

DIN EN 62734

ICS 35.100.70; 35.110; 35.240.50

Einsprüche bis 2014-06-18

Entwurf

**Industrielle Kommunikationsnetze –
Funk-Kommunikationsnetze und -profile –
ISA 100.11a
(IEC 65C/735A/CDV:2013);
Englische Fassung FprEN 62734:2013**

Industrial communication networks –
Wireless communication network and communication profiles –
ISA 100.11a
(IEC 65C/735A/CDV:2013);
English version FprEN 62734:2013

Réseaux de communication industriels –
Réseau de communication sans fil et profils de communication –
ISA 100.11a
(CEI 65C/735A/CDV:2013);
Version anglaise FprEN 62734:2013

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-04-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (Hausanschrift: Stresemannallee 15, 60596 Frankfurt am Main).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 882 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Nationales Vorwort

Die Englische Fassung des europäischen Dokuments FprEN 62734:2013 „Industrielle Kommunikationsnetze – Funk-Kommunikationsnetze und -profile – ISA 100.11a“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65C/735A/CDV:2013 „Industrial communication networks – Wireless communication network and communication profiles – ISA 100.11a“ unverändert in den Entwurf FprEN 62734:2013 übernommen worden.

Das internationale Dokument wurde vom SC 65C „Industrial networks“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium K 956 „Feldbus“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnichtsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

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

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für den vorliegenden Normentwurf erfüllt.

Da sich die Benutzer des vorliegenden Normentwurfs der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung EN 62734 veröffentlicht. Zu Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Normentwurfs hinzugefügt. Für viele der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Normentwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

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.

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

Nationaler Anhang NA (informativ)

3 Begriffe, Abkürzungen Akronyme und Vereinbarungen

3.1 Begriffe

3.1.1 (N)-Schicht und andere Begriffe aus dem Basis-Referenzmodell der Kommunikation offener Systeme

3.1.1.1

abstrakte Syntax

(en: **abstract syntax**)

Festlegung von (N)-PDUs durch Anwendung von Notationsregeln, die von den zu ihrer Darstellung verwendeten Kodierungsverfahren unabhängig sind

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.1.1.2, modifiziert – verallgemeinert für die N-Schicht]

3.1.1.2

Zurechenbarkeit

(en: **accountability**)

Eigenschaft, die gewährleistet, dass Aktionen einer Instanz auch auf diese zurückgeführt werden können

[Quelle: ISO 7489-2:1989, 3.3.3]

3.1.1.3

Quittierung

(en: **acknowledgement**)

Funktion der (N)-Schicht, die es einer empfangenden Instanz einer (N)-Schicht ermöglicht, eine sendende Instanz einer (N) Schicht über den Empfang einer PDU zu informieren

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.16]

3.1.1.4

Anwendungsinstanz

(en: **application-entity**)

aktives Element innerhalb eines Anwendungsprozesses, welches ein bestimmtes Leistungspotential im Rahmen von OSI verkörpert, das für die AL definiert ist und einem bestimmten Anwendungsinstanztyp entspricht (ohne Verwendung zusätzlicher Leistungspotentiale)

Anmerkung 1 zum Begriff: Dabei handelt es sich um eine geringfügige Spezialisierung der (N)-Instanz, weil die AL für OSI nicht relevante Anwendungsfunktionen enthält. Jede Anwendungsinstanz stellt genau einen Prozess in der Umgebung der Kommunikation offener Systeme dar.

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.1.1.1]

3.1.1.5

Anwendungsmanagement

(en: **application-management**)

auf das Management von OSI-Anwendungsprozessen bezogene Funktionen in der AL

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 8.1.1]

3.1.1.6**Assoziation****(en: association)**

zusammenwirkende Beziehung zwischen Systeminstanzen, gewöhnlich zum Zweck der Übertragung von Informationen zwischen ihnen

[Quelle: ISO 62443-1-1:2009, 3.2.7]

3.1.1.7**(N)-Assoziation****(en: (N)-association)**

zusammenwirkende Beziehung zwischen Aufrufen von Instanzen der (N)-Schicht

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.1]

3.1.1.8**Berechtigung****(en: authorization)**

Erteilung von Rechten, wozu auch die Gewährung des Zugriffs basierend auf Zugriffsrechten gehört

[Quelle: ISO 7498-2:1989, 3.3.10]

3.1.1.9**Verfügbarkeit****(en: availability)**

Eigenschaft, einer berechtigten Instanz auf Verlangen zugänglich und nutzbar zu sein

[Quelle: ISO 7498-2:2009, 3.3.11]

3.1.1.10**Blockbildung****(en: blocking)**

von einer (N)-Instanz ausgeführte Funktion zur Abbildung mehrerer (N)-SDUs auf eine (N)-PDU

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.11]

3.1.1.11**Mehrpunktverbindung mit zentraler Steuerung****(en: centralized-multi-endpoint-connection)**

Mehrpunktverbindung, bei der Daten, die von der an den zentralen Verbindungsendpunkt angeschlossenen Instanz gesendet werden, von allen anderen Instanzen empfangen werden, während von den anderen Instanzen gesendete Daten nur von der zentralen Instanz empfangen werden

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.2]

3.1.1.12**verschlüsselter Text****(en: ciphertext)**

durch Verschlüsselung erzeugte Daten, so dass der semantische Inhalt der resultierenden Daten nicht einsehbar ist (siehe Klartext)

Anmerkung 1 zum Begriff: Bezogen auf eine PDU ist verschlüsselter Text eine Information in einer PDU, die durch Verschlüsselung verdeckt wird, in seiner verdeckten Form nach der Verschlüsselung und vor der Entschlüsselung.

[Quelle: ISO 7498-2:2009, 3.3.14, in Übereinstimmung mit den ISO/IEC-Direktiven, Teil 2]

3.1.1.13**Klartext****(en: cleartext)**

- a) allgemein verständliche Daten mit einsehbarem semantischem Inhalt
- b) Information in einer PDU, die nicht durch Verschlüsselung verdeckt wird

Anmerkung 1 zum Begriff: Bezogen auf eine PDU ist Klartext eine Information in der PDU, die nicht durch Verschlüsselung verdeckt wird und die in der PDU, wenn vorhanden, immer einsehbar ist.

[Quelle: ISO 7498-2:2009, 3.3.15]

3.1.1.14

Gefährdung

(en: **compromise**)

Verletzung der Computersicherheit, wobei Programme oder Daten möglicherweise modifiziert, zerstört oder unberechtigten Instanzen zugänglich gemacht worden sind

[Quelle: ISO/IEC 2382-8:1998, 08.05.11]

3.1.1.15

Verkettung

(en: **concatenation**)

von einer (N)-Instanz ausgeführte Funktion zur Abbildung mehrerer (N)-PDUs auf eine (N-1)-SDU

Anmerkung 1 zum Begriff: Blockbildung und Verkettung dienen verschiedenen Zwecken, obwohl sie ähnliche Funktionen ausführen (sie ermöglichen beide die Zusammenfassung von Dateneinheiten). Verkettung ermöglicht z. B. der (N)-Schicht die Zusammenfassung einer oder mehrerer Quittierungs-(N)-PDUs mit einer (oder mehreren) (N)-PDU(s), die Benutzerdaten enthalten. Das wäre mit der Blockbildungsfunktion allein nicht möglich. Außerdem ist zu beachten, dass die beiden Funktionen so miteinander kombinierbar sind, dass die (N)-Schicht Blockbildung und Verkettung ausführt.

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.13]

3.1.1.16

konkrete Syntax

(en: **concrete syntax**)

diejenigen Aspekte der bei der Spezifikation von Daten angewendeten Regeln, die eine spezifische Darstellung dieser Daten verkörpern

[Quelle: ISO/IEC 7498-1:1994 korrigierte Ausgabe von 1996, 7.1.1.1]

3.1.1.17

Vertraulichkeit

(en: **confidentiality**)

Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden

Anmerkung 1 zum Begriff: Im allgemeinen Kontext der Informationssicherheit wahrt die Vertraulichkeit eine berechtigte Sperrung des Informationszugriffs und der Offenlegung der Information, einschließlich von Mitteln zur Wahrung der Privatsphäre und von anwendungsrelevanten Informationen.

[Quelle: ISO 7498-2:2009, 3.3.16]

3.1.1.18

(N)-Verbindung

(en: **(N)-connection**)

von einer Instanz der (N+1)-Schicht für die Übertragung von Daten zwischen zwei oder mehr (N+1)-Instanzen angeforderte Assoziation

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.1]

3.1.1.19

(N)-Verbindungsendpoint

(en: **(N)-connection endpoint**)

Abschluss an einem Ende einer (N)-Verbindung innerhalb eines (N)-Dienstzugangspunkts

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.3]

3.1.1.20**(N)-Verbindungsendpunkt-Bezeichner****(en: (N)-connection-endpoint-identifier)**

Bezeichner eines (N)-Verbindungsendpunkts zur Bezeichnung der entsprechenden (N)-Verbindung an einem (N)-SAP

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.4.1.5]

3.1.1.21**(N)-Verbindungsendpunkt-Suffix****(en: (N)-connection-endpoint-suffix)**

Teil eines (N)-Verbindungsendpunkt-Bezeichners, der im Bereich eines (N)-SAP eindeutig ist

[Quelle: ISO/IEC-7498-1:1994 in der korrigierten Ausgabe von 1996, 5.4.1.6]

3.1.1.22**(N)-verbindungsorientierte Übertragung****(en: (N)-connection-mode-transmission)**

(N)-Datenübertragung im Kontext einer (N)-Verbindung

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.17]

3.1.1.23**(N)-verbindungslose Übertragung****(en: (N)-connectionless-mode-transmission)**

(N)-Datenübertragung, die nicht im Kontext einer (N)-Verbindung stattfindet und die nicht erforderlich ist, um eine logische Beziehung zwischen (N)-SDUs aufrechtzuerhalten

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.18]

3.1.1.24**korrespondierende (N)-Instanzen****(en: correspondent-(N)-entities)**

(N)-Instanzen, die über eine (N-1)-Verbindung verbunden sind

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.5]

3.1.1.25**Kryptoanalyse****(en: cryptanalysis)**

Analyse eines kryptografischen Systems und/oder von dessen Ein- und Ausgabewerten zur Ableitung vertraulicher Variablen und/oder sensibler Daten einschließlich von Klartext

[Quelle: ISO 7498-2:2009, 3.3.18]

3.1.1.26**Datenintegrität****(en: data integrity)**

Eigenschaft, dass Daten nicht unberechtigt geändert oder zerstört worden sind

[Quelle: ISO 7498-2:1989, 3.3.21]

3.1.1.27**Authentifizierung des Datenursprungs****(en: data-origin authentication)**

Bestätigung, dass die Quelle der empfangenen Daten die geforderte Quelle ist

[Quelle: ISO 7489-2:1989, 3.3.22]

3.1.1.28**(N)-Datenübertragung****(en: (N)-data transmission)**

(N)-Teildienst, der SDUs von einer Instanz einer (N+1)-Schicht zu einer oder mehreren (N+1)-Instanzen übermittelt

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.3.2]

3.1.1.29

Aufheben der Blockbildung

(en: **deblocking**)

von einer (N)-Instanz ausgeführte Funktion zur Identifikation mehrerer (N)-SDUs, die in einer (N)-PDU enthalten sind

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist das Aufheben der Blockbildung die Umkehrfunktion der Blockbildung.

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.12]

3.1.1.30

Mehrpunktverbindung ohne zentrale Steuerung

(en: **decentralized-multi-endpoint-connection**)

Mehrpunktverbindung, bei der Daten, die von einer an einen Verbindungsendpunkt angeschlossenen Instanz gesendet werden, von allen anderen Instanzen empfangen werden

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.3]

3.1.1.31

Entschlüsselung

(en: **decryption**)

Umkehrung einer entsprechenden umkehrbaren Verschlüsselung

[Quelle: ISO 7498-2:1989, 3.3.24]

3.1.1.32

Demultiplexen

(en: **demultiplexing**)

von einer (N)-Instanz ausgeführte Funktion, die (N)-PDUs für mehr als eine (N)-Verbindung innerhalb einer (N-1)-Verbindung identifiziert

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist das Demultiplexen die Umkehrfunktion des Multiplexens.

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.5]

3.1.1.33

digitale Signatur

(en: **digital signature**)

an eine Dateneinheit angefügte Daten oder eine kryptografische Transformation (siehe Kryptografie) einer Dateneinheit, mit der ein Empfänger der Dateneinheit die Möglichkeit der Überprüfung der Quelle und Integrität der Dateneinheit erhält und die einen Schutz gegen Fälschung z. B. durch den Empfänger bietet

[Quelle: ISO 7498-2:1989, 3.3.26]

3.1.1.34

(N)-Instanz

(en: **(N)-entity**)

aktives Element innerhalb eines (N)-Teilsystems, welches ein bestimmtes Leistungspotential verkörpert, das für die (N)-Schicht definiert ist und einem bestimmten (N)-Instanztyp entspricht (ohne Verwendung zusätzlicher Leistungspotentiale)

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.11]

3.1.1.35

(N)-Instanzaufruf

(en: **(N)-entity-invocation**)

spezielle Nutzung eines Teils oder des gesamten Leistungspotentials einer gegebenen (N)-Instanz (ohne Verwendung zusätzlicher Leistungspotentiale)

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.12]

3.1.1.36**(N)-Instanztyp****(en: (N)-entity-type)**

Beschreibung einer Klasse von (N)-Instanzen in Form der für die (N)-Schicht definierten Leistungspotentiale

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.10]

3.1.1.37**(N)-Schnittstellen-Steuerinformationen****(en: (N)-interface-control-information)**

zwischen einer (N+1)-Instanz und einer (N)-Instanz ausgetauschte Informationen zur Koordinierung ihres gemeinsamen Betriebs

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.4]

3.1.1.38**(N)-Schicht****(en: (N)-layer)**

Unterteilung der OSI-Architektur, die aus Teilsystemen desselben Ranges (N) gebildet wird

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 4.2.1]

3.1.1.39**(N)-Schicht-Management****(en: (N)-layer-management)**

auf das Management der (N)-Schicht bezogene Funktionen, die teilweise in der (N)-Schicht selbst gemäß dem (N)-Protokoll der Schicht (Aktivitäten wie Aktivierung und Übertragungssicherung) und teilweise als Teilmenge des Systemmanagements ausgeführt werden

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 8.1.6]

3.1.1.40**Mehrpunktverbindung****(en: multi-endpoint-connection)**

Verbindung mit mehr als zwei Verbindungsendpunkten

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.4]

3.1.1.41**Multiplexen****(en: multiplexing)**

von einer (N)-Instanz ausgeführte Funktion, bei der eine (N-1)-Verbindung zur Unterstützung von mehreren (N)-Verbindungen benutzt wird

Anmerkung 1 zum Begriff: Der Begriff Multiplexen wird im engeren Sinn auch für die Funktion benutzt, die von der sendenden (N)-Instanz ausgeführt wird, während der Begriff Demultiplexen für die Funktion benutzt wird, die von der empfangenden (N)-Instanz ausgeführt wird.

