darstellungstypen für UTC, **UTCTime** und **GeneralizedTime**. **UTCTime** hat eine zweistellige Jahresdarstellung, **GeneralizedTime** eine vierstellige.

3.2.16

Datenübertragungsphase

Phase von der Fertigstellung des Aufbaus einer Assoziation bis zu der Initialisierung der Beendigung der Assoziation

Anmerkung 1 zum Begriff: In einigen Spezifikationen wird diese Phase als „Sitzung“ bezeichnet. Diese Bezeichnung wird hier vermieden, da sie in der OSI-Architektur und der TLS für andere Zwecke verwendet wird.

3.2.17

E2E-Sicherheit

Sicherheitseinrichtungen auf der Anwendungsschicht, die mit oder ohne Vertraulichkeit (Verschlüsselung) zwischen zwei Einheiten mit null oder mehr zwischengeschalteten Einheiten Ende-zu-Ende-Authentifizierung der Datenquelle und Ende-zu-Ende-Integrität sicherstellen

3.2.18

Zertifikat mit öffentlichem Schlüssel der Endeinheit

Zertifikat mit öffentlichem Schlüssel, das einer Einheit ausgestellt wird, die dann als eine Endeinheit innerhalb einer Infrastruktur mit öffentlichem Schlüssel dient

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509:2016, 03.05.1931]

3.2.19

Umgebungsprotokoll-Dateneinheit

Anwendungsprotokoll-Dateneinheit (APDU), die Protokollsteuerinformationen für das Umgebungsprotokoll und eine Sicherheitsprotokoll-Dateneinheit beinhaltet

3.2.20

Internetprotokoll-Suite

Netzwerk-Kommunikationsprotokolle und ein Beschreibungssystem, die für das Internet und ähnliche Netzwerke verwendet werden

Anmerkung 1 zum Begriff: Auch als TCP/IP-Suite oder TCP/IP-Modell bezeichnet.

3.2.21

nativer Modus

Szenario, in dem die Partner in einer Assoziation oder dem Aufbau einer Assoziation die E2E-Sicherheit nach diesem Teil von IEC 62351 anwenden und möglicherweise TLS unterstützen

3.2.22

Füllwert

einmal verwendete Zahl, entweder zum Schutz gegen Wiedereinspielungsangriffe oder als Initialisierungsvektor für kryptografische Algorithmen

3.2.23

Präsentationsdatenwert

in der abstrakten Syntax festgelegte Informationseinheit, die von dem zugrunde liegenden Dienst in einer OSI-Betriebsumgebung übertragen wird

3.2.24

geschütztes (Anwendungs-)Protokoll

Anwendungsprotokoll, das durch E2E-Sicherheit geschützt wird

3.2.25

geschützte Protokolldateneinheit

über ein geschütztes Anwendungsprotokoll definierte Anwendungsprotokoll-Dateneinheit (APDU)

3.2.26

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 | Rec. ITU-T X.509 definiert werden.

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

3.2.27

Salt

Zufalls-Zeichenkette, die verwendet wird, um Entropie zu einem anderen, möglicherweise zufälligen Wert hinzuzufügen

Anmerkung 1 zum Begriff: Der Salt kann auch vor dem Hashing mit einem Passwort verkettet werden, um eine Kollision zu vermeiden und gegen eine Wiedereinspielung zu schützen.

3.2.28

sichere Protokolldateneinheit

Anwendungsprotokoll-Dateneinheit (APDU), die Sicherheitsprotokoll-Steuerinformationen und, wenn relevant, eine geschützte Protokolldateneinheit beinhaltet

3.2.29

Server

Einheit, die Assoziationsanforderungen von Clients annimmt

Anmerkung 1 zum Begriff: Der Begriff legt die Rolle einer Einheit für eine bestimmte Assoziation fest. Die Einheit darf eine weitere Rolle für eine andere Assoziation einnehmen.

3.2.30

Transportprofil

Profil, das die Protokolle und Vereinbarungen über die unteren vier Schichten des OSI-Referenzmodells repräsentiert

3.2.31

Vertrauensanker

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

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

3.2.32

XML-Stanza

Eine Stanza ist die grundlegende Bedeutungseinheit in XMPP. Eine Stanza ist ein Element auf erster Ebene (bei Tiefe = 1 des Streams), dessen Elementname „message“, „presence“ oder „iq“ ist und dessen qualifizierender XML-Namensraum „jabber:client“ oder „jabber:server“ ist.

[QUELLE: IETF RFC 6120:2011, 4.1]

3.3 Abkürzungen

Für die Anwendung dieses Dokuments gelten die Abkürzungen nach IEC TS 62351-2 und die folgenden Abkürzungen:

ACSE	Assoziationssteuerungsdienstelement (en: association control service element)
AE	authentifizierte Verschlüsselung (en: authenticated encryption)
APDU	Anwendungsprotokoll-Dateneinheit (en: application protocol data unit)
API	Anwendungsprogramm-Schnittstelle (en: application programming interface)
BER	grundlegende Codierungsregeln (en: Basic Encoding Rules)
CA	Zertifizierungsstelle (en: certification authority)
CBC	Betrieb von Blockchiffren (en: Cipher Block Chaining)
CRL	Zertifikatsperrliste (en: certification revocation list)
DER	besondere Codierungsregeln (en: Distinguished Encoding Rules)
DHE	kurzlebiger Diffie-Hellman (en: Ephemeral Diffie-Hellman)
E2E	Ende-zu-Ende (en: end-to-end)
ECDHE	kurzlebiger Elliptische-Kurven-Diffie-Hellman (en: Elliptic Curve Ephemeral Diffie-Hellman)
EnvPDU	Umgebungsprotokoll-Dateneinheit (en: environment protocol data unit)
GCM	Galois/Counter-Betriebsmodus (en: Galois/Counter Mode)
GMAC	Galois-Nachrichtenauthentifizierungscode (en: Galois Message Authentication Code)
HKDF	HMAC-basierte Extract-and-Expand-Schlüsselableitungsfunktion (en: HMAC-based Extract-and-Expand Key Derivation Function)
HMAC	Schlüssel-Hash-Nachrichtenauthentifizierungscode (en: Keyed-hash Message Authentication Code)
ICCP	Protokoll für die Kommunikation zwischen Netzleitstellen (en: Inter-Control Centre Communications Protocol)