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.4]

3.1.1.42**Password****(en: password)**

vertrauenswürdige Authentifizierungsinformation, die in der Regel aus einer Zeichenfolge besteht

[Quelle: ISO 7498-2:1989, 3.3.39]

3.1.1.43**Partner-(N)-Instanzen****(en: peer-(N)-entities)**

Instanzen innerhalb derselben (N)-Schicht

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.3]

3.1.1.44

Authentifizierung der Partnerinstanz

(en: **peer-entity authentication**)

Bestätigung, dass eine Partnerinstanz in einer Assoziation die geforderte Assoziation ist

[Quelle: ISO 7489-2:1989, 3.3.40]

3.1.1.45

(N)-Protokoll

(en: **(N)-protocol**)

Menge von Regeln und Formaten (Semantik und Syntax), die das Kommunikationsverhalten von (N)-Instanzen bei der Ausführung von (N)-Funktionen bestimmen

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.2.1.9]

3.1.1.46

Adressierungsinformation des (N)-Protokolls

(en: **(N)-protocol-addressing-information**)

diejenigen Elemente der (N)-PCI mit der Adressierungsinformation

[Quelle: ISO/IEC 7498-3:1997, 3.4.20]

3.1.1.47

Steuerinformation des (N)-Protokolls

(en: **(N)-protocol-control-information**)

zwischen (N)-Instanzen ausgetauschte Informationen zur Koordinierung ihres gemeinsamen Betriebs

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.1]

3.1.1.48

(N)-Protokolldateneinheit

(en: **(N)-protocol-data-unit**)

in einem (N)-Protokoll festgelegte Dateneinheit, die aus der Steuerinformation des (N)-Protokolls und möglichen (N)-Benutzerdaten besteht

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.3]

3.1.1.49

Versionsbezeichner des (N)-Protokolls

(en: **(N)-protocol-version-identifier**)

zwischen korrespondierenden (N)-Instanzen übermittelter Bezeichner, der die Auswahl der Version eines (N)-Protokolls ermöglicht

[Quelle: ISO/IEC 7498-1:1994 korrigierte Ausgabe von 1996, 5.8.1.18]

3.1.1.50

Dienstgüte

(en: **quality of service**)

a) Gesamtheit der Merkmale einer einem Benutzer gebotenen Dienstleistung, die dessen Zufriedenheit mit dieser Dienstleistung kennzeichnet

[Quelle: ISO 61907:2009, 3.1.15]

b) vereinbarte Parameter für eine Verbindungsstrecke einschließlich von

- Priorität;
- Zeitfenster für Steuernachrichten;
- Zulässigkeit einer Nachrichtenzustellung außerhalb der Reihenfolge; und
- Zulässigkeit einer Nachrichtenzustellung in Teilschritten

Anmerkung 1 zum Begriff: Die Dienstgüte ist gekennzeichnet durch das Zusammenwirken der Dienstbereitschaft, der Dienstanwendbarkeit, der Dienstverfügbarkeit, der Dienstintegrität und anderer diensteigener Einflüsse.

Anmerkung 2 zum Begriff: ISO definiert Qualität als Fähigkeit eines Produkts oder einer Dienstleistung, den Bedarf eines Benutzers zu befriedigen.

3.1.1.51

Vereinigen

(en: reassembling)

von einer (N)-Instanz durchgeführte Funktion zur Abbildung mehrerer (N)-PDUs auf eine (N)-SDU

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist das Vereinigen die Umkehrfunktion des Segmentierens.

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.10]

3.1.1.52

Rekombination

(en: recombining)

von einer (N)-Instanz ausgeführte Funktion, die (N)-PDUs für eine einzelne (N)-Verbindung in (N-1)-SDUs identifiziert, die auf mehr als einer (N-1)-Verbindung empfangen werden

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist die Rekombination die Umkehrfunktion des Aufteilens.

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.7]

3.1.1.53

(N)-Weiterleitung

(en: (N)-relay)

(N)-Funktion, mit der eine (N)-Instanz von einer Partner-(N)-Instanz erhaltene Daten zu einer anderen Partner-(N)-Instanz weiterleitet

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.3.1.6]

3.1.1.54

Zurücksetzen

(en: reset)

Funktion, die die entsprechenden (N)-Instanzen auf einen vordefinierten Zustand zurücksetzt, wobei ein Datenverlust oder eine Vervielfältigung von Daten möglich ist

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.17]

3.1.1.55

Sicherheitskennzeichen

(en: security label)

an eine Ressource (die eine Dateneinheit sein kann) gebundene Markierung, die die Sicherheitsattribute dieser Ressource benennt oder bezeichnet

[Quelle: ISO 7498-2:1989, 3.3.49]

3.1.1.56

Segmentieren

(en: segmenting)

von einer (N)-Instanz ausgeführte Funktion zur Abbildung einer (N)-SDU auf mehrere (N)-PDUs

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.9]

3.1.1.57

(N)-Wähler

(en: (N)-selector)

der Teil einer (N)-Adresse, der speziell zum adressierten (N)-Teilsystem gehört, d. h., der einen oder mehrere (N)-SAPs innerhalb eines OSI-Endsystems bezeichnet, sobald dieses OSI-Endsystem eindeutig adressiert ist

[Quelle: ISO/IEC 7498-3:1997, 6.2.3, modifiziert]

3.1.1.58

Trennung

(en: **separation**)

von einer (N)-Instanz durchgeführte Funktion zur Identifikation mehrerer (N)-PDUs, die in einer (N-1)-SDU enthalten sind

Anmerkung 1 zum Begriff: Wenn kein Fehler vorliegt, ist die Trennung die Umkehrfunktion der Verkettung.

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.14]

3.1.1.59

Sequenzierung

(en: **sequencing**)

von der (N)-Schicht ausgeführte Funktion zur Wahrung der Reihenfolge der (N)-SDUs, die der (N)-Schicht übergeben werden

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.15]

3.1.1.60

(N)-Dienst

(en: **(N)-service**)

Leistungspotential der (N)-Schicht und der darunter liegenden Schichten, das für die (N+1)-Instanzen an der Grenze zwischen der (N)-Schicht und der (N+1)-Schicht bereitgestellt wird

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 4.2.2]

3.1.1.61

(N)-Dienstzugangspunkt

(en: **(N)-service access point**)

Punkt, an dem einer Instanz der (N+1)-Schicht (N)-Dienste von einer Instanz der (N)-Schicht bereitgestellt werden

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.3.3]

3.1.1.62

Adresse des (N)-Dienstzugangspunkts

(en: **(N)-service-access-point-address**)

(N)-Adresse zur Identifikation eines einzelnen (N)-SAP

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.4.1.2]

3.1.1.63

(N)-Dienst-Dateneinheit

(en: **(N)-service-data-unit**)

Informationsmenge, deren Identität bei einer Übertragung zwischen Partner-(N+1)-Instanzen gewahrt bleibt und die von den unterstützenden (N)-Instanzen nicht interpretiert wird

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.4]

3.1.1.64

Aufteilung

(en: **splitting**)

Funktion innerhalb der (N)-Schicht, mit welcher eine (N)-Verbindung durch mehrere (N-1)-Verbindungen unterstützt wird

Anmerkung 1 zum Begriff: Der Begriff Aufteilung wird im engeren Sinn auch für die Funktion benutzt, die von der sendenden (N)-Instanz ausgeführt wird, während der Begriff Rekombination für die Funktion benutzt wird, die von der empfangenden (N)-Instanz ausgeführt wird

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.8.1.6]

3.1.1.65**Systemverwaltung****(en: system management)**

auf das Management verschiedener OSI-Ressourcen und deren Status über alle Schichten der OSI-Architektur bezogene Funktionen in der AL

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 8.1.4]

3.1.1.66**Transfersyntax****(en: transfer syntax)**

abstrakte und konkrete Syntax, die für die Übertragung von Daten zwischen offenen Systemen verwendet wird

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.2.1.2]

3.1.1.67**Benutzeranwendungsprozess****(en: user application process)**

aktiver Prozess innerhalb des obersten Teilbereichs der AL, d. h. beim Benutzer der OSI-Dienste

Anmerkung 1 zum Begriff: Die Aspekte eines UAP, die für die Zwecke von OSI berücksichtigt werden müssen, werden von einer oder mehreren Anwendungsinstanzen eines oder mehrerer Anwendungstypen dargestellt, die in ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.1.2.2 und 7.1.2.3, definiert sind.

Anmerkung 2 zum Begriff: Die Sammlung von UAPs wird mitunter als Benutzerschicht bezeichnet, auch wenn ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 7.1.2.1, angibt, dass die AL keine Grenze zu einer höheren Schicht besitzt. Im OSI-Basis-Referenzmodell umfasst die AL die UAPs.

3.1.1.68**(N)-Benutzerdaten****(en: (N)-user-data)**

im Auftrag der (N+1)-Instanzen, für die die (N)-Instanzen Dienste bereitstellen, zwischen (N)-Instanzen übertragene Daten

[Quelle: ISO/IEC 7498-1:1994 in der korrigierten Ausgabe von 1996, 5.6.1.2]

3.1.2 Weitere Begriffe

ANMERKUNG Quellen von Definitionen ohne Verweisung in der vorliegenden Norm können den Literaturhinweisen entnommen werden.

3.1.2.1**Zugriffskontrolle****(en: access control)**

Sicherstellung, dass der Zugriff auf Werte autorisiert und eingeschränkt nach den Unternehmens- und Sicherheitsanforderungen erfolgt

[Quelle: ISO/IEC 27000:2009, 2.1]

3.1.2.2**Alarm****(en: alarm)**

Bedingung, deren Zustand beibehalten wird, bis die Bedingung nach einer gemeldeten Zustandsänderung beseitigt ist

BEISPIELE sind das Auftreten einer Alarmbedingung oder einer Rückkehrbedingung zum Normalbetrieb, die für einen entsprechenden UAP von möglicher Bedeutung ist.

3.1.2.3

Warnung

(en: alert)

Meldung einer Ereignisbedingung oder einer Alarmbedingung

3.1.2.4

Anwenden, Anwendung, Anwendungs-

(en: application)

(Verb) Vorgang des Anwendens

(Substantiv) System oder Problem, für das ein Computer angewendet wird; Programm, welches die Funktionen für Endbenutzer zur Verfügung stellt

(Adjektiv) oberste Protokollschicht in der ISO-Definition; Arten der Anwendung nach der Kritikalität

3.1.2.5

Anwendungsprozess

(en: application process)

Element, welches die Informationsverarbeitung für eine bestimmte Anwendung ausführt

3.1.2.6

asymmetrischer kryptografischer Algorithmus, asymmetrischer Verschlüsselungsalgorithmus

(en: asymmetric-key (cryptographic) algorithm)

kryptografischer Algorithmus mit einem öffentlichen Schlüssel

(en: public key cryptographic algorithm)

Algorithmus für die Verschlüsselung oder die entsprechende Entschlüsselung, bei dem sich die für die Ver- und Entschlüsselung verwendeten Schlüssel unterscheiden

[Quelle: ISO/IEC 10181-1:1996, 3.3.1]

3.1.2.7

Authentifizierung

(en: authentication)

Authentifizierung des Datenursprungs (3.1.1.27) und/oder Authentifizierung der Partnerinstanz (3.1.1.44)

Anmerkung 1 zum Begriff: Im allgemeinen Kontext der Informationssicherheit: Nachweis der Identität eines Benutzers, eines Prozesses oder eines Geräts, häufig als Vorbedingung, um den Zugriff auf Ressourcen in einem Informationssystem zuzulassen.

3.1.2.8

Authentifizierungscode

(en: authentication code)

vollständige oder abgeschnittene kryptografische Prüfsumme, die auf einer geeigneten Sicherheitsfunktion beruht (siehe 3.1.2.89)

Anmerkung 1 zum Begriff: Der Authentifizierungscode wird auch als Nachrichtenauthentifizierungscode (MAC) bezeichnet. Wird er in einem Kontext benutzt, in dem das Akronym MAC anders definiert ist, wie z. B. in Normen über lokale Netzwerke, wird er als Nachrichtenintegritätscode (MIC) bezeichnet.

[Quelle: ISO/IEC 19790:2006, 3.8, modifiziert durch den Vorsatz „vollständig oder abgeschnitten“]

3.1.2.9

Backbone-Netzwerk

(en: backbone network)

in der vorliegenden Norm nicht festgelegtes Netzwerk, im Allgemeinen mit der Netzwerktechnologie IPv6 oder IPv4, für das Routing zwischen dem drahtlosen Netzwerk nach dieser Norm und

- a) verbundenen Back-End-Geräten, die teilweise in dieser Norm festgelegt sind, wie Systemmanager, Sicherheitsmanager und Protokoll-Gateways; und
- b) Geräten, die die drahtlose TL, AL und die Managementprotokolle dieser Norm in natürlicher Form unterstützen

3.1.2.10**Backbone-Router****(en: backbone router)**

Router für die Übermittlung zwischen dem drahtlosen Netzwerk dieser Norm und einem Hochgeschwindigkeits-Backbone-Netzwerk

3.1.2.11**Datensicherung****(en: backup)**

Prozedur, Verfahren oder Hardware zur Wiederherstellung verlorener oder zerstörter Daten oder zur Aufrechterhaltung des Systembetriebs

[Quelle: ISO 2382-12:1988, 12.01.17]

3.1.2.12**Bandbreite****(en: bandwidth)**

in Abhängigkeit von Kontext der Angabe:

- analoge Bandbreite (Hz); numerische Differenz zwischen der oberen und der unteren Frequenz eines Frequenzbereichs
- digitale Bandbreite (bits); Datenmenge, die innerhalb eines gegebenen Zeitraums einen Kommunikationskanal durchlaufen kann

3.1.2.13**Black Channel****(en: black channel)**

Kommunikationskanal eines Sicherheitssystems ohne Sicherheitsfunktionen zusätzlich zur grundlegenden Kommunikationsfähigkeit

3.1.2.14**Blacklist****(en: blacklist)**

Liste von HF-Kanälen, über die die Übertragung verboten ist

Anmerkung 1 zum Begriff: Eine Blacklist gilt zeitweilig oder dauerhaft, lokal oder netzwerkweit.