ICV	Integritätsprüfwert (en: integrity check value)
IPSec	Internetprotokoll-Sicherheit (en: Internet Protocol security)
JID	Kennzeichner für Dauerbelegung (en: jabber identifier)
MAC	Nachrichtenauthentifizierungscode (en: message authentication code)
MMS	Festlegung der Nachrichtenformate für Fertigungszwecke (en: Manufacturing Message Specification)
OCSP	Online-Zertifikat Status-Protokoll (en: Online Certificate Status Protocol)
PDU	Protokolldateneinheit (en: protocol data unit)
PDV	Präsentationsdatenwert (en: presentation data value)
PPDU	Darstellungsprotokoll-Dateneinheit (en: presentation protocol data unit)
PrPDU	geschützte Protokolldateneinheit (en: protected protocol data unit)
SecPDU	Sicherheitsprotokoll-Dateneinheit (en: security protocol data unit)
SPDU	Sitzungsprotokoll-Dateneinheit (en: session protocol data unit)
TASE.2	Fernwirk-Anwendungs-Dienstelement 2 (en: Telecontrol Application Service Element 2)
TPDU	Transportprotokoll-Dateneinheit (en: transport protocol data unit)
UTC	koordinierte Weltzeit (en: Coordinated Universal Time)
VPN	virtuelles Privatnetz (en: virtual private network)
XER	XML-Codierungsregeln (en: XML Encoding Rules)
XML	erweiterbare Auszeichnungssprache (en: eXtensible markup language)
XMPP	erweiterbares Nachrichten- und Anwesenheitsprotokoll (en: eXtensible messaging and presence protocol)
XSD	XML Schema Definition (en: XML schema definition)

4 In diesem Teil von IEC 62351 behandelte Sicherheitsfragen

4.1 Kommunikations-Referenzmodelle

In Bild 1 sind das OSI-Referenzmodell und die Beziehung zwischen diesem Modell und einem OSI-Protokollstapel und einer Internetprotokoll-Suite dargestellt.

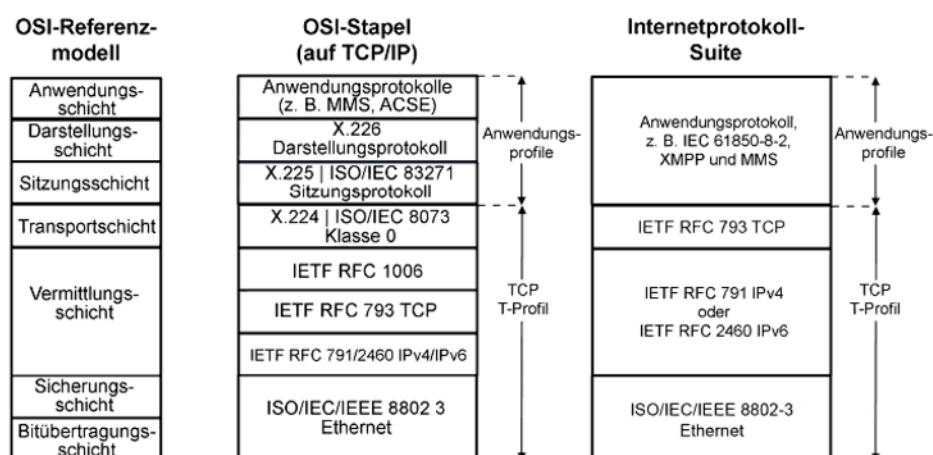


Bild 1 – Anwendungs- und Transportprofile (informativ)

Im Zusammenhang dieses Dokuments und in den meisten anderen Fällen ist der OSI-Stapel ein hybrider Stapel, der auf einem OSI-Stapel basierenden Anwendungen, wie z. B. der Manufacturing Message Specification (MMS), die Kommunikation über ein TCP/IP-basiertes Netzwerk wie das öffentliche Internet ermög-

licht. Die oberen vier Schichten sind OSI-Protokolle, während der OSI-Netzwerkdienst von IETF RFC 1006 auf einem TCP/IP-Stapel bereitgestellt wird.

In der Internetprotokoll-Suite werden die oberen drei OSI-Stapel in einer Anwendungsschicht zusammengeführt.

4.2 Sicherheit von Anwendungs- und Transportprofilen

Im Hinblick auf den für dieses Dokument relevanten Kommunikationsaspekt (siehe Tabelle 1) werden die folgenden Punkte behandelt:

- Transportprofile: Ein Transportprofil (T-Profil) definiert die Protokolle und Anforderungen an die Schichten 1 bis 4 des OSI-Referenzmodells.
- Anwendungsprofile: Ein Anwendungsprofil (A-Profil) definiert die Protokolle und Anforderungen an die Schichten 5 bis 7 des OSI-Referenzmodells.

Dies wird auch in [Bild 1](#) dargestellt.

In diesem Teil von IEC 62351 werden zwei T-Sicherheitsspezifikationen und zwei Anwendungs-Sicherheitspezifikationen unterschieden.

Sicherheitstechnisch wird die T-Sicherheit, falls vorhanden, typischerweise durch die Transportschicht-Sicherheit (TLS) entsprechend der Definition in IETF RFC 5246 bereitgestellt.

Tabelle 1 – Zusammenhänge zwischen der Sicherheit und der Kombination von Sicherheitsmaßnahmen

Anwendungs-sicherheit	A-Sicherheitsprofil	Keine	A-Sicherheitsprofil	E2E-Sicherheit ohne Verschlüsselung	E2E-Sicherheit ohne Verschlüsselung	E2E-Sicherheit mit Verschlüsselung	E2E-Sicherheit mit Verschlüsselung
Transportsicherheit	Keine	TLS	TLS	Keine	TLS	Keine	TLS
Anmerkung	Anmerkung 1	Anmerkung 2		Anmerkung 3		Anmerkung 4	

Für die Anwendung der T-Sicherheit wird davon ausgegangen, dass TLS nach den Festlegungen in 6.3 für die OSI-Betriebsumgebung verwendet wird. Für andere Umgebungen liegt die Verwendung von TLS außerhalb des Anwendungsbereichs dieses Dokuments und wird durch die Referenznorm festgelegt.

Anmerkung 1 Die alleinige Verwendung des A-Sicherheitsprofils ohne TLS führt zu einem unsicheren System.

Anmerkung 2 Die Verwendung von TLS mit oder ohne A-Sicherheitsprofil ergibt eine angemessene Sicherheit unter der Voraussetzung, dass alle anderen Sicherheitsmaßnahmen eingehalten werden, einschließlich der Verwendung von sicheren TLS-Chiffrensammlungen, und dass es sich um eine Peer-to-Peer-Kommunikation ohne zwischengeschaltete Einheiten handelt. Die Verwendung des A-Sicherheitsprofils ermöglicht zusätzlich zu der durch TLS bereitgestellten Authentifizierung die Authentifizierung von Anwendungsinstanzen auf der Anwendungsschicht.

Anmerkung 3 Die Verwendung von E2E-Sicherheit ohne Verschlüsselung mit oder ohne TLS bietet die gegenseitige Authentifizierung und E2E-Integritätsschutz und damit eine angemessene Sicherheit, vorausgesetzt, es besteht keine Vertraulichkeitspflicht und andere Sicherheitsmaßnahmen werden eingehalten. Die Verwendung von TLS bietet Vertraulichkeit (Verschlüsselung) und Integritätsschutz auf Transportschicht-Hops, für den Fall, dass die E2E-Sicherheit kompromittiert sein sollte.

Anmerkung 4 Wie in Anmerkung 3, jedoch mit Ende-zu-Ende-Verschlüsselung (Vertraulichkeit).

ANMERKUNG Wenn in einer ICCP-Umgebung Vertraulichkeit benötigt wird, aber keine Verschlüsselung nach diesem Teil von IEC 62351-4 verwendet wird, wird empfohlen, eine andere Form von Verschlüsselungstechnologie, wie etwa ein VPN, zu verwenden.

4.3 Kompatibilitätsmodus und nativer Modus

In diesem Dokument werden zwei sich gegenseitig ausschließende Betriebsmodi festgelegt, d. h. der Datenaustausch findet ausschließlich in einem der beiden Modi statt:

- a) Der Kompatibilitätsmodus ist ein Betriebsmodus, der mit IEC TS 62351-4:2007 kompatibel ist. Die in diesem Modus für TLS verwendeten Chiffrensammlungen werden in [6.3.4.2](#) festgelegt und die Spezifikation der Anwendungssicherheit ist in [Abschnitt 11](#) enthalten.

Der Betriebsmodus ist für MMS nur in einer OSI-Betriebsumgebung unter Bezug auf ISO 9506-2:2003 und Rec ITU-T X.227:1995 relevant. Dieser Betriebsmodus wird für neue Implementierungen nicht empfohlen.

- b) Der native Betriebsmodus stellt die wichtigste Ergänzung in diesem Dokument dar. Er ermöglicht die erweiterte Unterstützung für TLS nach [6.3.4.3](#) sowie Ende-zu-Ende-Sicherheit zwischen zwei Anwendungsinstanzen mit null oder mehr zwischengeschalteten Anwendungsinstanzen, wie in den [Abschnitten 12 bis 16](#) festgelegt.

4.4 Sicherheitsbedrohungen, denen entgegengewirkt wird

4.4.1 Allgemeines

IEC TS 62351-1 enthält eine Diskussion der Sicherheitsbedrohungen und Angriffsverfahren.

Die aufgeführten Sicherheitsbedrohungen werden durch die Umsetzung der in diesem Dokument aufgeführten Spezifikation/Empfehlungen entschärft.

Welchen Sicherheitsbedrohungen entgegengewirkt wird, hängt davon ab, ob der Kompatibilitätsmodus oder der native Modus verwendet wird.

4.4.2 Sicherheitsbedrohungen, denen im Kompatibilitätsmodus entgegengewirkt wird

Wenn [IEC 62351-3:2018](#) für zu übertragende Daten nicht zur Anwendung kommt, aber das A-Sicherheitsprofil gilt, so wird den folgenden Sicherheitsbedrohungen entgegengewirkt:

- Maskerade beim Assoziationsaufbau.

Wenn [IEC 62351-3:2018](#) angewendet wird, wird zusätzlich zu den vorstehend genannten auch den folgenden Sicherheitsbedrohungen entgegengewirkt:

- Unautorisierte Veränderung (Manipulation) von Informationen, durch Verwendung von digitalen Signaturen und Integritätsprüfwerten (ICV). Letztere werden auch als Nachrichtenauthentifizierungscodes (MAC) bezeichnet.
- Diebstahl oder Missbrauch von Informationen, durch Verwendung von Vertraulichkeit (Verschlüsselung).

4.4.3 Sicherheitsbedrohungen, denen im nativen Modus entgegengewirkt wird

Wenn TLS angewendet wird, wird auf den einzelnen Hops den folgenden Sicherheitsbedrohungen entgegengewirkt:

- Maskerade beim Verbindungsaufbau.
- Unautorisierte Veränderung (Manipulation) von Informationen, durch Verwendung von digitalen Signaturen und Integritätsprüfwerten (ICV).
- Diebstahl oder Missbrauch von Informationen, durch Verwendung von Vertraulichkeit (Verschlüsselung).

Bei E2E-Sicherheit ohne Verschlüsselung wird den folgenden Bedrohungen bei der Ende-zu-Ende-Kommunikation entgegengewirkt:

- Maskerade beim Ende-zu-Ende-Assoziationsaufbau.

- Unautorisierter Veränderung (Manipulation), sowohl während der Phase des Quittungsbetriebs als auch während der Datenübertragungsphase, durch Verwendung von digitalen Signaturen und Ende-zu-Ende-Integritätsprüfwerten (ICV).
- Wiedereinspielung, durch Verwendung von Zeit, Assoziations-ID und Sequenznummern.

Bei E2E-Sicherheit ohne Verschlüsselung wird zusätzlich den folgenden Bedrohungen entgegengewirkt:

- Diebstahl oder Missbrauch von Informationen, durch Verwendung von Ende-zu-Ende-Vertraulichkeit (Verschlüsselung).

4.5 Angriffsverfahren, denen entgegengewirkt wird

4.5.1 Allgemeines

Welchen Angriffsverfahren entgegengewirkt wird, hängt davon ab, ob der Kompatibilitätsmodus oder der native Modus verwendet wird.

4.5.2 Angriffe, denen im Kompatibilitätsmodus entgegengewirkt wird

Die Angriffsverfahren, denen durch die Umsetzung von **IEC 62351-3:2018** wie in diesem Dokument beschrieben entgegengewirkt wird, werden in der folgenden Liste nicht aufgeführt.

- Man-in-the-Middle: Dieser Bedrohung wird durch Authentifizierung entgegengewirkt, und zwar mittels digitaler Signaturen während des TLS-Quittungsbetriebs und mittels ICV während der Datenübertragung.
- Manipulationserkennung/Nachrichtenintegrität: Diesem Angriff wird auf die gleiche Weise entgegengewirkt wie dem Man-in-the-Middle-Angriff.
- Maskerade: Diesem Angriff wird auf die gleiche Weise entgegengewirkt wie dem Man-in-the-Middle-Angriff.

4.5.3 Angriffe, denen im nativen Modus entgegengewirkt wird

Wenn TLS angewendet wird, wird auf den einzelnen Hops den folgenden Angriffen entgegengewirkt:

- Man-in-the-Middle: Dieser Bedrohung wird durch Authentifizierung entgegengewirkt, und zwar mittels digitaler Signaturen während des TLS-Quittungsbetriebs und mittels ICV während der Datenübertragung.
- Manipulationserkennung/Nachrichtenintegrität: Diesem Angriff wird auf die gleiche Weise entgegengewirkt wie dem Man-in-the-Middle-Angriff.
- Maskerade: Diesem Angriff wird auf die gleiche Weise entgegengewirkt wie dem Man-in-the-Middle-Angriff.

Bei E2E-Sicherheit ohne Verschlüsselung wird den folgenden Angriffen bei der Ende-zu-Ende-Kommunikation entgegengewirkt:

- Man-in-the-Middle: Dieser Bedrohung wird durch Authentifizierung entgegengewirkt, und zwar mittels digitaler Signaturen während der Ende-zu-Ende-Assoziation und mittels ICV während der Datenübertragung.
- Manipulationserkennung/Nachrichtenintegrität: Diesem Angriff wird auf die gleiche Weise entgegengewirkt wie dem Man-in-the-Middle-Angriff.
- Maskerade: Diesem Angriff wird auf die gleiche Weise entgegengewirkt wie dem Man-in-the-Middle-Angriff.
- Wiedereinspielung: Diesem Angriff wird durch Verwendung von Zeit und Sequenznummern entgegengewirkt.