3.1.2.15**Blockverschlüsselung****(en: block cipher)**

kryptografisches Element, das mit einem symmetrischen Schlüssel eine schlüsselabhängige pseudozufällige Permutation einer Bitfolge fester Größe erzeugt

3.1.2.16**Sammelaufruf****(en: broadcast)**

für alle Knoten vorgesehene Übertragung

Anmerkung 1 zum Begriff: Der Empfang eines Sammelaufrufs ist häufig auf bestimmte Schichten beschränkt, z. B. MAC- oder Netzwerkschicht.

Anmerkung 2 zum Begriff: Viele Protokolle unterer Schichten geben keine Quittierung für Sammelaufrufe.

3.1.2.17**kanonische Transfersyntax****(en: canonical transfer syntax)****vollständige Transfersyntax****(en: full transfer syntax)**

vollständige Codierung eines Objekts für eine Übertragung zwischen Geräten vor der Komprimierung

3.1.2.18

Verschlüsseln

(en: cipher)

kryptografisches Verfahren für den Schutz der Vertraulichkeit von Daten bestehend aus drei Komponenten: einem Verschlüsselungsalgorithmus, einem Entschlüsselungsalgorithmus und einem Verfahren zur Erzeugung von Schlüsseln

[QUELLE: wird in anderen ISO/IEC-Normen auf eine unbekannte Ausgabe von ISO/IEC 18033-1 zurückgeführt, für eine bessere Lesbarkeit abgestimmt]

3.1.2.19

Koexistenz

(en: coexistence)

Fähigkeit mehrerer Systeme, ihre Aufgaben in einer vorgegebenen Umgebung auszuführen, wobei sie nach ähnlichen Regeln handeln können oder nicht

3.1.2.20

komprimierte Transfersyntax

(en: compressed transfer syntax)

Codierung eines Objekts für eine Übertragung zwischen Geräten nach der Komprimierung

3.1.2.21

Konstruktionsoption

(en: construction option)

Menge von Leistungsmerkmalen, die ein Entwickler in ein Gerät aufnehmen oder daraus ausschließen kann

3.1.2.22

Vertrag

(en: contract)

Vereinbarung zwischen dem Systemmanager und einem Gerät im Netzwerk, die die Zuweisung von Netzwerkressourcen durch den Systemmanager umfasst, um einen bestimmten Kommunikationsbedarf dieses Geräts zu unterstützen

3.1.2.23

kryptografischer Algorithmus

(en: cryptographic algorithm)

Algorithmus auf der wissenschaftlichen Grundlage der Kryptografie, einschließlich von Verschlüsselungsalgorithmen, kryptografischen Hash-Algorithmen, digitalen Signaturalgorithmen und Schlüsselvereinbarungsalgorithmen

Anmerkung 1 zum Begriff: Beispiele für kryptografische Algorithmen sind Block- und Bitstromverschlüsselung und verschlüsselte Hash-Funktionen. Eine unverschlüsselte Hash-Funktion ist formal kein kryptografischer Algorithmus, obwohl es sich oft um eine Einwegfunktion mit einer ähnlichen Beständigkeit gegen Angriffe handelt und sie mit einem kryptografischen Algorithmus mit einem festen Schlüssel erzeugt wird. Die SHA-Familie der Hash-Funktionen ist so aufgebaut.

[Quelle: ISO/IEC 62443-1-1:2009, 3.2.34]

3.1.2.24

kryptografischer Schlüssel

(en: cryptographic key)

Schlüssel

(en: key)

Symbolfolge zur Steuerung des Ablaufs einer kryptografischen Transformation

[Quelle: ISO/IEC 19790:2006, 3.15]

mathematischer Wert, der benutzt wird

- a) in einem Algorithmus zur Erzeugung von verschlüsseltem Text aus Klartext oder umgekehrt, und
- b) zur Festlegung des Ablaufs einer kryptografischen Funktion (z. B. die synchronisierte Erzeugung des Schlüsselmaterials) oder zur Berechnung oder Validierung einer digitalen Signatur

[Quelle: ISO/IEC 62351-2:2008, 2.2.64]

3.1.2.25

kryptografische Schlüsselkomponente

(en: cryptographic key component)

Schlüsselkomponente

(en: key component)

in einer Sicherheitsfunktion benutzte(r) Parameter zur Ausführung einer kryptografischen Funktion

[Quelle: ISO/IEC 19790:2006, 3.16]

3.1.2.26

kryptografisches Modul

(en: cryptographic module)

in der kryptografischen Umgebung enthaltene Hardware, Software und/oder Firmware zur Umsetzung geeigneter Sicherheitsfunktionen

[Quelle: ISO/IEC 19790:2006, 3.17]

3.1.2.27

Kryptoperiode

(en: cryptoperiod)

Zeitspanne, für die die Anwendung eines spezifischen Schlüssels zugelassen ist oder in der die Schlüssel für ein gegebenes System oder eine gegebene Anwendung wirksam bleiben

[Quelle: ISO/IEC 11568-4:2007, 3.9]

3.1.2.28

Datenauthentizität

(en: data authenticity)

Gewissheit über die Informationsquelle

[Quelle: ISO/IEC/IEEE 8802-15-4:2010, 3.11]

3.1.2.29

Datenschlüssel

(en: data key)

Datenauthentifizierungsschlüssel

(en: data authenticating key)

kryptografischer Datenschlüssel

(en: data encrypting key)

kryptografischer Schlüssel für die Verschlüsselung, Entschlüsselung oder Authentifizierung von Daten

[Quelle: ISO/IEC 11568-2:2012, 3.5]

3.1.2.30

Implementierungsoption

(en: deployment option)

Menge von Leistungsmerkmalen, die ein Geräteentwickler in ein Gerät aufnehmen muss, über deren Nutzung der Endbenutzer oder dessen Vertreter (z. B. der Netzwerksicherheitsmanager) jedoch entscheiden kann

3.1.2.31

abgeleiteter Schlüssel

(en: derived key)

symmetrischer Schlüssel, der aus einem vorherigen symmetrischen Schlüssel abgeleitet wird

Anmerkung 1 zum Begriff: Solche Schlüssel dienen der Begrenzung der Kryptoperiode eines einzelnen Schlüssels, während die Anforderungen des Schlüsselarchivs erfüllt werden, sofern der unabhängige Schlüssel, von dem der abgeleitete Schlüssel abgeleitet wurde (eventuell über viele Erzeugungen von Ableitungen), vorher diese Archivanforderungen erfüllt hat.

3.1.2.32

(Schlüssel-)Zerstörung

(en: (key) destruction)

im Sinne der Sicherheit vollständige Löschung oder physische Zerstörung des Schlüsselmaterials, so dass es nicht wieder hergestellt werden kann

3.1.2.33

deterministischer Zufallsbitgenerator

(en: deterministic random bit generator)

- a) Zufallsbitgenerator, der durch Anwendung eines deterministischen Algorithmus auf einen geeigneten zufälligen Anfangswert, der als Startwert bezeichnet wird, und möglicherweise bestimmte Sekundäreingabewerte, von denen die Sicherheit des Zufallsbitgenerators nicht abhängt, eine zufällige Bitfolge erzeugt

Anmerkung 1 zum Begriff: Insbesondere können auch nicht deterministische Quellen Bestandteil dieser sekundären Eingabewerte sein.

[Quelle: ISO/IEC 18031:2011, 3.10]

- b) Prozess zur Erzeugung einer nicht vorhersagbaren Bitserie, die in dem Sinne zufällig ist, dass der Ausgabewert des Generators auf keine Weise beschrieben werden kann; der Prozess ist wirksamer, als die einfache Auflistung der gesamten Zeichenfolge der Ausgabewerte

Anmerkung 2 zum Begriff: Deterministische Zufallsbitgeneratoren besitzen nachweisbare Vorteile. Die Nichtvorhersagbarkeit ihrer Ausgabewerte hängt von der Nichtvorhersagbarkeit ihres Startwerts ab und bei Hybridgeneratoren von der Rate, mit der neue nichtvorhersagbare Eingabewerte (mit hoher Entropie) bezogen auf die Anzahl der erzeugten Ausgabebits eingegeben werden. Die gemeinsamen Quellen dieser Nichtvorhersagbarkeit können der Anmerkung in 3.1.2.94, nicht deterministischer Zufallsbitgenerator, entnommen werden.

3.1.2.34

Gerätesicherheits-Managementobjekt

(en: device security management object)

Anwendungssoftware innerhalb eines Geräts, die als lokaler Partner eines Sicherheitsmanagers wirkt

3.1.2.35

Duocast

(en: duocast)

Variante des Einzelaufrufs, bei der ein zweiter Empfänger so zeitgesteuert wird, dass er die DPDU mithört und innerhalb einer einzelnen D-Transaktion eine zweite Quittierung liefert

Anmerkung 1 zum Begriff: Duocast ist in Bild 84 grafisch dargestellt.

3.1.2.36

verschlüsselter Schlüssel

(en: encrypted key)

kryptografischer Schlüssel, der mit einer zugelassenen Sicherheitsfunktion mit einem Schlüssel zur Schlüsselverschlüsselung (KEK) verschlüsselt wird

Anmerkung 1 zum Begriff: Mit diesem Vorgang wird der Wert des zugrunde liegenden Klartextschlüssels verdeckt.

[Quelle: ISO/IEC 19790:2006, 3.25]

3.1.2.37

Verschlüsselung

(en: encryption)

umkehrbare Operation, bei dem Daten durch einen kryptografischen Algorithmus in verschlüsselten Text umgewandelt wird, so dass der Informationsinhalt der Daten verdeckt wird

[Quelle: ISO/IEC 9798-1:2010, 3.13]

3.1.2.38**Instanz****(en: entity)**

Person, Organisation, Gerät oder Prozess

3.1.2.39**flüchtiger Schlüssel****(en: ephemeral key)**

kryptografischer Schlüssel, der für jede Ausführung eines Schlüsseleinführungsprozesses erzeugt wird und der andere Anforderungen des Schlüsseltyps erfüllt (z. B. für jeden Nachrichtenaustausch oder jede Sitzung eindeutig)

Anmerkung 1 zum Begriff: In bestimmten Fällen werden flüchtige Schlüssel innerhalb einer einzigen Sitzung mehr als einmal benutzt (z. B. bei Sammelaufrufen), wobei der Absender nur ein flüchtiges Schlüsselpaar je Nachricht erzeugt und der private Schlüssel (dieses Paares) mit dem öffentlichen Schlüssel jedes Empfängers gesondert kombiniert wird.

3.1.2.40**Ereignis****(en: event)**

vorübergehende (d. h. zustandslose) Bedingung, mit der gemeldet wird, wenn etwas geschehen ist

BEISPIELE sind das Auftreten einer Alarmbedingung oder einer Rückkehrbedingung zum Normalbetrieb, die für einen entsprechenden UAP von möglicher Bedeutung ist.

3.1.2.41**Feldgerät****(en: field device)**

technisches Gerät, das so konstruiert ist, dass es dem Anlagenbetrieb standhält, und das über DPDUs und Protokolle höherer Schichten in Übereinstimmung mit der vorliegenden Norm kommuniziert

Anmerkung 1 zum Begriff: Feldgeräte schließen Router, Sensoren und Aktoren ein.

3.1.2.42**Feldnetzwerk****(en: field network)**

Aufbau aus zwei oder mehr Feldgeräten, die mit dem in der vorliegenden Norm definierten drahtlosen Protokoll verbunden sind

3.1.2.43**Feld-Router****(en: field router)**

Router innerhalb eines Feldnetzwerks, der gleichzeitig ein Feldgerät darstellt (d. h. kein Backbone-Router)

3.1.2.44**Kommunikation durch Anwendung eines Fremdprotokolls****(en: foreign protocol application communication)**

optimierte Übermittlung von PDUs oder Teilen von PDUs von einem ersten Protokoll innerhalb eines zweiten Protokolls durch selektiven Gebrauch von Caching, Komprimierung, Adressenumwandlung und Proxy-Verfahren

3.1.2.45**Fragment****(en: fragment)**

Segment

Anmerkung 1 zum Begriff: Fragment und Fragmentierung sind von IETF in Internetprotokollspezifikationen benutzte Begriffe zur Beschreibung der OSI-Begriffe Segment und Segmentierung. In der vorliegenden Norm werden die Begriffe Fragment und Segment im Grunde synonym benutzt, wobei Fragment in der Regel in der Vermittlungsschicht und mitunter in anderen Protokollschichten benutzt wird.

3.1.2.46

Gateway

(en: gateway)

Funktion (eines Geräts), die als Protokollübersetzer zwischen einer AE gemäß der vorliegenden Norm und anderen, verschiedenartigen AEs wirkt

3.1.2.47

Hash-basierter Nachrichtenauthentifizierungscode

(en: hash-based message authentication code)

Nachrichtenauthentifizierungscode, der eine geeignete verschlüsselte Hash-Funktion benutzt

Anmerkung 1 zum Begriff: Diese Definition wurde aus der zweiten Ausführung von ISO/IEC 9797-2 verallgemeinert, die sich auf die HMAC-Konstruktion bezieht, welche auch in FIPS 198A [USA] festgelegt ist.

[Quelle: ISO/IEC 9797-2:2011, verallgemeinert]

3.1.2.48

Hash-Funktion

(en: hash function)

Funktion zur Abbildung von Bitfolgen auf Bitfolgen fester Länge, die die folgenden zwei Eigenschaften erfüllen: für einen gegebenen Ausgabewert ist es mathematisch unmöglich, auf dessen ursprünglichen Eingabewert zurückzuschließen; für einen gegebenen Eingabewert ist es mathematisch unmöglich, einen zweiten Eingabewert zu finden, der denselben Ausgabewert ergibt

Anmerkung 1 zum Begriff: Die mathematische Machbarkeit hängt von den spezifischen Sicherheitsanforderungen und der Sicherheitsumgebung ab.

Anmerkung 2 zum Begriff: Siehe Anmerkung von 3.1.2.23.

[Quelle: ISO/IEC 9796-2:2010, 3.6]

3.1.2.49

Hash-Wert

(en: hash value)

vollständiges oder abgeschnittenes Ergebnis nach der Anwendung einer Hash-Funktion auf Informationen

3.1.2.50

Identität

(en: identity)

kennzeichnende Eigenschaft oder Persönlichkeit einer Person oder Instanz

3.1.2.51

unabhängiger Schlüssel

(en: independent key)

symmetrischer Schlüssel, der aus einer Bitquelle hoher Entropie und nicht aus einem vorherigen Schlüssel abgeleitet wird

3.1.2.52

Infrastruktur

(en: infrastructure)

technische Strukturen, die die Datenkommunikation innerhalb einer Anlage unterstützen

BEISPIEL Beispiele für eine Infrastruktur sind Teile des IT-Netzes einer Anlage, etwa unter Anwendung von IEEE 802.3 oder IEEE 802.11 oder IEC 61158, Typ 10 (PROFINet), oder IEC 61158, Typ 9 (FOUNDATION™ Fieldbus HSE).¹

¹ PROFIBUS und Fieldbus Foundation sind die Markennamen verschiedener Handelsorganisationen. Diese Information ist zum Vorteil der Anwender der Norm angegeben und stellt keine Empfehlung für die Markennameninhaber oder eines ihrer Produkte dar. Für die Übereinstimmung mit diesem Profil ist die Verwendung des Markennamens nicht notwendig. Die Anwendung der Markennamen muss durch den Markennameninhaber genehmigt werden.

3.1.2.53**Initialisierungsvektor****(en: initialization vector)**

Bitblock, der notwendig ist, damit eine kryptografische Verschlüsselung im Streaming-Betrieb einen einmaligen Bitstrom unabhängig von anderen Bitströmen, die mit derselben kryptografischen Verschlüsselung erzeugt werden, generieren kann

3.1.2.54**interoperabel****(en: interoperable)**

Fähigkeit zur Zusammenarbeit, um eine festgelegte Menge von Funktionen auszuführen

BEISPIEL Zwei Geräte sind interoperabel, wenn sie zusammenarbeiten können, um die in einer Systemkonfiguration festgelegten Funktionen ausführen zu können.

[Quelle: ISO/IEC 61499-4:2005, 3.5]

3.1.2.55**Kerberos-Protokoll****(en: Kerberos protocol)**

spezifisches Netzwerk-Authentifizierungsprotokoll, mit dem über ein unsicheres Netzwerk kommunizierende Einzelpersonen auf sichere Weise gegenseitig ihre Identität prüfen können

3.1.2.56**Schlüsselvereinbarung****(en: key agreement)**

Einführung eines vorher vereinbarten, geheimen Schlüssels zwischen Instanzen auf eine Weise, dass keine von ihnen den Wert dieses Schlüssels vorher bestimmen kann

[Quelle: ISO/IEC 11770-1:2010, 2.13]

3.1.2.57**Schlüsselarchiv****(en: key archive)**

Verschlüsselungssystem mit der Fähigkeit einer Ersatzentschlüsselung, das es berechtigten Personen (Benutzern, Zuständigen einer Organisation und Beamten offizieller Stellen) ermöglicht, unter bestimmten vorgeschriebenen Bedingungen verschlüsselten Text mit Hilfe von Informationen zu entschlüsseln, die von einer oder mehreren vertrauenswürdigen Stellen bereitgestellt werden, welche spezielle Datenwiederherstellungsschlüssel besitzen, die sich nicht notwendigerweise von den zur Verschlüsselung der Information benutzten Schlüsseln unterscheiden müssen

3.1.2.58**Schlüsselzentrale****(en: key center)**

zentralisierter Schlüsselverteilungsprozess, gewöhnlich unter Anwendung eines gesonderten Computersystems, der zur Verschlüsselung und Verteilung von T-Schlüsseln, die von einer Benutzergemeinschaft benötigt werden, Schlüssel zur Schlüsselverschlüsselung (KEK) benutzt

Anmerkung 1 zum Begriff: Schlüsselzentralen sind in der Regel zertifiziert und auf eine zugelassene, unabhängige Prüfstelle rückführbar, so dass sie die Anforderungen von ISO/IEC 19790 (entspricht FIPS 140-2) für kryptografische Module der Ebene 3 oder der Ebene 4 erfüllen.

3.1.2.59**Schlüsselbestätigung****(en: key confirmation)**

Zusicherung für eine Instanz, dass eine andere bezeichnete Instanz im Besitz des richtigen Schlüssels ist

[Quelle: ISO/IEC 11770-1:2010, 2.16]

3.1.2.60

Schlüsselderegistrierung

(en: key de-registration)

Kennzeichnung aller Datensätze und der Assoziationen des Schlüsselmaterials zur Angabe, dass der Schlüssel nicht mehr benutzt wird

3.1.2.61

Schlüsselableitung

(en: key derivation)

Prozess, mit dem ein oder mehrere Schlüssel aus einem vorher vereinbarten, geheimen Schlüssel und anderen Informationen abgeleitet werden

3.1.2.62

Schlüsselverteilung

(en: key distribution)

Weitergabe eines Schlüssels und von anderem Verschlüsselungsmaterial von einer Instanz, der der Schlüssel entweder gehört oder die den Schlüssel erzeugt, zu einer anderen Instanz, die den Schlüssel benutzen soll

3.1.2.63

Schlüsselverteilungszentrale

(en: key distribution center)

vertrauenswürdige Instanz, die Schlüssel erzeugt oder erwirbt und die Schlüssel an kommunizierende Stellen verteilt und die mit jeder dieser Stellen vorher einen eindeutigen symmetrischen Schlüssel vereinbart hat

[Quelle: ISO/IEC 11770-1:2010, 2.22]

3.1.2.64

Schlüssel zur Schlüsselverschlüsselung

(en: key encryption key)

kryptografischer Schlüssel zur Ver- oder Entschlüsselung anderer Schlüssel

Anmerkung 1 zum Begriff: Bei der bewährten Vorgehensweise wird die Verwendung von symmetrischen (geheimen) KEKs auf eine Schlüsselverpackung und nicht die Schlüsselweitergabe oder die Anwendung als Sitzungsschlüssel (d. h. Datenschlüssel) beschränkt.

Anmerkung 2 zum Begriff: KEKs können eine Hierarchie bilden. In der vorliegenden Norm werden KEKs häufig als „Masterschlüssel“ bezeichnet, obwohl die beiden Begriffe nicht als Synonyme gelten.

3.1.2.65

Schlüsselhinterlegung

(en: key escrow)

- a) Managementfunktion, mit der eine berechnete Stelle auf einen privaten kryptografischen Ersatzschlüssel zugreifen kann

Anmerkung 1 zum Begriff: Dabei kann es sich um eine rechtliche Forderung handeln, damit Beamte offizieller Stellen Zugriff auf einen privaten geheimen Schlüssel einer Instanz und/oder CA erhalten.

[Quelle: ISO/IEC 21188:2006, 3.34]

- b) Verschlüsselungssystem mit einer Fähigkeit einer Ersatzentschlüsselung, das es berechtigten Personen (Benutzern, Zuständigen einer Organisation und Beamten offizieller Stellen) ermöglicht, unter bestimmten vorgeschriebenen Bedingungen verschlüsselten Text mit Hilfe von Informationen zu entschlüsseln, die von einer oder mehreren vertrauenswürdigen Stellen bereitgestellt werden, welche spezielle Datenwiederherstellungsschlüssel besitzen, die sich nicht notwendigerweise von den zur Verschlüsselung der Information benutzten Schlüsseln unterscheiden müssen

3.1.2.66

Schlüsseleinführung

(en: key establishment)

- a) Prozess, mit dem ein vorher vereinbarter Schlüssel einer oder mehreren Instanzen zur Verfügung gestellt wird, wobei der Prozess eine Schlüsselvereinbarung oder eine Schlüsselweitergabe einschließt

[Quelle: ISO/IEC 11770-1:2010, 2.23]

- b) Prozess, mit dem kryptografische Schlüssel unter kryptografischen Modulen von Hand (z. B. Key Loader), automatisch (z. B. Schlüsselweitergabe- und/oder -vereinbarungsprotokolle) oder durch eine Kombination beider Verfahren (bestehend aus Schlüsselweitergabe und Schlüsselvereinbarung) sicher verteilt werden

3.1.2.67

Installation von Schlüsselmaterial

(en: **keying material installation**)

Installation von Schlüsselmaterial für den operativen Einsatz

3.1.2.68

Schlüsselmanagement

(en: **key management**)

Regulierung und Durchführung von Erzeugung, Registrierung, Zertifizierung, Deregistrierung, Verteilung, Installation, Speicherung, Archivierung, Aufhebung, Ableitung und Löschung von Schlüsselmaterial entsprechend einer Sicherheitsrichtlinie

[Quelle: ISO/IEC 11770-1:2010, 2.28]

3.1.2.69

Schlüsselmanagementarchiv

(en: **key management archive**)

Ablage zur Aufbewahrung von Schlüsselmaterial von historischem Interesse

3.1.2.70

Infrastruktur des Schlüsselmanagements

(en: **key management infrastructure**)

Rahmen und Dienste zur Generierung, Herstellung, Verteilung, Lenkung, Darstellung und Löschung des gesamten kryptografischen Materials einschließlich von symmetrischen Schlüsseln sowie Signierung öffentlicher Schlüssel und Erzeugung eigener statischer und flüchtiger asymmetrischer Schlüsselpaare

Anmerkung 1 zum Begriff: Dazu gehören alle Elemente (Hardware, Software, andere Ausrüstung und Dokumentation), Anlagen, Personal, Verfahren, Normen und Informationen, aus denen das System besteht, welches die Zustellung und Verteilung kryptografischer Produkte und Dienste zum Endbenutzer verwaltet und unterstützt.

Anmerkung 2 zum Begriff: Schlüsselmanagementdienste umfassen Schlüsselbestellung, Verteilung, Erneuerung, Aktualisierung von Attributen des Schlüsselmaterials, Aufhebung des Zertifikats, Schlüsselwiederherstellung und die Verteilung, Darstellung, Rückverfolgung und Lenkung der Software, die entweder Sicherheitsfunktionen des Schlüsselmaterials oder kryptografische Funktionen ausführt.

3.1.2.71

Schlüsselmanager

(en: **key manager**)

Infrastrukturgerät des Schlüsselmanagers, das Schlüsselmanagementdienste zur Verfügung stellt

3.1.2.72

(asymmetrisches) Schlüsselpaar

(en: **(asymmetric) key pair**)

Paar zusammengehöriger Schlüssel, wobei der private Schlüssel die private Umwandlung und der öffentliche Schlüssel die öffentliche Umwandlung festlegt

Anmerkung 1 zum Begriff: Ein Schlüsselpaar wird zusammen mit asymmetrischen kryptografischen Algorithmen benutzt.

[Quelle: ISO/IEC 11770-1:2010, 2.2]

3.1.2.73

Schlüsselwiederherstellung

(en: key recovery)

Mechanismen und Prozesse, die es berechtigten Instanzen ermöglichen, Schlüsselmaterial aus sicheren Schlüsselreserve- oder -archivspeichern wiederherzustellen

3.1.2.74

Schlüsselregistrierung

(en: key registration)

Vorgang der offiziellen Eintragung des Schlüsselmaterials von einer Registrierungsstelle

3.1.2.75

Schlüsselaufhebung

(en: key revocation)

Vorgang, mit dem betroffenen Instanzen vor dem Ende der festgelegten Kryptoperiode des Schlüsselmaterials mitgeteilt wird, dass dieses Schlüsselmaterial betrieblich nicht mehr genutzt werden sollte

3.1.2.76

Schlüsselweitergabe

(en: key transport)

Vorgang der Übergabe eines Schlüssels von einer Instanz zu einer anderen Instanz mit einem geeigneten Schutz

Anmerkung 1 zum Begriff: Im Zusammenhang mit einem öffentlichen (asymmetrischen) Verschlüsselungsalgorithmus wird das Schlüsselmaterial mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und anschließend mit dem privaten Schlüssel des Empfängers entschlüsselt. Im Zusammenhang mit einem symmetrischen Algorithmus wird das Schlüsselmaterial mit einem vorher von den beiden Stellen vereinbarten Schlüssel zur Schlüsselverschlüsselung (KEK) verpackt.

[Quelle: ISO/IEC 11770-1:2010, 2.33]

3.1.2.77

Schlüsselaktualisierung

(en: key update)

an einem kryptografischen Schlüssel durchgeführte Funktion zur Berechnung eines neuen zugehörigen Schlüssels

3.1.2.78

Schlüsselnutzungsdauer

(en: key usage period)

entweder die Absendernutzungsdauer oder die Empfängernutzungsdauer eines symmetrischen Schlüssels

3.1.2.79

Schlüsselverpackung

(en: key wrapping)

Verfahren zur Verschlüsselung von Schlüsseln (zusammen mit der zugehörigen Integritätsfunktion), die sowohl Vertrauenswürdigkeit als auch den Schutz der Integrität unter Anwendung eines symmetrischen Schlüssels bietet

3.1.2.80

Schlüssel zur Schlüsselverpackung

(en: key wrapping key)

(symmetrischer) Schlüssel zur Schlüsselverpackung (KEK)

3.1.2.81

Schlüsselmaterial

(en: keying material)

Daten, die zur Einführung und Aufrechterhaltung kryptografischer Verschlüsselungsbeziehungen notwendig sind

BEISPIEL Schlüssel, Initialisierungswerte

[Quelle: ISO/IEC 11770-1:2010, 2.27]

3.1.2.82

Latenzzeit

(en: **latency**)

Dauer von der Erzeugung der Daten in der Datenquelle bis zur Bereitstellung im Zielgerät

Anmerkung 1 zum Begriff: Die vorgesehenen Messpunkte sind a) technische Geräte oder b) Schichtgrenzen innerhalb von mehrschichtiger Software (z. B. von der sendenden Transportfunktion zur empfangenden Transportfunktion oder von der sendenden Anwendung zum sendenden Modem).

3.1.2.83

Lease

(en: **lease**)

differenzierte Zuweisung der Kommunikationsressource je Sitzung an einem GIAP

3.1.2.84

geringstes Recht

(en: **least privilege**)

Sicherheitsgrundsatz, nach dem Zugriffsrechte (z. B. Programmausführungsrechte, Dateiänderungsrechte) von berechtigten Personen und deren Vertretern im Netz auf die geringsten notwendigen Rechte zur Ausführung ihrer Aufgaben beschränkt werden

3.1.2.85

Übertragungsstrecke

(en: **link**)

kurzzeitiger oder dauerhafter Verbindungspfad zwischen zwei oder mehr Geräten für die Sendung oder den Empfang von Nachrichten

3.1.2.86

Masterschlüssel

(en: **master key**)

kryptografischer Schlüssel zur Ableitung anderer Schlüssel

Anmerkung 1 zum Begriff: Bei der bewährten Vorgehensweise ist die Nutzung von Masterschlüsseln als Sitzungsschlüssel (d. h. Datenschlüssel), was deren Kryptoanalyse vereinfachen würde, verboten. Sie dürfen als KEKs häufig auf der obersten Ebene einer KEK-Hierarchie eingesetzt werden.