Bei E2E-Sicherheit ohne Verschlüsselung wird zusätzlich den folgenden Angriffen entgegengewirkt:

- Diebstahl oder Missbrauch von Informationen, durch Verwendung von Ende-zu-Ende-Vertraulichkeit (Verschlüsselung).

4.6 Protokollierung

Es ist wichtig, dass sicherheitsrelevante Verletzungen in einem eigenen Protokoll aufgezeichnet werden, dessen Inhalt inhärent vor Manipulationen (z. B. der Veränderung oder dem Löschen von Informationen) geschützt ist. Implementierer sollten versuchen, genug Informationen aufzuzeichnen, um Sicherheitsaudits und Verfolgungen zu erleichtern. Wie diese Empfehlung tatsächlich umgesetzt wird, wird jeweils lokal festgelegt.

Relevante Mitteilungen und Definitionen zur Überwachung und Sicherheitsprotokollierung werden in zwei unterschiedlichen Teilen von IEC 62351 angesprochen: **IEC 62351-7** behandelt die Überwachung im Zusammenhang mit der Netzwerkverwaltung und IEC 62351-14 die Sicherheitsprotokollierung.

5 Spezifische Anforderungen

5.1 Spezifische Anforderungen an den Kommunikationsstapel nach ICCP/IEC 60870-6-x

Dieser Abschnitt ist dann relevant und normativ, wenn dieser Teil von IEC 62351 gemeinsam mit dem ICCP, auch bekannt als Fernwirk-Anwendungs-Dienstelement 2 (TASE.2), nach Definition in IEC 60870-6-503:2014 [2], IEC 60870-6-702:2014 [3] und IEC 60870-6-802:2014 [4] verwendet wird.

Bei der Implementierung der MMS für das ICCP müssen Mechanismen für die Konfiguration und Nutzung der Sicherheitsfunktionen eingebaut werden. Diese werden als bilaterale Vereinbarungen nach IEC 60870-6-503:2014 bereitgestellt.

Im Allgemeinen muss Folgendes bereitgestellt werden:

- Ein Mechanismus für die Konfiguration der Informationen zu Zertifikaten mit öffentlichem Schlüssel und die Bindung dieser Informationen an die Zugriffsauthentifizierung (z. B. die bilateralen Tabellen).
- Ein Mechanismus für die Konfiguration des zulässigen eingehenden Transportprofils für den Zugriffskontrollmechanismus der Implementierung. Es werden die folgenden Auswahlmöglichkeiten vorgeschlagen:
 - DON'T_CARE: Der Aufbau einer MMS-Assoziation ist sowohl mit als auch ohne T-Sicherheit zulässig.
 - NON_SECURE: würde anzeigen, dass keine T-Sicherheit für die Zulassung des Aufbaus einer MMS-Assoziation verwendet werden darf.
 - SECURE: würde anzeigen, dass der Aufbau einer MMS-Assoziation nur mit T-Sicherheit zulässig wäre.
- Ein Mechanismus für die Konfiguration der zur Initialisierung einer MMS-Assoziation zu verwendenden Anwendungssicherheit. Es werden die folgenden Auswahlmöglichkeiten vorgeschlagen:
 - NON_SECURE: würde anzeigen, dass keine Anwendungssicherheit für die Zulassung des Aufbaus einer MMS-Assoziation verwendet werden darf.
 - SECURE: würde anzeigen, dass der Aufbau einer MMS-Assoziation nur mit dem A-Sicherheitsprofil nach [Abschnitt 11](#) (oder IEC TS 62351-4:2007) zulässig wäre.
 - END-TO-END-SECURE: würde anzeigen, dass der Aufbau einer MMS-Assoziation nur mit E2E-Sicherheit zulässig wäre.
- Ein Mechanismus zur Übermittlung/Verifizierung der Assoziationsparameter. Diese Parameter sollten Adressinformationen, einen Hinweis auf das verwendete Profil (z. B. Ende-zu-Ende, sicher, nicht sicher) und die Parameter für die Authentifizierung im Quittungsbetrieb beinhalten.

Diese Informationen müssen gemeinsam mit den erwarteten Assoziationswerten der konfigurierten MMS dazu verwendet werden zu ermitteln, ob eine MMS-Assoziation aufgebaut werden sollte. Wie die Einheit über die tatsächliche Annahme entscheidet, ist jeweils lokal festzulegen.

Es ist wünschenswert, dass, wenn eine einzelne Assoziation aufgrund von Änderungen an der Konfiguration neu gestartet werden muss, hierzu nicht auch andere Assoziationen neu gestartet werden müssen. Einige Spezifikationen, auf die verwiesen wird, erfordern jedoch einen kompletten Neustart aller Assoziationen.

5.2 Spezifische Anforderungen an IEC 61850

Wenn eine Referenznorm der Reihe IEC 61850 die Ausführung im Kompatibilitätsmodus verlangt, muss der Anwendungskontext **basic-AC** (siehe 11.1.4.2) in der Assoziationsanforderung festgelegt werden. Wenn die Ausführung im nativen Modus verlangt wird, muss der Anwendungskontext **e2eMmsAC** (siehe 15.2.2) festgelegt werden.

6 Transportsicherheit

6.1 Allgemeines

Die T-Sicherheit legt keine Sicherheitsempfehlungen für TCP, IP oder Ethernet fest. Stattdessen wird in den Spezifikationen für die T-Sicherheit festgelegt, wie die Transportschicht-Sicherheit (TLS) richtig zur Sicherung des Datenverkehrs über die Transportschicht eingesetzt wird. Diese Spezifikation bezieht sich teilweise auf das TLS-Profil nach IEC 62351-3:2018.

6.2 Anwendung der Transportschicht-Sicherheit (TLS)

6.2.1 Allgemeines

In IEC 62351-3:2018 wird ein allgemeines Profil der TLS festgelegt, das viele Parameter offen lässt. In 6.2.2 bis 6.2.9 werden die geforderten Werte und Einstellungen dieser Parameter zur Übereinstimmung mit diesem Dokument beschrieben und festgelegt. Die festgelegten Parametertypen umfassen:

- Die zu unterstützenden verbindlichen TLS-Chiffrensammlungen
- Die empfohlene Festlegung hinsichtlich der Wiederaufnahme von Sitzungsparametern aus einer früheren Verbindung auf Grundlage der Sitzungslaufzeit
- Die empfohlene Festlegung hinsichtlich der Neuaushandlung von Sitzungsparametern auf Grundlage der Sitzungslaufzeit
- Die empfohlene Standard-Bewertungsdauer der Zertifikatsperrliste (CRL), sofern zur Überprüfung der Sperre CRLs verwendet werden
- Bei Verwendung von OCSP für die Überprüfung von Zertifikatsperrungen: der Umgang mit fehlgeschlagenen Zugriffen auf den OCSP-Antwortsender
- Der Umgang mit Aktionen zur Validierung von Zertifikaten mit öffentlichem Schlüssel
- Die Konformitätsanforderungen für diesen Teil von IEC 62351. Die Konformitätserklärung wird in Abschnitt 17 bereitgestellt.