3.1.2.87

Maschentopologie

(en: **mesh topology**)

Netztopologie, bei der redundante, physikalisch verschiedene Routing-Pfade zwischen jedem Paar von Netzknoten zur Verfügung stehen

Anmerkung 1 zum Begriff: Mit einer drahtlosen Netztopologie kann der Deckungsgrad über die Multihop-Fähigkeit erweitert und/oder die Kommunikationszuverlässigkeit durch die Bereitstellung redundanter Pfade zwischen Geräten erhöht werden.

3.1.2.88

Nachrichtenauthentifizierung

(en: **message authentication**)

Feststellung, dass eine Nachricht von einem Mitglied einer berechtigten Gruppe von Kommunizierenden erstellt und seitdem nicht verändert wurde

Anmerkung 1 zum Begriff: Dieser Vorgang wird auch als PDU-Authentifizierung bezeichnet.

3.1.2.89

Nachrichtenauthentifizierungscode

(en: message authentication code)

Nachrichtenintegritätscode

(en: message integrity code)

mit einem symmetrischen Schlüssel erzeugte kryptografische Prüfsumme, die gewöhnlich an Daten angefügt wird, um ähnlich einer digitalen Signatur die Datenintegrität und die Authentifizierung der Quelle zu sichern

[Quelle: ISO/IEC 26907:2009, 4.16]

3.1.2.90

Nachrichtenauthentifizierungscode-Algorithmus

(en: message authentication code algorithm)

Algorithmus zur Berechnung einer Funktion, die Bitfolgen und einen geheimen Schlüssel auf Bitfolgen fester Länge abbildet und die folgenden beiden Eigenschaften erfüllt:

- für jeden Schlüssel und jede Eingabefolge kann die Funktion erfolgreich berechnet werden;
- für jeden festen Schlüssel und unter der Voraussetzung, dass der Schlüssel vorher nicht bekannt ist, ist es mathematisch unmöglich, den Funktionswert einer neuen Eingabefolge zu berechnen, selbst bei Kenntnis einer Menge von Eingabefolgen und entsprechender Funktionswerte, wenn der Wert der i -ten Eingabefolge nach Untersuchung des ersten Wertes der $i-1$ -ten Funktionswerte (für ganzzahlige Werte von $i > 1$) ausgewählt worden ist

[Quelle: ISO/IEC 9797-1:2011, 3.10]

3.1.2.91

MIC-Berechnungssyntax

(en: MIC-computation syntax)

konkrete Darstellung einer n -SDU-verbundenen Protokollinformation, die gewöhnlich über einen vorgesetzten Pseudo-Header angefügt wird und für die Anbindung von selektiven n -Adressen und der n -PCI und mitunter selektiven $(n-1)$ -Adressen und einer $(n-1)$ -PCI an die n -SDU benutzt wird, bevor ein Integritätsprüfcode (MIC) für diesen Verbund berechnet wird

3.1.2.92

Gruppenaufruf

(en: multicast)

Nachrichtenübermittlung von einer Quelle zu einer Menge vorgesehener Empfänger

Anmerkung 1 zum Begriff: Die Teilnehmer der Menge sind entweder unbestimmt oder bestimmt, wobei letztere eine Nullmenge sein kann.

Anmerkung 2 zum Begriff: Ein Sammelaufruf ist eine besondere Form des Gruppenaufrufs gewöhnlich mit einer unbestimmten Menge vorgesehener Empfänger. Siehe auch Einzelaufruf.

Anmerkung 3 zum Begriff: Im Gegensatz zum Sammelaufruf wird der Gruppenaufruf in der vorliegenden Norm nicht unterstützt.

3.1.2.93

Netzwerk-Managementobjekt

(en: network management object)

Anwendungssoftware innerhalb eines Geräts, die als lokaler Partner eines Netzwerkmanagers wirkt

3.1.2.94

nicht-deterministischer Bitgenerator

(en: non-deterministic bit generator)

Zufallsbitgenerator, dessen Sicherheit von der Abtastung einer Entropiequelle abhängt

Anmerkung 1 zum Begriff: Quellen solcher Bits sind der Lawinendurchbruch einer Zenerdiode, Schrotrauschen, Wärmerauschen, radioaktiver Zerfall, kosmische Strahlung usw.

Anmerkung 2 zum Begriff: Zur Bereinigung ihrer Ausgabewerte und zur Ermittlung von Fehlern in dem Kreis, der die Zufälligkeit sichert, ist eine Nachverarbeitung solcher Rauschquellen erforderlich. Nur der nachverarbeitete Bitstrom ist als Startwert für einen deterministischen Bitgenerator geeignet.

[Quelle: ISO/IEC 18031:2011, 3.23]

3.1.2.95

Nicht-Abstreitbarkeit

(en: non-repudiation)

Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachenden Instanzen nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von Instanzen an dem Ereignis zu entscheiden

Anmerkung 1 zum Begriff: Im allgemeinen Kontext der Informationssicherheit bietet die Nicht-Abstreitbarkeit die Zusicherung, dass der Absender der Informationen einen dauerhaften Zustellungsnachweis oder der Empfänger einen dauerhaften Nachweis der Absenderidentität erhält, so dass die Stelle, die den nicht-abstreitbaren Nachweis erhalten hat, später nicht glaubhaft bestreiten kann, die Information verarbeitet zu haben.

[Quelle: ISO/IEC 27000:2009, 2.27]

3.1.2.96

Nonce

(en: nonce)

einmalig verwendete Zahl oder Wert, bei dem die Aussicht auf eine Wiederholung (meistens) gering ist

3.1.2.97

operative Phase

(en: operational phase)

operativer Einsatz

(en: operational use)

Phase im Lebenszyklus des Schlüsselmaterials, in der dieses für kryptografische Standardvorgänge benutzt wird

3.1.2.98

operative Speicherung

(en: operational storage)

normale Speicherung von operativem Schlüsselmaterial während dessen Kryptoperiode

3.1.2.99

Absendernutzungsdauer

(en: originator usage period)

Dauer in der Kryptoperiode eines symmetrischen Schlüssels, während der Daten kryptografisch geschützt sein können

3.1.2.100

PDU-Authentifizierung

(en: PDU authentication)

siehe 3.1.2.88, Nachrichtenauthentifizierung

3.1.2.101

Schutzdauer

(en: period of protection)

Zeitspanne, während der die Integrität und/oder die Vertrauenswürdigkeit eines Schlüssels aufrechterhalten werden müssen

3.1.2.102

Klartext

(en: plaintext)

unverschlüsselte Information (bezogen auf einen Ver- oder Entschlüsselungsvorgang)

Anmerkung 1 zum Begriff: In der Regel ist die Klartexteingabe in eine Verschlüsselungsoperation noch nicht verschlüsselt, aber in einigen Fällen ist die Eingabe selbst eine Ausgabe einer anderen kryptografischen Operation.

[Quelle: ISO/IEC 10116:2006, 3.11, modifiziert durch einen eingeklammerten Kommentar]

3.1.2.103

Management auf der Grundlage einer Sicherheitsrichtlinie

(en: **policy-based management**)

administrativer (innerbetrieblicher) Ansatz zur Vereinfachung des Managements eines vorgegebenen Systems über das Aufstellen von Sicherheitsrichtlinien zur Behandlung von Situationen, deren Eintreten nachvollziehbar möglich ist

3.1.2.104

privater Schlüssel

(en: **private key**)

(kryptografischer) Schlüssel eines asymmetrischen Schlüsselpaares einer Instanz, der privat bleibt

Anmerkung 1 zum Begriff: In einem asymmetrischen (öffentlichen) Verschlüsselungssystem ist der private Schlüssel an einen öffentlichen Schlüssel gebunden. Der private Schlüssel ist nur dem Eigentümer des Schlüsselpaares bekannt und wird verwendet für:

- die Berechnung des entsprechenden öffentlichen Schlüssels;
- die Berechnung einer digitalen Signatur, die durch den entsprechenden öffentlichen Schlüssel verifizierbar ist;
- die Entschlüsselung der Daten, die mit dem entsprechenden öffentlichen Schlüssel verschlüsselt worden sind; oder
- die Berechnung eines Teils gemeinsam genutzter Daten zusammen mit anderen Informationen.

[Quelle: ISO/IEC 11770-1:2010, 2.35]

3.1.2.105

Pseudo-Header

(en: **pseudo-header**)

Information, die einer PDU vor der Berechnung eines MIC für die PDU logisch vorangestellt wird, die aber ansonsten in der PDU nicht enthalten ist

3.1.2.106

öffentlicher Schlüssel

(en: **public key**)

Schlüssel eines asymmetrischen Schlüsselpaares einer Instanz, der in der Regel ohne Gefährdung der Sicherheit öffentlich verfügbar gemacht werden kann

[Quelle: ISO/IEC 11770-1:2010, 2.35]

3.1.2.107

Zertifikat des öffentlichen Schlüssels

(en: **public key certificate**)

Informationen über den öffentlichen Schlüssel einer Instanz, die von einer Zertifizierungsstelle eingetragen sind

Anmerkung 1 zum Begriff: Mit Zusatzinformationen im Zertifikat kann die Kryptoperiode des Schlüssels angegeben werden und wie er anzuwenden ist.

[Quelle: ISO/IEC 11770-1:2010, 2.37]

3.1.2.108

Empfängernutzungsdauer

(en: **recipient usage period**)

Dauer in der Kryptoperiode eines symmetrischen Schlüssels, während der die geschützte Information verarbeitet wird

Anmerkung 1 zum Begriff: Diese Dauer erstreckt sich häufig über die zulässige Absendernutzungsdauer hinaus.

3.1.2.109**dynamisches Störausgleichsverhalten****(en: resilience)**

Fähigkeit einer Funktionseinheit, beim Auftreten von Fehlern oder Abweichungen eine geforderte Funktion weiterhin auszuführen

[Quelle: ISO/IEC 2382-14:1997, 14.04.06]

3.1.2.110**Sperrfrist****(en: retention period)**

Mindestdauer, die ein Schlüssel oder andere mit der Verschlüsselung im Zusammenhang stehende Informationen in einem Archiv aufbewahrt werden sollten

3.1.2.111**Stabilität****(en: robustness)**

Umfang, in dem ein System oder ein Bauteil beim Auftreten von ungünstigen Eingabewerten oder bei ungünstigen Umgebungsbedingungen einwandfrei funktionsfähig ist; vergleiche Fehlzustandstoleranz, Fehler-toleranz

[Quelle: ISO/IEC/IEEE 24765:2010, 3.2601]

3.1.2.112**Router****(en: router)**

Gerät, das NPDU's in einem Computernetzwerk auf der Basis von Informationen der Vermittlungsschicht befördert

3.1.2.113**geheimer Schlüssel****(en: secret key)**

mit symmetrischen Verschlüsselungsverfahren von einer festgelegten Menge von Instanzen verwendeter Schlüssel

[Quelle: ISO/IEC 11770-3:2008, 3.38]

3.1.2.114**sicheres Kommunikationsprotokoll****(en: secure communications protocol)**

Kommunikationsprotokoll, das eine angemessene Vertraulichkeit, Authentifizierung, Integrität des Inhalts und Nachrichtenlaufzeitüberwachung bereitstellt

3.1.2.115**Sicherheitsassoziation****(en: security association)**

Beziehung zwischen zwei oder mehr Instanzen, für die Attribute (Zustandsinformationen und Vorschriften) bestehen, nach denen die Bestimmungen von Sicherheitsdiensten, die diese Instanzen betreffen, geregelt werden

[Quelle: ISO/IEC 10745:1995, 0000]

3.1.2.116**Sicherheitsdomäne****(en: security domain)**

Menge von Werten und Ressourcen, die einer gemeinsamen Sicherheitsrichtlinie unterliegen

Anmerkung 1 zum Begriff: Sicherheitsdomänen sind oft so organisiert (z. B. hierarchisch), dass sie größere Domänen bilden.

[Quelle: ISO/IEC 18028-3:2005, 3.19]

3.1.2.117

Sicherheitsmanager

(en: security manager)

Anwendungssoftware, die verschiedene Aspekte der operativen Sicherheit eines Netzwerks mit mehreren Geräten in der Regel durch Wechselwirkung mit Gerätesicherheits-Managementobjekten (DSMO) im (in den) überwachten Gerät(en) überwacht

Anmerkung 1 zum Begriff: Ein Netzwerksicherheitsmanager ist häufig ein dediziertes Gerät, das sowohl physikalisch als auch konstruktiv geschützt ist. (Siehe ISO/IEC 19790 (entspricht FIPS 140-2) und NIST/CSE Cryptographic Module Validation Program, <http://csrc.nist.gov/cryptval/cmvp.htm>).

3.1.2.118

Sicherheitsdienste

(en: security services)

Mechanismen zur Sicherung von Vertraulichkeit, Datenintegrität, Authentifizierung und/oder Nicht-Abstreitbarkeit von Informationen

3.1.2.119

Aufgabentrennung

(en: separation of duties)

Sicherheitsgrundsatz, nach dem kritische Funktionen unter verschiedenen Mitarbeitern aufgeteilt werden, im Bestreben sicherzustellen, dass keine Einzelperson genug Informationen oder Zugriffsrechte besitzt, um schädigende Betrugsdelikte zu begehen

3.1.2.120

Sitzung

(en: session)

T-Assoziation

3.1.2.121

Sitzungsschlüssel

(en: session key)

T-Schlüssel

(en: T-key)

kurzzeitiger Datenschlüssel, der von TLEs benutzt wird

3.1.2.122

Signaturerzeugung

(en: signature generation)

Anwendung eines digitalen Signaturalgorithmus und eines privaten Schlüssels zur Erzeugung einer digitalen Signatur für Daten

3.1.2.123

Signaturauthentifizierung

(en: signature authentication)

Anwendung eines digitalen Signaturalgorithmus und eines öffentlichen Schlüssels zur Überprüfung einer digitalen Signatur für Daten

3.1.2.124

Quellenauthentifizierung

(en: source authentication)

Bestätigung, dass die Quelle der Daten die geforderte Quelle ist

3.1.2.125

aufgeteiltes Wissen

(en: split knowledge)

Vorgang, bei dem ein kryptografischer Schlüssel in mehrere Schlüsselkomponenten aufgeteilt wird, die einzeln keine Kenntnisse über den ursprünglichen Schlüssel offenlegen als eventuell dessen Größe und die anschließend in einer Anzahl von vordefinierten Gruppierungen der mehrfachen spezifischen Schlüssel zur Wiederherstellung des ursprünglichen Schlüssels zusammengefasst werden können

3.1.2.126**statischer Schlüssel****(en: static key)**

Schlüssel, der kein flüchtiger Schlüssel ist und für eine relativ lange Anwendungsdauer vorgesehen ist, in der Regel in aufeinander folgenden Aufrufen eines Einführungsschemas für einen kryptografischen Schlüssel

3.1.2.127**Bitstromverschlüsselung****(en: stream cipher)**

kryptografisches Element, das einen symmetrischen Schlüssel und einen Initialisierungsvektor benutzt und mit ununterbrochenen Strömen von Eingabewerten arbeitet anstatt mit festen Blöcken

3.1.2.128**Teilnetz****(en: subnet)**

Teilnetzwerk, d. h. Teil eines vollständigen Netzwerks, entweder in der Sicherungsschicht oder der Vermittlungsschicht (Schichten 2 oder 3 des OSI-Basis-Referenzmodells)

3.1.2.129**Überrahmen****(en: superframe)**

Zusammenfassung von Zeitschlitzten mit gemeinsamer Wiederholungsperiode und möglicherweise anderen gemeinsamen Attributen

3.1.2.130**symmetrischer Schlüssel****(en: symmetric key)**

geheimer Schlüssel, der von zwei oder mehr Stellen gemeinsam benutzt wird und sowohl für die Ver- und Entschlüsselung als auch für die Berechnung und Verifizierung des Nachrichtenintegritätscodes benutzt werden kann

[Quelle: ISO/IEC 26907:2009, 4,27]

3.1.2.131**(kryptografischer) Algorithmus mit symmetrischem Schlüssel****(en: symmetric-key (cryptographic) algorithm)**

kryptografischer Algorithmus, der den gleichen (gewöhnlich geheimen) Schlüssel für eine Operation und deren Umkehrung (z. B. Ver- und Entschlüsselung) benutzt

3.1.2.132**Systeminitialisierung****(en: system initialization)**

in Bezug auf die Sicherheit Einrichtung und Konfiguration eines Systems für einen sicheren Betrieb

3.1.2.133**Systemmanager****(en: system manager)**

Anwendungssoftware, die verschiedene operative Aspekte eines Netzwerks mit mehreren Geräten mit Ausnahme der Sicherheit in der Regel durch Wechselwirkung mit Netzwerk-Managementobjekten im (in den) überwachten Gerät(en) überwacht

Anmerkung 1 zum Begriff: Ein Netzwerkmanager überwacht entweder ein gesamtes Netzwerk mit mehreren Geräten oder er wirkt untergeordnet zu einem anderen Netzwerkmanager und überwacht dabei nur einen Teil des gesamten Netzwerks.

Anmerkung 2 zum Begriff: Ein Netzwerkmanager ist nicht immer ein dediziertes Gerät.

3.1.2.134**System-/Sicherheitsmanager****(en: system/security manager)**

Funktionalität des Systemmanagers im Auftrag der Funktionalität des Sicherheitsmanagers

3.1.2.135

Bedrohung

(en: threat)

Umstand oder Ereignis mit der Möglichkeit der nachteiligen Beeinflussung von Anlagenbetrieb (einschließlich von Funktion, Erscheinungsbild oder Ansehen), Werten oder Einzelpersonen durch ein Informationssystem über unberechtigten Zugriff, Zerstörung, Löschung, Modifikation von Daten, Nachrichtenlaufzeit und/oder Dienstverweigerung

3.1.2.136

D-Transaktion

(en: D-transaction)

MPDU, die keine MPDU mit direkter Quittierung ist, zuzüglich einer Folge von null oder mehr MPDUs mit direkter Quittierung, die unmittelbar folgen und ein Resultat der ersten MPDU (und möglicherweise aller anderen) sind, alle im selben Kanal und im selben Zeitschlitz

3.1.2.137

Tunneling

(en: tunneling)

Einkapselung eines ersten Protokolls innerhalb eines zweiten Kommunikationsprotokolls zur Beförderung von PDUs aus dem ersten Protokoll

3.1.2.138

Dienstleistungsfeld

(en: type-of-service)

gemeinsamer Name, der einer Menge von Protokollelementen und zugehörigen Attributen der Dienstgüte gegeben wird, die zusammen ein Teilprotokoll (z. B. Echtzeit für Audio, zeitkritische Daten und nicht zeitkritische Daten) mit eindeutigen Funktionen bilden

3.1.2.139

unberechtigte Offenlegung

(en: unauthorized disclosure)

Ereignis, bei dem Instanzen, die keinen berechtigten Zugriff darauf haben, Informationen aufgedeckt werden

3.1.2.140

Einzelaufruf

(en: unicast)

Nachrichtenübermittlung von einer Quelle zu einem einzigen vorgesehenen Empfänger; siehe auch Gruppenaufruf und Sammelaufruf

3.1.2.141

Benutzerinitialisierung

(en: user initialization)

Vorgang, mit dem ein Benutzer die kryptografische Anwendung für den Einsatz vorbereitet (z. B. Installation und Konfiguration von Software und Hardware)

3.1.2.142

Benutzerregistrierung

(en: user registration)

Vorgang, mit dem eine Instanz Mitglied einer Sicherheitsdomäne wird

3.1.2.143

vollständige Löschung

(en: zeroisation)

Verfahren der Löschung elektronisch gespeicherter Daten, kryptografischer Schlüssel und kritischer gespeicherter Parameter durch Veränderung oder Löschung des Speicherinhalts in einer Weise, dass die Wiederherstellung der Daten verhindert wird

3.1.3 Symbole für symmetrische Schlüssel, asymmetrische Schlüssel und Zertifikate

ANMERKUNG In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-bit-Schlüssel. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.1

K_DL

aktueller Datenschlüssel für alle Geräte im lokalen D-Teilnetz

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-bit-Schlüssel. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.2

K_global

bekannter Schlüssel mit einem statischen und veröffentlichten Wert, der die PDU-Struktur und die Verarbeitung vereinheitlicht, wenn ein gemeinsam benutzter, geheimer Schlüssel ungeeignet oder unbekannt ist

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-bit-Schlüssel. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.3

K_open

bekannter Schlüssel mit einem statischen und veröffentlichten Wert, der die PDU-Struktur und die Verarbeitung vereinheitlicht, wenn ein gemeinsam benutzter, geheimer Schlüssel ungeeignet oder unbekannt ist

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-bit-Schlüssel. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.4

K_join

Schlüssel zum sicheren Laden (Bootstrap) eines neuen Geräts in ein Netzwerk

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-bit-Schlüssel. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.5

K_join_wrapped

verpackte Version eines K_join-Schlüssels, der zur Wiederherstellung bei einem ausgefallenen Sicherheitsmanager benutzt wird

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-bit-Schlüssel. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.6

K_master

Masterschlüssel, der als KEK zur Schlüsselverteilung und für das Sicherheitsmanagement eines einzelnen Geräts benutzt wird

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-bit-Schlüssel. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.7

K_session_AB

aktueller Datenschlüssel für eine Sitzung zwischen Gerät A und Gerät B, der identisch mit K_session_BA ist

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte symmetrische Schlüssel sind 128-bit-Schlüssel. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.3.8

CA_root

öffentlicher Schlüssel einer Zertifizierungsstelle, die ein Zertifikat eines öffentlichen Schlüssels für ein Gerät ausgestellt hat

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte asymmetrische Schlüssel besitzen eine kryptografische Bitstärke von mindestens 128 bit. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

Anmerkung 2 zum Begriff: Dieser Schlüssel wird im Allgemeinen als Wurzelschlüssel bezeichnet und unterstützt den Nachweis der wahren Identität des Geräts, das das Zertifikat übermittelt, sowie einige zugehörige Verschlüsselungsinformationen.

3.1.3.9

Cert-A

Zertifikat des öffentlichen Schlüssels von Gerät A, das während der Ausführung eines authentifizierten Einführungsprotokolls für einen öffentlichen Schlüssel den Nachweis der wahren Identität des Geräts sowie einige zugehörige Verschlüsselungsinformationen unterstützt

Anmerkung 1 zum Begriff: In der vorliegenden Norm definierte asymmetrische Schlüssel besitzen eine kryptografische Bitstärke von mindestens 128 bit. Die genaue Beschreibung des kryptografischen Materials kann Abschnitt 7 entnommen werden.

3.1.4 Begriffe zur Beschreibung des Geräteverhaltens

3.1.4.1

Leistungspotential

(en: capability)

Fähigkeit der Ausführung von Handlungen einschließlich von Attributen der Befähigungen und Maße der Fähigkeiten wie Kapazität

BEISPIEL Anzahl der verbundenen Geräte, die ein Router unterstützen kann

Anmerkung 1 zum Begriff: Das Mindest-Leistungspotential wird durch Profile bestimmt.

[Quelle: ISO/IEC 62264-1:2003, 3.6]

3.1.4.2

Konfiguration

(en: configuration)

- a) Parametersatz, der 1) das Verhalten ändert und 2) vom Systemmanager eingestellt werden kann
- b) Vorgang der Festlegung und Verwaltung dieser Parameter

BEISPIEL Hop-Limit der Vermittlungsschicht

Anmerkung 1 zum Begriff: Konfigurationen mit entsprechenden Standardwerten (z. B. NL-Hop-Limit = 64)

3.1.4.3

Leistungsmerkmal

(en: feature)

offensichtliche Eigenschaft eines Geräts

BEISPIEL batteriebetrieben

3.1.4.4

verbindlich

(en: mandatory)

gefordertes Element für die Beanspruchung der Übereinstimmung mit der vorliegenden Norm

BEISPIEL Unterstützung der Kryptografie mit einem symmetrischen Schlüssel

3.1.4.5

wahlfrei

(en: optional)

Element, für das keine Übereinstimmung mit der vorliegenden Norm gefordert wird, das aber bei Vorhandensein ein Verhalten in Übereinstimmung mit der vorliegenden Norm aufweisen muss

BEISPIEL Unterstützung der Kryptografie mit einem asymmetrischen Schlüssel

CONTENTS

FOREWORD.....	23
0 Introduction	25
0.1 General	25
0.2 Document structure	25
0.3 Potentially relevant patents	25
1 Scope.....	27
2 Normative references	27
3 Terms, definitions, abbreviated terms, acronyms, and conventions.....	28
3.1 Terms and definitions	28
3.2 Abbreviated terms and acronyms.....	55
3.3 Conventions	61
4 Overview	63
4.1 General	63
4.2 Interoperability and related issues	63
4.3 Quality of service.....	64
4.4 Worldwide applicability	64
4.5 Network architecture.....	64
4.6 Network characteristics	70
5 Systems	77
5.1 General	77
5.2 Devices	77
5.3 Networks	85
5.4 Protocol suite structure.....	96
5.5 Data flow	98
5.6 Time reference	104
5.7 Firmware upgrades.....	105
5.8 Wireless backbones and other infrastructures.....	105
6 System management role	105
6.1 General	105
6.2 DMAP	107
6.3 System manager	131
7 Security	185
7.1 General	185
7.2 Security services	186
7.3 PDU security	190
7.4 Join process	223
7.5 Session establishment.....	255
7.6 Key update	260
7.7 Functionality of the security manager role.....	267
7.8 Security policies	269
7.9 Security functions available to the AL	272
7.10 Security statistics collection, threat detection, and reporting	275
7.11 DSMO functionality.....	276
8 Physical layer	283
8.1 General	283
8.2 Default physical layer	283

9	Data-link layer	285
9.1	General	285
9.2	DDSAP	354
9.3	Data DPDU and ACK/NAK DPDU	357
9.4	DL management information base	383
9.5	DLE methods	432
9.6	DL alerts	434
10	Network layer	437
10.1	General	437
10.2	NL functionality overview	437
10.3	NLE data services	457
10.4	NL management object	460
10.5	NPDU formats	467
11	Transport layer	476
11.1	General	476
11.2	TLE reference model	476
11.3	Transport security entity	477
11.4	Transport data entity	478
11.5	TPDU encoding	482
11.6	TL model	484
12	Application layer	495
12.1	General	495
12.2	Energy considerations	495
12.3	Legacy control system considerations	495
12.4	Introduction to object-oriented modeling	496
12.5	Object model	498
12.6	Object attribute model	499
12.7	Method model	502
12.8	Alert model	502
12.9	Alarm state model	503
12.10	Event state model	504
12.11	Alert reporting	504
12.12	Communication interaction model	506
12.13	AL addressing	516
12.14	Management objects	520
12.15	User objects	520
12.16	Data types	551
12.17	Application services provided by application sublayer	558
12.18	AL flow use of lower layer services	594
12.19	AL management	595
12.20	Process control industry standard data structures	613
12.21	Additional tables	616
12.22	Coding	617
12.23	Syntax	640
12.24	Detailed coding examples (INFORMATIVE)	652
13	Provisioning	653
13.1	General	653
13.2	Terms and definitions for devices with various roles or states	654

13.3	Provisioning procedures	656
13.4	Pre-installed symmetric keys	656
13.5	Provisioning using out-of-band mechanisms	657
13.6	Provisioning networks	657
13.7	State transition diagrams	660
13.8	Device management application protocol objects used during provisioning	664
13.9	Management objects	667
13.10	Device provisioning service object	673
13.11	Provisioning functions [INFORMATIVE]	680
Annex A (informative)	User layer / application profiles	684
A.1	Overview	684
A.2	User layer	684
A.3	Application profile	684
Annex B (normative)	Role profiles	686
B.1	Introduction	686
B.2	System	687
B.3	System manager	687
B.4	Security manager	688
B.5	Physical layer	689
B.6	Data-link layer	689
B.7	Network layer	694
B.8	Application layer	695
B.9	Provisioning	696
B.10	Gateway (informative)	696
Annex C (informative)	Background information	698
C.1	Industrial needs	698
C.2	Usage classes	698
C.3	The Open Systems Interconnection Basic Reference Model	700
Annex D (normative)	Configuration defaults	704
D.1	General	704
D.2	System management	704
D.3	Security	705
D.4	Data-link layer	705
D.5	Network layer	707
D.6	Transport layer	707
D.7	Application layer	707
D.8	Provisioning	709
D.9	Gateway (informative)	710
Annex E (informative)	Use of backbone networks	711
E.1	General	711
E.2	Recommended characteristics	711
E.3	Internet protocol backbones	711
Annex F (normative)	Basic security concepts – Notation and representation	713
F.1	Strings and string operations	713
F.2	Integers, octets, and their representation	713
F.3	Entities	713
Annex G (informative)	Using certificate chains for over-the-air provisioning	714
Annex H (normative)	Security building blocks	715