Neben den bereits von IEC 62351-3:2018 geforderten und in diesem Abschnitt festgelegten Parametern ist eine weitere Festlegung ausgewählter Parameter nach 6.3 für die OSI-Betriebsumgebung und nach 6.4 für die XMPP-Betriebsumgebung erforderlich.

6.2.2 Der Begriff der TLS-Chiffrensammlung

Eine Chiffrensammlung ist in TLS eine Menge kryptografischer Algorithmen zur Kombination von Peer-Authentifizierung, Verschlüsselung, Nachrichtenauthentifizierungscode (MAC) und Schlüsselaustauschalgorithmus. Eine Chiffrensammlung wird durch einen spezifischen Chiffrensammlungswert identifiziert, der in der ClientHello- und der ServerHello-Nachricht verwendet wird. Diese Werte werden von IANA in der TLS Cipher Suite Registry registriert.

6.2.3 Wiederaufnahme von TLS-Sitzungen

Eine Implementierung, für die die Konformität mit dieser Spezifikation erklärt wird, muss eine mindestens alle zwei Stunden stattfindende Sitzungswiederaufnahme unterstützen.

ANMERKUNG Diese Anforderung gilt nicht für die Unterstützung des Kompatibilitätsmodus.

6.2.4 Neuaushandlung von TLS-Sitzungen

Eine Implementierung, für die die Konformität mit diesem Dokument erklärt wird, muss eine Sitzungsneuaushandlung mit mindestens der halben CRL-Aktualisierungsperiode unterstützen (siehe 6.2.7). Der untere Grenzwert für die Neuaushandlung der Sitzung beträgt 10 Minuten.

ANMERKUNG Diese Anforderung schützt die Leistung von Client und Server, indem sie verhindert, dass zu viele vollständige TLS-Quittungsverfahren und damit verbundene Validierungen von Zertifikaten mit öffentlichem Schlüssel erfolgen.

6.2.5 Unterstützte Anzahl von Vertrauensankern

Implementierungen, die dieser Spezifikation entsprechen, müssen mindestens zwei verschiedene Vertrauensanker unterstützen. Diese Anforderung entspricht dem in [IEC 62351-9](#) beschriebenen Zertifikatmanagement für von Anbietern und Betreibern verteilte Zertifikate mit öffentlichem Schlüssel.

6.2.6 Größe von Zertifikaten mit öffentlichem Schlüssel

Eine Implementierung, für die die Konformität mit diesem Dokument erklärt wird, muss für Zertifikate mit öffentlichem Schlüssel mindestens eine Größe von 8 192 Oktetten unterstützen. Ob auch größere Zertifikate mit öffentlichem Schlüssel unterstützt werden, wird jeweils lokal festgelegt.

Eine Implementierung, die ein Zertifikat mit öffentlichem Schlüssel erhält, dessen Größe die von ihr unterstützte Größe überschreitet, muss die Verbindung beenden und ein Sicherheitsereignis melden („Warnung: Sitzung aufgrund nicht unterstützter Größe des Zertifikats mit öffentlichem Schlüssel beendet“).

6.2.7 Bewertungsdauer für den Sperrstatus von Zertifikaten mit öffentlichem Schlüssel

Eine Implementierung, für die die Konformität mit diesem Teil von IEC 62351 erklärt wird, muss eine mindestens alle 24 Stunden erfolgende CRL-Aktualisierung unterstützen. Die Standard-Bewertungsperiode für gesperrte Zertifikate mit öffentlichem Schlüssel beträgt 24 Stunden. Diese Bewertungsperiode muss konfigurierbar sein.

Eine Implementierung, welche OCSP für die Informationen aus der Überprüfung einer Sperre unterstützt, darf die OCSP-Antwort höchstens 24 Stunden im Cache speichern.

Wenn auf den CRL-Provider, den OCSP-Antwortsender oder eine lokal im Cache gespeicherte CRL oder OCSP-Antwort nicht zugegriffen werden kann, muss ein Sicherheitsereignis gemeldet werden („Warnung: Zertifikatsperrinformationen nicht verfügbar“).

Wie in [IEC 62351-3:2018](#) vorgegeben, darf die Tatsache, dass die Sperrinformationen nicht abgerufen werden können, nicht die Beendigung der Sitzung nach sich ziehen.

6.2.8 Validierung von Zertifikaten mit öffentlichem Schlüssel

Eine Implementierung, für die die Konformität mit dieser Spezifikation erklärt wird, muss unter Beachtung der jeweiligen lokalen Vorschriften den Aufbau oder die Neuaushandlung einer Verbindung abbrechen können, wenn ein von dem Client oder dem Server verwendetes Zertifikat mit öffentlichem Schlüssel gesperrt oder abgelaufen ist.

Wenn aufgrund eines gesperrten oder abgelaufenen Zertifikats mit öffentlichem Schlüssel der Verbindungsaufbau verweigert oder eine Verbindung während der Sitzungsneuaushandlung abgebrochen wird, sollte ein Sicherheitsereignis gemeldet werden („Vorfall: gesperrtes Zertifikat mit öffentlichem Schlüssel“). Wenn das Zertifikat mit öffentlichem Schlüssel abgelaufen ist, muss ein Sicherheitsereignis gemeldet werden („Warnung: abgelaufenes Zertifikat mit öffentlichem Schlüssel“).

6.2.9 Umgang mit Sicherheitsereignissen

Informationen zu Sicherheitsereignissen und aus der Überwachung sollten der umgebenden Infrastruktur mittels Anwendung von **IEC 62351-7:2017** und/oder IEC 62351-14 zugänglich gemacht werden. **IEC 62351-7:2017** definiert den Umgang mit Informationen aus der Sicherheitsüberwachung, während IEC 62351-14 den Umgang mit Nachrichten mit Sicherheitswarnungen und Sicherheitsvorfällen festlegt.

6.3 T-Sicherheit in einer OSI-Betriebsumgebung

6.3.1 Allgemeines

TLS entsprechend der Festlegung für die T-Sicherheit muss nach **IEC 62351-3:2018** mit den in 6.2 festgelegten Parametern verwendet werden. In 6.3.2 bis 6.3.4 werden die zu verwendenden Kommunikations-Ports und Chiffrensammlungen genauer festgelegt.