H.1	Symmetric key cryptographic building blocks	715
H.2	Asymmetric-key cryptographic building blocks	716
H.3	Keying information	716
H.4	Key agreement schemes	718
H.5	Keying information schemes	718
H.6	Challenge domain parameter generation and validation	719
H.7	Challenge validation primitive	720
H.8	Secret key generation (SKG) primitive	720
H.9	Block-cipher-based cryptographic hash function	721
H.10	Elliptic curve cryptography manual certificate scheme	722
Annex I (informative)	Definition templates	725
I.1	Object type template	725
I.2	Standard object attributes template	725
I.3	Standard object methods	726
I.4	Standard object alert reporting template	727
I.5	Data structure definition	728
Annex J (informative)	Operations on attributes	730
J.1	Operations on attributes	730
J.2	Synchronized cutover	734
Annex K (normative)	Standard object types	735
Annex L (informative)	Standard data types	740
Annex M (normative)	Identification of tunneled legacy fieldbus protocols	742
Annex N (informative)	Tunneling and native object mapping	743
N.1	Overview	743
N.2	Tunneling	743
N.3	Foreign protocol application communication	743
N.4	Native object mapping	744
N.5	Tunneling and native object mapping tradeoffs	744
Annex O (informative)	Generic protocol translation	745
O.1	Overview	745
O.2	Publish	745
O.3	Subscribe	746
O.4	Client	747
O.5	Server	748
Annex P (informative)	Exemplary GIAP adaptations for this standard	749
P.1	General	749
P.2	Parameters	749
P.3	Session	749
P.4	Lease	749
P.5	Device list report	750
P.6	Topology report	750
P.7	Schedule report	750
P.8	Device health report	750
P.9	Neighbor health report	750
P.10	Network health report	750
P.11	Time	750
P.12	Client/server	750
P.13	Publish/subscribe	751

P.14	Bulk transfer	752
P.15	Alert	752
P.16	Gateway configuration	753
P.17	Device configuration	753
Annex Q (informative)	Exemplary GIAP adaptations for IEC 62591	754
Q.1	General	754
Q.2	Parameters	755
Q.3	Session	755
Q.4	Lease	756
Q.5	Device list report	756
Q.6	Topology report	756
Q.7	Schedule report	757
Q.8	Device health report	757
Q.9	Neighbor health report	758
Q.10	Network health report	758
Q.11	Time	758
Q.12	Client/server	759
Q.13	Publish/subscribe	760
Q.14	Bulk transfer	761
Q.15	Alert	761
Q.16	Gateway configuration	762
Q.17	Device configuration	762
Annex R (informative)	Host system interface to standard-compliant devices via a gateway	763
R.1	Background	763
R.2	Device application data integration with host systems	764
R.3	Host system configuration tool	764
R.4	Field device / distributed control systems integration	766
R.5	Gateway	767
R.6	Asset management application support	767
Annex S (informative)	Symmetric-key operation test vectors	769
S.1	DPDU samples	769
S.2	TPDU samples	770
Annex T (informative)	Data-link and network headers for join requests	771
T.1	Overview	771
T.2	MAC header (MHR)	771
T.3	DL header (DHR)	771
T.4	NL header	772
Annex U (informative)	Gateway role	773
U.1	General	773
U.2	Notional GIAP	777
U.3	Example uses of WISN standard services and objects	821
Annex V (informative)	Country-specific and region-specific provisions	841
V.1	General	841
V.2	Operation within a fixed regulatory regime	841
V.3	Operation on a platform that moves between regulatory regimes	841
V.4	Compliance with EN 300 328 [INFORMATIVE]	842
Bibliography		845

Figure 1 – Standard-compliant network	66
Figure 2 – Typical single-layer PDU without fragmenting or blocking.....	67
Figure 3 – Full multi-layer PDU structure used by this standard	67
Figure 4 – Physical devices versus roles	80
Figure 5 – Notional representation of device phases	84
Figure 6 – Simple star topology	87
Figure 7 – Simple hub-and-spoke topology	88
Figure 8 – Mesh topology.....	89
Figure 9 – Simple star-mesh topology.....	90
Figure 10 – Example where network and D-subnet overlap	91
Figure 11 – Example where network and D-subnet differ.....	92
Figure 12 – Network with multiple gateways.....	93
Figure 13 – Basic network with backup gateway	94
Figure 14 – Network with backbone	95
Figure 15 – Network with backbone – device roles.....	96
Figure 16 – Reference model used by this standard.....	97
Figure 17 – Basic data flow.....	98
Figure 18 – Data flow between I/O devices	99
Figure 19 – Data flow with legacy I/O device.....	100
Figure 20 – Data flow with backbone-resident device.....	101
Figure 21 – Data flow between I/O devices via backbone subnet	102
Figure 22 – Data flow to standard-aware control system	103
Figure 23 – Management architecture	106
Figure 24 – DMAP	109
Figure 25 – Example of management SAP flow through standard protocol suite.....	111
Figure 26 – System manager architecture concept.....	132
Figure 27 – UAP-system manager interaction during contract establishment.....	154
Figure 28 – Contract-related interaction between DMO and SCO	157
Figure 29 – Contract source, destination, and intermediate devices	169
Figure 30 – Contract establishment example.....	177
Figure 31 – Contract ID usage in source	178
Figure 32 – Contract termination.....	181
Figure 33 – Contract modification with immediate effect.....	183
Figure 34 – Examples of DPDU and TPDU scope	185
Figure 35 – Keys and associated lifetimes	187
Figure 36 – Key lifetimes	189
Figure 37 – DPDU structure	192
Figure 38 – DLE and DLS processing for a D-transaction initiator	193
Figure 39 – Received DPDU – DLE and DSC	195
Figure 40 – TPDU structure and protected coverage.....	208
Figure 41 – TMIC parameters	209
Figure 42 – TL and TSC interaction, outgoing TPDU	210

Figure 43 – TL and TSC interaction, incoming TPDU	211
Figure 44 – Example: Overview of the symmetric-key join process.....	228
Figure 45 – Example: Overview of the symmetric-key join process of a backbone device	229
Figure 46 – Asymmetric-key-authenticated key agreement scheme.....	239
Figure 47 – Example: Overview of the asymmetric-key join process for a device with a DL	242
Figure 48 – Example: Overview of the asymmetric-key join process of a backbone device	243
Figure 49 – Device state transitions for join process and device lifetime	255
Figure 50 – High-level example of session establishment	256
Figure 51 – Key update protocol overview.....	261
Figure 52 – Device key establishment and key update state transition	267
Figure 53 – DL protocol suite and PHPDU/DPDU structure.....	286
Figure 54 – Graph routing example	289
Figure 55 – Inbound and outbound graphs	291
Figure 56 – Slotted-channel-hopping	295
Figure 57 – Slow-channel-hopping	296
Figure 58 – Hybrid operation.....	296
Figure 59 – Radio spectrum usage	297
Figure 60 – Predefined channel-hopping-pattern1	299
Figure 61 – Two groups of DLEs with different channel-hopping-pattern-offsets.....	300
Figure 62 – Interleaved channel-hopping-pattern1 with sixteen different channel- hopping-pattern-offsets.....	301
Figure 63 – Example timeslot allocation for slotted-channel-hopping.....	302
Figure 64 – Example timeslot allocation for slow-channel-hopping	303
Figure 65 – Hybrid mode with slotted-channel-hopping and slow-channel-hopping.....	304
Figure 66 – Combining slow-channel-hopping and slotted-channel-hopping	304
Figure 67 – Example of a three-timeslot superframe and how it repeats.....	305
Figure 68 – Superframes and links.....	305
Figure 69 – Multiple superframes with aligned timeslots.....	306
Figure 70 – Example superframe for slotted-channel-hopping	310
Figure 71 – Example superframe for slow-channel-hopping	311
Figure 72 – Components of a slow-channel-hopping superframe.....	311
Figure 73 – Example configuration for avoiding collisions among routers	312
Figure 74 – Hybrid configuration	313
Figure 75 – Timeslot allocation and message queue	315
Figure 76 – 250 ms alignment intervals.....	318
Figure 77 – Timeslot durations and timing.....	319
Figure 78 – Clock source acknowledges receipt of a Data DPDU	324
Figure 79 – Transaction timing attributes	326
Figure 80 – Dedicated and shared transaction timeslots	327
Figure 81 – Unicast transaction	328
Figure 82 – PDU wait time (PWT)	331

Figure 83 – Duocast support in the standard.....	332
Figure 84 – Duocast transaction	333
Figure 85 – Shared timeslots with active CSMA/CA	334
Figure 86 – Transaction during slow-channel-hopping periods	335
Figure 87 – DL management SAP flow through standard protocol suite.....	338
Figure 88 – PhPDU and DPDU structure	357
Figure 89 – Typical ACK/NAK DPDU layout	365
Figure 90 – Relationship among DLMO indexed attributes	403
Figure 91 – Address translation process	440
Figure 92 – Fragmentation process.....	442
Figure 93 – Reassembly process	443
Figure 94 – Processing of a NSDU received from a TLE	445
Figure 95 – Processing of a received NPDU	446
Figure 96 – Processing of a NPDU received by a NLE from the backbone	448
Figure 97 – Delivery of a received NPDU at its final destination NLE	449
Figure 98 – Routing from a field device direct to a field-connected gateway without backbone routing.....	450
Figure 99 – Protocol suite diagram for routing from a field device direct to a field-connected gateway without backbone routing	451
Figure 100 – Routing a NPDU from a field device to a gateway via a backbone router	452
Figure 101 – Protocol suite diagram for routing an APDU from a field device to a gateway via a backbone router	453
Figure 102 – Routing from a field device on one D-subnet to another field device on a different D-subnet.....	454
Figure 103 – Protocol suite diagram for routing from an I/O device on one D-subnet to another I/O device on a different D-subnet	455
Figure 104 – Example of routing over an Ethernet backbone network	456
Figure 105 – Example of routing over a fieldbus backbone network	457
Figure 106 – Distinguishing between NPDU header formats	468
Figure 107 – TLE reference model	476
Figure 108 – UDP pseudo-header for IPv6.....	478
Figure 109 – TPDU structure	482
Figure 110 – User application objects in a UAP	498
Figure 111 – Alarm state model	503
Figure 112 – Event model	504
Figure 113 – A successful example of multiple outstanding requests, with response concatenation.....	509
Figure 114 – An example of multiple outstanding unordered requests, with second write request initially unsuccessful.....	510
Figure 115 – An example of multiple outstanding ordered requests, with second write request initially unsuccessful	511
Figure 116 – Send window example 1, with current send window smaller than maximum send window.....	513
Figure 117 – Send window example 2, with current send window the same size as maximum send window, and non-zero usable send window width	514

Figure 118 – Send window example 3, with current send window the same size as maximum send window, and usable send window width of zero	514
Figure 119 – General addressing model.....	516
Figure 120 – UAP management object state diagram.....	523
Figure 121 – Alert report reception state diagram	525
Figure 122 – Alert-reporting example	525
Figure 123 – Upload/Download object download state diagram	541
Figure 124 – Upload/Download object upload state diagram	541
Figure 125 – Publish sequence of service primitives	561
Figure 126 – client/server model two-part interactions	566
Figure 127 – client/server model four-part interactions: Successful delivery.....	566
Figure 128 – client/server model four-part interactions: Request delivery failure	567
Figure 129 – client/server model four-part interactions: Response delivery failure	567
Figure 130 – AlertReport and AlertAcknowledge, delivery success.....	582
Figure 131 – AlertReport, delivery failure	582
Figure 132 – AlertReport, acknowledgment failure	583
Figure 133 – Concatenated response for multiple outstanding write requests (no message loss)	590
Figure 134 – Management and handling of malformed APDUs received from device X	596
Figure 135 – The provisioning network.....	658
Figure 136 – State transition diagrams outlining provisioning steps during a device lifecycle	660
Figure 137 – State transition diagram showing various paths to joining a secured network	663
Figure 138 – Provisioning objects and interactions	665
Figure C.1 – OSI Basic Reference Model	700
Figure O.1 – Generic protocol translation publish diagram	745
Figure O.2 – Generic protocol translation subscribe diagram	746
Figure O.3 – Generic protocol translation client/server transmission diagram.....	747
Figure O.4 – Generic protocol translation client/server reception diagram.....	748
Figure R.1 – Host integration reference model	763
Figure R.2 – Configuration using an electronic device definition.....	765
Figure R.3 – Configuration using FDT/DTM approach	766
Figure U.1 – Gateway scenarios	775
Figure U.2 – Basic gateway model	776
Figure U.3 – Internal sequence of primitives for session interface.....	780
Figure U.4 – Internal sequence of primitives for lease management interface	780
Figure U.5 – Internal sequence of primitives for system report interfaces.....	781
Figure U.6 – Internal sequence of primitives for time interface	781
Figure U.7 – Internal sequence of primitives for Client/server interface initiated from gateway to an adapter device	782
Figure U.8 – Internal sequence of primitives for publish interface initiated from gateway to an adapter device	782
Figure U.9 – Internal sequence of primitives for subscribe interface initiated from an adapter device.....	783

Figure U.10 – Internal sequence of primitives for publisher timer initiated from gateway to an adapter device	783
Figure U.11 – Internal sequence of primitives for subscriber timers initiated from an adapter device	783
Figure U.12 – Internal sequence of primitives for the bulk transfer interface	784
Figure U.13 – Internal sequence of primitives for the alert subscription interface	784
Figure U.14 – Internal sequence of primitives for the alert notification interface	785
Figure U.15 – Internal sequence of primitives for gateway management interfaces	785
Figure U.16 – Tunnel object model	821
Figure U.17 – Distributed tunnel endpoints	822
Figure U.18 – Multicast, broadcast, and one-to-many messaging	823
Figure U.19 – Tunnel object buffering	824
Figure U.20 – publish/subscribe publisher CoSt flowchart	827
Figure U.21 – publish/subscribe publisher periodic flowchart	827
Figure U.22 – publish/subscribe subscriber common periodic and CoSt flowchart	828
Figure U.23 – Network address mappings	829
Figure U.24 – Connection_Info usage in protocol translation	830
Figure U.25 – Transaction_Info usage in protocol translation	831
Figure U.26 – Interworkable tunneling mechanism overview diagram	832
Figure U.27 – Bulk transfer model	835
Figure U.28 – Alert model	836
Figure U.29 – Alert cascading	837
Figure U.30 – Native publish/subscribe and client/server access	838
Table 1 – Standard management object types in DMAP	110
Table 2 – Metadata_attribute data structure	112
Table 3 – Alert types for communication diagnostic category	114
Table 4 – Alert types for security alert category	114
Table 5 – Alert types for device diagnostic alert category	114
Table 6 – Alert types for process alert category	114
Table 7 – ARMO attributes	116
Table 8 – ARMO alerts	119
Table 9 – Alarm_Recovery method	120
Table 10 – DMO attributes	122
Table 11 – DMO alerts	130
Table 12 – System management object types	133
Table 13 – DSO attributes	135
Table 14 – Address_Translation_Row data structure	136
Table 15 – Read_Address_Row method	136
Table 16 – Input argument usage for Read_Address_Row method	138
Table 17 – Output argument usage for Read_Address_Row method	138
Table 18 – Attributes of SMO in system manager	140
Table 19 – Proxy_System_Manager_Join method	142
Table 20 – Proxy_System_Manager_Contract method	144

Table 21 – Effect of different join commands on attribute sets	146
Table 22 – Attributes of DMSO in system manager	146
Table 23 – System_Manager_Join method.....	147
Table 24 – System_Manager_Contract method	149
Table 25 – Attributes of STSO in system manager	153
Table 26 – Attributes of SCO in system manager	156
Table 27 – SCO method for contract establishment, modification, or renewal.....	160
Table 28 – Input argument usage for SCO method for contract establishment, modification, or renewal.....	167
Table 29 – Output argument usage for SCO method for contract establishment, modification, or renewal.....	168
Table 30 – Contract_Data data structure.....	171
Table 31 – New_Device_Contract_Response data structure	174
Table 32 – SCO method for contract termination, deactivation and reactivation	180
Table 33 – DMO method to notify of contract termination	181
Table 34 – DMO method to notify of contract modification.....	183
Table 35 – Security levels	190
Table 36 – Structure of the security control field	190
Table 37 – Sec.DpduPrep.Request elements	196
Table 38 – Sec.DpduPrep.Response elements	197
Table 39 – Sec.DAckCheck.Request elements.....	198
Table 40 – Sec.DAckCheck.Response elements	199
Table 41 – Sec.DInitialCheck.Request elements	200
Table 42 – Sec.DInitialCheck.Response elements	201
Table 43 – Sec.DAckPrep.Request elements	202
Table 44 – Sec.DAckPrep.Response elements	203
Table 45 – Structure of the WISN DPDU nonce	204
Table 46 – Structure of the 32-bit truncated TAI time used in the D-nonce	204
Table 47 – TSC pseudo-header structure.....	209
Table 48 – Sec.TpduOutCheck.Request elements	212
Table 49 – Sec.TpduOutCheck.Response elements.....	212
Table 50 – Sec.TpduSecure.Request elements.....	213
Table 51 – Sec. TpduSecure.Response elements	214
Table 52 – Sec.TpduInCheck.Request elements	215
Table 53 – Sec.TpduInCheck.Response elements	216
Table 54 – Sec.TpduVerify.Request elements.....	217
Table 55 – Sec.TpduVerify.Response elements	218
Table 56 – Structure of TL security header	218
Table 57 – Structure of the TPDU nonce.....	219
Table 58 – Structure of 32-bit truncated nominal TAI time used in the T-nonce	219
Table 59 – Proxy_Security_Sym_Join method	231
Table 60 – Security_Sym_Join method	232
Table 61 – Security_Confirm method	232
Table 62 – Security_Sym_Join_Request data structure.....	233

Table 63 – Security_Sym_Join_Response data structure	234
Table 64 – Structure of compressed security level field.....	235
Table 65 – Master key security level	236
Table 66 – Security_Sym_Confirm data structure.....	236
Table 67 – Implicit certificate format	238
Table 68 – Usage_serial_number structure	238
Table 69 – Proxy_Security_Pub_Join method	245
Table 70 – Security_Pub_Join method	246
Table 71 – Proxy_Security_Pub_Confirm method	247
Table 72 – Security_Pub_Confirm method	247
Table 73 – Network_Information_Confirmation method	248
Table 74 – Format of asymmetric join request internal structure	249
Table 75 – Format of the protocol control field	249
Table 76 – Format of asymmetric join response internal structure	250
Table 77 – Format of first join confirmation internal structure	251
Table 78 – Format of join confirmation response internal structure.....	252
Table 79 – Join process and device lifetime state machine	254
Table 80 – Security_New_Session method	257
Table 81 – Security_New_Session_Request data structure.....	258
Table 82 – Security_New_Session_Response data structure	259
Table 83 – New_Key method	262
Table 84 – Security_Key_and_Policies data structure	263
Table 85 – Security_Key_Update_Status data structure.....	265
Table 86 – T-key and D-key state transition	266
Table 87 – Attributes of PSMO in the system manager	267
Table 88 – Structure of policy field.....	270
Table 89 – Key_Type	270
Table 90 – Key_Usage.....	271
Table 91 – Granularity	271
Table 92 – DSMO attributes.....	276
Table 93 – KeyDescriptor.....	278
Table 94 – T-keyLookupData OctetString fields	279
Table 95 – Delete key method	280
Table 96 – Key_Policy_Update method.....	281
Table 97 – DSMO Alerts	282
Table 98 – Timing requirements.....	284
Table 99 – Graph table on ND20.....	290
Table 100 – Graph table on ND21.....	290
Table 101 – Approximating nominal timing with 32 KiHz clock	320
Table 102 – DL_Config_Info structure.....	346
Table 103 – CountryCode	352
Table 104 – DD-DATA.request parameters	355
Table 105 – DD-DATA.confirm parameters.....	356

Table 106 – Value set for status parameter.....	356
Table 107 – DD-DATA.indication parameters	356
Table 108 – ExtDLUint, one-octet variant.....	359
Table 109 – ExtDLUint, two-octet variant	359
Table 110 – Data DPDU MHR	360
Table 111 – Data DPDU DHDR.....	361
Table 112 – Data DPDU DMXHR	362
Table 113 – DROUT structure, compressed variant	363
Table 114 – DROUT structure, uncompressed variant.....	364
Table 115 – DADDR structure.....	365
Table 116 – ACK/NAK DPDU MHR	366
Table 117 – ACK/NAK DPDU DHR	367
Table 118 – ACK/NAK DPDU DHDR	368
Table 119 – Advertisement DAUX structure	369
Table 120 – Advertisement selections elements.....	370
Table 121 – Advertisement selections.....	370
Table 122 – Advertisement time synchronization elements	371
Table 123 – Advertisement time synchronization structure	371
Table 124 – Join superframe information subfields	372
Table 125 – Join superframe information structure.....	373
Table 126 – Superframe derived from advertisement	373
Table 127 – Join information elements.....	374
Table 128 – Join information structure	374
Table 129 – Defaults for links created from advertisements	376
Table 130 – dlmo.Neighbor entry created from advertisements	377
Table 131 – dlmo.Graph entry created from advertisements.....	377
Table 132 – dlmo.Route entry created from advertisements	377
Table 133 – Solicitation header subfields.....	380
Table 134 – Solicitation header structure	380
Table 135 – Solicitation DAUX fields.....	380
Table 136 – Solicitation DAUX structure	381
Table 137 – Activate link DAUX fields	382
Table 138 – Activate link DAUX structure.....	382
Table 139 – Report received signal quality DAUX fields	383
Table 140 – Report received signal quality DAUX structure	383
Table 141 – DLMO attributes	384
Table 142 – D-subnet filter octets	393
Table 143 – dlmo.TaiAdjust OctetString fields.....	393
Table 144 – dlmo.TaiAdjust OctetString structure	394
Table 145 – dlmo.EnergyDesign OctetString fields.....	394
Table 146 – dlmo.EnergyDesign OctetString structure	394
Table 147 – dlmo.DeviceCapability OctetString fields	395
Table 148 – dlmo.DeviceCapability OctetString structure	395

Table 149 – dlmo.DiscoveryAlert fields	397
Table 150 – dlmo.DiscoveryAlert structure	397
Table 151 – dlmo.Candidates OctetString fields	398
Table 152 – dlmo.Candidates structure	399
Table 153 – dlmo.SmoothFactors OctetString fields	400
Table 154 – dlmo.SmoothFactors structure	400
Table 155 – dlmo.QueuePriority fields	401
Table 156 – dlmo.QueuePriority structure	401
Table 157 – dlmo.ChannelDiag fields	402
Table 158 – dlmo.ChannelDiag structure	402
Table 159 – dlmo.Ch fields	405
Table 160 – dlmo.Ch structure	405
Table 161 – Transaction receiver template fields	408
Table 162 – Transaction receiver template structure	408
Table 163 – Transaction initiator template fields	409
Table 164 – Transaction initiator template structure	409
Table 165 – Default transaction responder template, used during join process	410
Table 166 – Default transaction initiator template, used during join process	410
Table 167 – Default transaction responder template, used during join process	411
Table 168 – dlmo.Neighbor fields	413
Table 169 – dlmo.Neighbor structure	414
Table 170 – ExtendGraph fields	415
Table 171 – ExtGraph structure	415
Table 172 – dlmo.NeighborDiagReset fields	416
Table 173 – dlmo.NeighborDiagReset structure	416
Table 174 – dlmo.Superframe fields	417
Table 175 – dlmo.Superframe structure	418
Table 176 – dlmo.Superframeldle fields	422
Table 177 – dlmo.Superframeldle structure	422
Table 178 – dlmo.Graph	423
Table 179 – dlmo.Graph structure	423
Table 180 – dlmo.Link fields	424
Table 181 – dlmo.Link structure	425
Table 182 – dlmo.Link[].Type structure	426
Table 183 – Allowed dlmo.Link[].Type combinations	427
Table 184 – Values for dlmo.Link[].Schedule	428
Table 185 – dlmo.Route fields	428
Table 186 – dlmo.Route structure	429
Table 187 – dlmo.NeighborDiag fields	430
Table 188 – Diagnostic summary OctetString fields	430
Table 189 – Diagnostic summary OctetString structure	431
Table 190 – Diagnostic ClockDetail OctetString fields	431
Table 191 – Diagnostic ClockDetail OctetString structure	432

Table 192 – Read_Row method	433
Table 193 – Write_Row method	433
Table 194 – Write_Row_Now method	434
Table 195 – dlmo.AlertPolicy fields	435
Table 196 – dlmo.AlertPolicy OctetString structure	435
Table 197 – DL_Connectivity alert	436
Table 198 – DL_Connectivity alert OctetString	436
Table 199 – NeighborDiscovery alert	437
Table 200 – Link-local address structure	438
Table 201 – Address translation table (ATT)	439
Table 202 – Example of a routing table	444
Table 203 – N-DATA.request elements	458
Table 204 – N-DATA.confirm elements	459
Table 205 – N-DATA.indication elements	460
Table 206 – NLMO attributes	461
Table 207 – Contract table structure	464
Table 208 – Route table elements	464
Table 209 – Address translation table structure	465
Table 210 – NLMO structured MIB manipulation methods	466
Table 211 – Alert to indicate dropped PDU/PDU error	467
Table 212 – Common header patterns	469
Table 213 – Basic NL header format	469
Table 214 – Contract-enabled NL header format	471
Table 215 – 6LoWPAN_IPHC encoding format	471
Table 216 – IPv6 NL header format	472
Table 217 – Full NL header in the DL	473
Table 218 – NL header format for fragmented NPDUs	474
Table 219 – Format of first fragment header	474
Table 220 – Format of second and subsequent fragment headers	475
Table 221 – UDP header encoding	479
Table 222 – UDP 6LoWPAN_NHC-for-UDP encoding octet	483
Table 223 – Optimal UDP header encoding	483
Table 224 – UDP header encoding with checksum and compressed port numbers	484
Table 225 – T-DATA.request elements	485
Table 226 – T-DATA.confirm elements	486
Table 227 – T-DATA.confirm status codes	487
Table 228 – T-DATA.indication elements	488
Table 229 – TLMO attributes	489
Table 230 – TL management object methods – Reset	490
Table 231 – TL management object methods – Halt	491
Table 232 – TL management object methods – PortRangeInfo	491
Table 233 – TL management object methods – GetPortInfo	492
Table 234 – TL management object methods – GetNextPortInfo	493

Table 235 – TL management object alert types – Illegal use of port	493
Table 236 – TL management object alert types – TPDU received on unregistered port	494
Table 237 – TL management object alert types – TPDU does not match security policies.....	494
Table 238 – State table for alarm transitions	503
Table 239 – State table for event transitions	504
Table 240 – UAP management object attributes.....	521
Table 241 – State table for UAP management object	522
Table 242 – UAP management object methods	523
Table 243 – Alert-receiving object attributes	524
Table 244 – State table for handling an AlertReport reception.....	524
Table 245 – AlertReceiving object methods	525
Table 246 – UploadDownload object attributes	527
Table 247 – UploadDownload object methods.....	531
Table 248 – UploadDownload object StartDownload method.....	532
Table 249 – UploadDownload object DownloadData method	533
Table 250 – UploadDownload object EndDownload method	535
Table 251 – UploadDownload object StartUpload method	536
Table 252 – UploadDownload object UploadData method	537
Table 253 – UploadDownload object EndUpload method	538
Table 254 – Download state table for unicast operation mode.....	539
Table 255 – Upload state table for unicast operation mode	542
Table 256 – Concentrator object attributes.....	544
Table 257 – Concentrator object methods.....	545
Table 258 – Dispersion object attributes	546
Table 259 – Dispersion object methods	547
Table 260 – Tunnel object attributes	548
Table 261 – Tunnel object methods	550
Table 262 – Interface object attributes	551
Table 263 – Interface object methods	551
Table 264 – Data type: ObjectAttributeIndexAndSize	552
Table 265 – Data type: Communication association endpoint.....	553
Table 266 – Data type: Communication contract data	555
Table 267 – Data type: Alert communication endpoint.....	556
Table 268 – Data type: Tunnel endpoint.....	556
Table 269 – Data type: Alert report descriptor.....	557
Table 270 – Data type: Process control alarm report descriptor for analog with single reference condition.....	557
Table 271 – Data type: ObjectIDandType.....	558
Table 272 – Data type: Unscheduled correspondent	558
Table 273 – AL services	559
Table 274 – Publish service	563
Table 275 – Read service	569
Table 276 – Write service	574