6.3.2 TCP-Ports

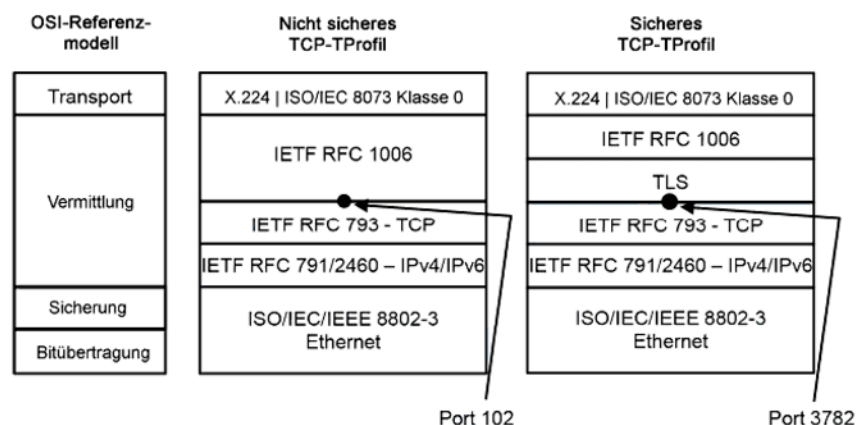


Bild 2 – T-Profile mit und ohne TLS-Schutz

Bild 2 zeigt die beiden relevanten TCP-T-Profile. Das eine ist das standardmäßige T-Profil nach IETF RFC 1006, das keine Transportsicherheit bietet. Das andere zeigt die Ergänzung durch TLS zwecks Sicherstellung der Transportsicherheit nach diesem Dokument.

Ohne Transportsicherheit muss der TCP-Port 102 nach IETF RFC 1006 verwendet werden.

Implementierungen, für die die Konformität mit diesem Teil von IEC 62351-4 erklärt wird, müssen den TCP-Port 3782 verwenden, um die Verwendung der Transportsicherheit anzuzeigen. Dieser Port ist von der IANA als sicherer ISO TP0-Port registriert.

IETF RFC 1006 unterstützt nur die Verwendung der Transportklasse 0 aus ISO/IEC 8073 | Rec. ITU-T X.224.

6.3.3 Deaktivierung der TLS

Die Implementierungen müssen eine Deaktivierung der TLS ermöglichen. Wenn die TLS deaktiviert ist, muss der TCP-Port 102 verwendet werden.

Die Deaktivierung der TLS darf entweder in Abhängigkeit von der zugrunde liegenden Sicherheit erfolgen, die über ein VPN bereitgestellt werden darf (womit in diesem Kontext ein Sicherheitsprotokoll unterhalb der TLS, IPsec oder ein anderes Protokoll, gemeint ist), oder in Abhängigkeit von dem eingesetzten Anwendungssicherheitsprofil.

6.3.4 Unterstützung von TLS-Chiffrensammlungen

6.3.4.1 Allgemeines

6.3.4.2 legt TLS-Chiffrensammlungen zur Unterstützung im Kompatibilitätsmodus fest und 6.3.4.3 legt TLS-Chiffrensammlungen zur Unterstützung im nativen Modus fest. Durch Spezifikationen, auf die verwiesen wird, kommen gegebenenfalls weitere verbindliche Chiffrensammlungen hinzu.

TLS priorisiert im TLS-Quittungsbetrieb die vorgeschlagenen Chiffrensammlungen in der Reihenfolge, in der sie auf der Liste der vorgeschlagenen Chiffrensammlungen in der ClientHello-Nachricht aufgeführt werden. Deshalb ist es erforderlich, dass die verbindlichen Chiffrensammlungen als Erste vorgeschlagen werden, gefolgt von den unterstützten optionalen Chiffrensammlungen.

6.3.4.2 Verbindliche und empfohlene Chiffrensammlungen für den Kompatibilitätsmodus

Alle Implementierungen, für die die Konformität mit IEC TS 62351-4:2007 erklärt wird, müssen mindestens TLS_DH_DSS_WITH_AES_256_SHA unterstützen.

Es wird empfohlen, die in Tabelle 2 (aus IEC TS 62351-4:2007) aufgeführten TLS-Chiffrensammlungen in Betracht zu ziehen. Aufgrund der Fortschritte der Kryptografie gelten einige Chiffrensammlungen als unsicher. Diese sind in der Originaltabelle aus IEC TS 62351-4:2007 gekennzeichnet.

Tabelle 2 – Kommentierte empfohlene Chiffrensammlungen aus IEC TS 62351-4:2007

Schlüsselaustausch		Verschlüsselung	Hash	Quelle	Unterstützung
Algorithmus	Signatur				
TLS_RSA_		WITH_RC4_128_	SHA	RFC 2246 (TLS 1.0)	Nicht zulässig (RC 4 als schwach erachtet)
TLS_RSA_		WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	Optional
TLS_DH_	DSS_	WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	Optional
TLS_DH_	RSA_	WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	Optional
TLS_DHE_	DSS_	WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	Optional
TLS_DHE_	RSA_	WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	Optional
TLS_DH_	DSS_	WITH_AES_128_	SHA	RFC 4346 (TLS 1.1)	Optional
TLS_DH_	DSS_	WITH_AES_256_	SHA	RFC 4346 (TLS 1.1)	Verbindlich
TLS_DH_		WITH_AES_128_	SHA	RFC 4346 (TLS 1.1)	Nicht zulässig (anonym)
TLS_DH_		WITH_AES_256_	SHA	RFC 4346 (TLS 1.1)	Nicht zulässig (anonym)

ANMERKUNG Der Aushandlungsmechanismus in der TLS wählt die letztendlich für eine bestimmte Verbindung verwendete Chiffrensammlung aus den konfigurierten zulässigen/vorhandenen Chiffrensammlungen aus.

6.3.4.3 Verbindliche und empfohlene Chiffrensammlungen für den nativen Modus

Alle Implementierungen, für die die Konformität mit dem nativen Modus erklärt wird, müssen mindestens TLS_RSA_WITH_AES_128_CBC_SHA256 unterstützen.

Es wird empfohlen, die in Tabelle 3 aufgeführten optionalen TLS-Chiffrensammlungen für die Verwendung in Betracht zu ziehen. Wie in Tabelle 3 vermerkt, stammen sie aus verschiedenen IETF-RFCs.

Tabelle 3 – Kombinationen von Chiffrensammlungen im Kontext dieses Dokuments

Schlüsselaustausch		Verschlüsselung	Hash	Quelle	Unterstützung
Algorithmus	Signatur				
TLS_RSA		WITH_AES_128_CBC_	SHA256	RFC 5246	Verbindlich
TLS_DH_	RSA_	WITH_AES_128_CBC_	SHA256	RFC 5246	Optional
TLS_DH_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5288 [5]	Verbindlich
TLS_DHE_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5288 [5]	Verbindlich
TLS_DH_	RSA_	WITH_AES_256_GCM_	SHA384	RFC 5288 [5]	Optional
TLS_ECDHE_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5289 [6]	Optional
TLS_ECDHE_	RSA_	WITH_AES_256_GCM_	SHA384	RFC 5289 [6]	Optional
TLS_ECDHE_	ECDSA_	WITH_AES_128_GCM_	SHA256	RFC 5289 [7]	Verbindlich
TLS_ECDHE_	ECDSA_	WITH_AES_256_GCM_	SHA384	RFC 5289 [7]	Optional

6.4 T-Sicherheit in einer XMPP-Betriebsumgebung

TLS für T-Sicherheit in einer XMPP-Umgebung muss nach IETF RFC 6120:2011, Abschnitt 5, verwendet werden. Die Unterabschnitte 13.7.2 bis 13.7.4 dieses RFC enthalten die Spezifikation für den Umgang mit Zertifikaten mit öffentlichem Schlüssel und fordern die Unterstützung der Chiffrensammlung TLS_RSA_WITH_AES_128_CBC_SHA. Da diese Chiffrensammlung aufgrund der Anwendung von SHA-1 als weniger sicher gilt, wird in diesem Teil von IEC 62351 stattdessen dringend die Unterstützung der Chiffrensammlung TLS_RSA_WITH_AES_128_CBC_SHA256 empfohlen, um besser für die Zukunft gerüstet zu sein. Außerdem wird die Berücksichtigung der in 6.2 festgelegten Parameter empfohlen.

IETF RFC 7590 enthält weitere Informationen zur Verwendung von TLS in XMPP. Dieses IETF-RFC fordert, dass die in IETF RFC 7525 enthaltenen Empfehlungen befolgt werden.

Die notwendigen T-Profil-Parameter müssen anhand der Referenznormen dieses Dokuments bestimmt werden.

7 Überblick über die Sicherheit der Anwendungsschicht (informativ)

7.1 Allgemeines

Während die T-Sicherheit für Authentifizierung, Integrität und Vertraulichkeit auf der Transportschicht sorgt, bietet die Anwendungssicherheit Sicherheit auf der Anwendungsschicht.

Dieser Teil von IEC 62351 legt zwei Klassen von Anwendungssicherheitsfunktionen fest:

- Eine Peer-to-Peer-Sicherheitspezifikation, die als A-Sicherheitsprofil bezeichnet wird und dem in IEC TS 62351-4:2007 festgelegten A-Profil entspricht; sie bietet nur Sicherheit für MMS-basierte Anwendungsprotokolle und unterstützt nur einen OSI-Protokollstapel. Diese Sicherheitspezifikation wird hier aufgeführt, weil sie von Communitys wie der ICCP-Community und von Implementierungen nach IEC 61850-8-1 benutzt wird. Im Allgemeinen wird dringend empfohlen, auf strengere Sicherheitsvorkehrungen umzustellen. Diese Sicherheitspezifikation bietet lediglich eine Peer-Authentifizierung auf der Anwendungsschicht während des Assoziationsaufbaus. Für die Nachrichten im anschließenden Datenaustausch (Datenübertragungsphase) gibt es keine kryptografische Bindung. Sie bietet keine Ende-zu-Ende-Authentifizierung mit zwischengeschalteten Einheiten und stellt keine Integrität und Vertraulichkeit bereit. Dieses Profil sollte nur gemeinsam mit T-Sicherheit verwendet werden.

Die Spezifikation des A-Sicherheitsprofils ist in [Abschnitt 11](#) enthalten.

- b) Ende-zu-Ende-Anwendungssicherheit (E2E-Sicherheit); sie bietet Ende-zu-Ende-Sicherheit auf der Anwendungsschicht mit null oder mehr zwischengeschalteten Einheiten, wohingegen T-Sicherheit nur auf den einzelnen Hops Sicherheit bietet.

E2E-Sicherheit kann in unterschiedlichen Betriebsumgebungen angewendet werden und kann unterschiedliche Protokolle schützen.

Die E2E-Sicherheit bietet Ende-zu-Ende-Datenursprungs-Authentifizierung und Ende-zu-Ende-Nachrichtenintegrität während des Aufbaus einer Assoziation sowie für die anschließende, an die anfängliche Authentifizierung gebundene Datenübertragungsphase. E2E-Sicherheit kann mit oder ohne Verschlüsselung verwendet werden.

Wenngleich die Sicherheitsinformationen von Ende zu Ende ausgetauscht werden, ist in gewisser Hinsicht eine zwischengeschaltete Einheit beteiligt, z. B., wenn das Routing nicht ausgeführt werden kann.

Die folgenden Abschnitte enthalten die Spezifikation für E2E-Sicherheit:

- [Abschnitt 12](#) definiert das Gesamtmodell oder die Architektur für E2E-Sicherheit, einschließlich der Beziehung der E2E-Sicherheit zu der Betriebsumgebung und dem geschützten Protokoll.
- [Abschnitt 13](#) legt das Protokoll für die E2E-Sicherheit fest, unabhängig von der Betriebsumgebung und dem geschützten Protokoll.
- [Abschnitt 14](#) legt Verfahren für den Umgang mit E2E-Sicherheitsfehlern fest.
- [Abschnitt 15](#) legt die Anforderungen an eine OSI-Betriebsumgebung fest, einschließlich der spezifischen Fehlerbehandlung.
- [Abschnitt 16](#) legt die Anforderungen an eine XMPP-Betriebsumgebung fest, einschließlich der spezifischen Fehlerbehandlung.

7.2 Beschreibungstechniken

7.2.1 Allgemeines

Zur Spezifikation des E2E-Sicherheitsprotokolls wird die Abstract Syntax Notation ONE (ASN.1) nach ISO/IEC 8824-1 | Rec. ITU-T X.680 verwendet. Die Verwendung von ASN.1 wird in 7.2.2 ausführlicher diskutiert.

Die abstrakte Syntax für das E2E-Sicherheitsprotokoll wird außerdem in W3C XML Schema Definition (W3C XSD) nach W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures [8] und W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes [9] ausgedrückt. Die Verwendung von W3C XSD wird in 7.2.3 ausführlicher diskutiert.

7.2.2 ASN.1 als XML-Schema-Definition

Die formale ASN.1-Spezifikation für die E2E-Sicherheit befindet sich in [Anhang B](#).

Es gibt verschiedene Codierungsregeln für eine abstrakte ASN.1-Syntax:

- a) In einer OSI-Betriebsumgebung, einschließlich des A-Sicherheitsprofils, erfordert dieser Teil von IEC 62351 die Unterstützung der grundlegenden Codierungsregeln (BER) nach ISO/IEC 8825-1 | Rec. ITU-T X.690.
- b) In einer XMPP-Betriebsumgebung darf die Codierung auf der ASN.1-Spezifikation mit den XML-Codierungsregeln (XER) beruhen, genauer gesagt den EXTENDED-XER nach ISO/IEC 8825-4 | Rec. ITU-T X.693.
- c) Nach ISO/IEC 9594-8 | Rec. ITU-T X.509 müssen Zertifikate mit öffentlichem Schlüssel und Attribut-zertifikate unter Verwendung der besonderen Codierungsregeln (DER) codiert werden. Die DER entsprechen den BER mit einigen Einschränkungen, die alle Codierungsoptionen aufheben. Die Implementierung muss überprüfen, ob Zertifikate mit öffentlichem Schlüssel und Attribut-zertifikate DER-codiert sind. Die DER sind ebenso in ISO/IEC 8825-1 | Rec. ITU-T X.690 festgelegt.

7.2.3 W3C XML Schema Definition (W3C XSD)

W3C XSD ist eine alternative abstrakte Syntax, die für die XML-Codierung von PDUs verwendet werden darf.

Wenn XML-Codierung erforderlich ist, muss entweder W3C XSD oder ASN.1 EXTENDED-XER unterstützt werden.

Nach 7.2.2 c) müssen Zertifikate mit öffentlichem Schlüssel und Attributzertifikate in ASN.1 DER codiert werden. Eine Implementierung, für die XSD verwendet wird, muss ein in DER codiertes Zertifikat mit öffentlichem Schlüssel bzw. ein in DER codiertes Attributzertifikat validieren können. Eine Implementierung, für die W3C XSD verwendet wird, muss außerdem berücksichtigen, dass der gesamte PKI-bezogene Datenverkehr (CRL-Abruf, OCSP-Zugriff usw.) eine ASN.1-BER-Codierung erfordert.

Die W3C XSD für die E2E-Sicherheit ist in [Anhang C](#) angegeben.

7.2.4 XML-Namensraum

Wenn eine XML-Codierung erforderlich ist, teilen die E2E-Sicherheit und die virtuelle API (siehe [12.1](#)) einen gemeinsamen XML-Namensraum, der als http://www.iec.ch/62351/2018/E2E_4 identifiziert wird.

8 Verwendung von kryptografischen Algorithmen

8.1 Allgemeines

Dieses Dokument greift in starkem Maße auf kryptografische Algorithmen zurück, um die geforderte Sicherheit sicherzustellen. In diesem Abschnitt werden relevante kryptografische Algorithmen eingeführt, die vom A-Sicherheitsprofil oder von der E2E-Sicherheit verwendet werden. In [Abschnitt 11](#) wird der kryptografische Algorithmus festgelegt, der vom A-Sicherheitsprofil verwendet wird, und in [Abschnitt 13](#) werden die kryptografischen Algorithmen festgelegt, die für die E2E-Sicherheit verwendet werden.

ISO/IEC 9594-8 | Rec. ITU-T X.509 definiert verschiedene ASN.1-Konstrukte für die formale Spezifikation kryptografischer Algorithmen. Diese Definitionen werden zum einfacheren Nachschlagen unter 8.2 wiedergegeben. In [8.3 bis 8.8](#) werden kryptografische Algorithmen aufgelistet, die von anderen Spezifikationen wie z. B. IETF-RFCs definiert werden. Diese Algorithmen sind relevant für dieses Dokument.

8.2 Grundlegende kryptografische Definitionen

```
ALGORITHM ::= CLASS {  
    &Type                OPTIONAL,  
    &id                   OBJECT IDENTIFIER UNIQUE }  
WITH SYNTAX {  
    [PARMS                &Type]  
    IDENTIFIED BY &id }
```

Die ASN.1-Informationsobjektklasse **ALGORITHM** wird für die formale Spezifikation von kryptografischen Algorithmen verwendet.

```
AlgorithmIdentifier{ALGORITHM:SupportedAlgorithms} ::= SEQUENCE {  
    algorithm  ALGORITHM.&id({SupportedAlgorithms}),  
    parameters ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,  
    ... }
```

Der parametrisierte Datentyp **AlgorithmIdentifier** gibt die generelle Syntax für einen kryptografischen Algorithmus entsprechend der Definition über die ASN.1-Informationsobjektklasse **ALGORITHM** an.

Die kryptografischen Algorithmen werden beständig weiterentwickelt. Dieser Teil von IEC 62351 ist offen für neue und sicherere Algorithmen. Bei den folgenden Algorithmusspezifikationen handelt es sich um Spezifikationen, die als sicher für die Verwendung über eine längere Zeitspanne gelten. Durch Spezifikationen, auf die verwiesen wird, und/oder durch Vereinbarungen der Implementierer kommen gegebenenfalls weitere in bestimmten Umgebungen zu verwendende kryptografische Algorithmen hinzu.

ASN.1 verfügt über das Konzept von ASN.1-Objektmengen, das es einer Spezifikation ermöglicht, eine Menge unterstützter kryptografischer Algorithmen für einen bestimmten Zweck festzulegen, wie in dem folgenden Beispiel dargestellt:

```
AlgorithmSet ALGORITHM ::= {
  algorithm-ID1 |
  algorithm-ID2 |
  ...
  algorithm-IDn,
  ... }
```

Wie vorstehend angegeben, wird ein kryptografischer Algorithmus durch einen Objektbezeichner identifiziert. Die Werte `algorithm-ID1` bis `algorithm-IDn` sind Wertreferenzen von Objektbezeichnern, die an einen spezifischen Typ von kryptografischem Algorithmus vergeben wurden. Die Menge steht für eine Menge kryptografischer Algorithmen, die in einer bestimmten Situation relevant sind.

Aufgrund der Erweiterungspunkte (...) wird ein ASN.1-Tool einen beliebigen Objektbezeichner akzeptieren, unabhängig davon, ob er einen kryptografischen Algorithmus des jeweiligen Typs kennzeichnet oder nicht. Im Rahmen einer Spezifikation, auf die verwiesen wird, oder im Rahmen einer Vereinbarung der Implementierer dürfen die Erweiterungspunkte entfernt und/oder zusätzliche Algorithmen hinzugefügt werden.

8.3 Algorithmen mit öffentlichem Schlüssel

An dieser Stelle werden zwei Algorithmen mit öffentlichem Schlüssel eingeführt:

```
rsaEncryptionAlgorithm ALGORITHM ::= {
  PARMS          NULL
  IDENTIFIED BY rsaEncryption }

rsaEncryption    OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1) }
```

IETF RFC 4055 gibt die formale Spezifikation für die `rsaEncryptionAlgorithm`-Algorithmen mit öffentlichem Schlüssel an.

```
ecPublicKey ALGORITHM ::= {
  PARMS          OBJECT IDENTIFIER
  IDENTIFIED BY id-ecPublicKey }

id-ecPublicKey   OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  ansi-x9-62(10045) keyType(2) 1 }      -- IETF RFC 5480
```

IETF RFC 5480 gibt die formale Spezifikation für den Algorithmus mit öffentlichem Schlüssel `ecPublicKey` an.

Der Algorithmus mit öffentlichem Schlüssel `ecPublicKey` erfordert eine Identifikation einer elliptischen Kurve als Parameter. Eine bestimmte elliptische Kurve wird durch einen Objektbezeichner (`en: object identifier`) identifiziert. Für diesen Teil von IEC 62351 sind die folgenden elliptischen Kurven relevant:

```
secp256r1        OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  ansi-x9-62(10045) curves(3) prime(1) 7 }
```

IETF RFC 5480 gibt die formale Spezifikation für die elliptische Kurve `secp256r1` an.

```
brainpoolP256r1  OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
  teletrust(36) algorithm(3) signature-algorithm(3) ecSign(2) 8 ellipticCurve(1)
  versionOne(1) 7 }
```

IETF RFC 5639 gibt die formale Spezifikation für die elliptische Kurve `brainpoolP256r1` an.

8.4 Hash-Algorithmen

An dieser Stelle wird ein einzelner Hash-Algorithmus eingeführt:

```
sha256 ALGORITHM ::= { -- IETF RFC 5754
  IDENTIFIED BY id-sha256 }
```