

DIN EN 13757-7

ICS 33.200; 35.100.10; 35.100.20

Einsprüche bis 2016-09-29

Entwurf**Kommunikationssysteme für Zähler –
Teil 7: Transport- und Sicherheitsdienste;
Deutsche und Englische Fassung prEN 13757-7:2016**

Communication systems for meters –
Part 7: Transport and security services;
German and English version prEN 13757-7:2016

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-07-29 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.din.de/go/entwuerfe 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 nhrs@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Heiz- und Raumluftechnik sowie deren Sicherheit (NHRs), 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

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 173 Seiten

DIN-Normenausschuss Heiz- und Raumluftechnik sowie deren Sicherheit (NHRs)
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Dieses Dokument (prEN 13757-7:2016) wurde vom Technischen Komitee CEN/TC 294 „Kommunikationssysteme für Zähler“ erarbeitet, dessen Sekretariat vom DIN (Deutschland) gehalten wird.

Für die deutsche Mitarbeit ist der Arbeitsausschuss NA 041-03-66 AA „Kommunikationssysteme für Zähler (SpA CEN/TC 294)“ im DIN-Normenausschuss Heiz- und Raumluftechnik sowie deren Sicherheit (NHRS) verantwortlich.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der prEN 13757-7 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

CEN/TC 294

Datum: 2016-07

prEN 13757-7:2016

CEN/TC 294

Sekretariat: DIN

Kommunikationssysteme für Zähler — Teil 7: Transport- und Sicherheitsdienste

Communication systems for meters — Part 7: Transport and security services

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.8f

Inhalt

	Seite
Europäisches Vorwort	7
Einleitung	8
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe	11
4 Abkürzungen und Symbole	13
4.1 Abkürzungen	13
4.2 Symbole	15
5 Schichtmodell	15
5.1 M-Bus-Schichten	15
5.2 Das CI-Feld-Prinzip	17
6 Authentifizierungs- und Fragmentierungs-Teilschicht (AFL, en: Authentication and Fragmentation Sublayer)	22
6.1 Einleitung	22
6.2 Übersicht über die AFL-Struktur	23
6.3 Komponenten der AFL	24
6.3.1 AFL-Längenfeld (AFL.AFL)	24
6.3.2 AFL-Fragmentierungskontrollfeld (AFL.FCL)	24
6.3.3 AFL-Nachrichtenkontrollfeld (AFL.MCL)	24
6.3.4 AFL-Schlüsselinformationfeld (AFL.KI)	25
6.3.5 AFL-Nachrichtenzählerfeld (AFL.MCR)	26
6.3.6 AFL-MAC-Feld (AFL.MAC)	26
6.3.7 AFL-Nachrichtenlängenfeld (AFL.ML)	26
7 Transportschicht (TPL)	27
7.1 Einleitung	27
7.2 Struktur ohne TPL-Header	27
7.3 Struktur mit kurzem TPL-Header	27
7.4 Struktur mit langem TPL-Header	28
7.5 CI-Feld-abhängige Elemente	28
7.5.1 Identifikationsnummer	28
7.5.2 Identifikation des Herstellers	29
7.5.3 Versionsidentifikation	29
7.5.4 Identifikation des Gerätetyps	29
7.5.5 Zugriffsnummer	31
7.5.6 Statusbyte in Zählernachrichten	33
7.5.7 Statusbyte in Partnernachrichten	34
7.5.8 Konfigurationsfeld	35
7.6 Konfigurationsfeld-abhängige Struktur	36
7.6.1 Allgemeines	36
7.6.2 Konfigurationsfelderweiterung	37
7.6.3 Optionale TPL-Header-Felder	37
7.6.4 Optionale TPL-Trailer-Felder	37
7.6.5 Teilverschlüsselung	37
7.7 Sicherheitsmodus-spezifische TPL-Felder	38

7.7.1	Gemeinsame Teilfelder des Konfigurationsfelds und der Konfigurationsfelderweiterung.....	38
7.7.2	Konfigurationsfeld des Sicherheitsmodus 0	41
7.7.3	Konfigurationsfeld der Sicherheitsmodi 2 und 3	42
7.7.4	Konfigurationsfeld des Sicherheitsmodus 5	43
7.7.5	Konfigurationsfeld des Sicherheitsmodus 7	45
7.7.6	Konfigurationsfeld des Sicherheitsmodus 8	47
7.7.7	Konfigurationsfeld des Sicherheitsmodus 9	50
7.7.8	Konfigurationsfeld des Sicherheitsmodus 10	52
8	Verwaltung der unteren Schichten	54
8.1	Allgemeines	54
8.2	Setzen der Baudrate für die M-Bus-Verbindungsschicht nach EN 13757-2.....	54
8.3	Adressstruktur bei Verwendung zusammen mit der drahtlosen Datenverbindungsschicht nach EN 13757-4	54
8.4	Selektion und Sekundäradressierung	55
8.5	Generalisiertes Selektionsverfahren	56
8.6	Suche nach installierten Slaves	57
8.6.1	Primäradressen	57
8.6.2	Sekundäradressen	57
8.6.3	Verfahren der Platzhaltersuche.....	57
9	Sicherheitsdienste.....	58
9.1	Allgemeines	58
9.2	Nachrichtenzähler	59
9.2.1	Überblick	59
9.2.2	Nachrichtenzähler C_M , der vom Zähler übertragen wird.....	59
9.2.3	Nachrichtenzähler C_{CP} , der vom Kommunikationspartner übertragen wird.....	60
9.2.4	Nachrichtenzähler C'_{CP} , der vom Zähler erhalten wird.....	60
9.2.5	Nachrichtenzähler C'_M und C''_M , die vom Kommunikationspartner empfangen werden	61
9.3	Authentifizierungsverfahren in der AFL.....	61
9.3.1	Überblick	61
9.3.2	Authentifizierungsverfahren AES-CMAC-128	62
9.3.3	Authentifizierungsverfahren AES-GMAC-128	62
9.4	Verschlüsselungs- und Authentifizierungsverfahren im TPL	63
9.4.1	Überblick über TPL-Schutzmechanismen	63
9.4.2	Herstellerspezifischer Schutzmechanismus (Sicherheitsmodus 1)	65
9.4.3	Schutzmechanismus DES-CBC (Sicherheitsmodus 2 und 3)	65
9.4.4	Schutzmechanismus AES-CBC-128 (Sicherheitsmodus 5).....	66
9.4.5	Schutzmechanismus AES-CBC-128 (Sicherheitsmodus 7).....	67
9.4.6	Schutzmechanismus AES-CTR-128 (Sicherheitsmodus 8)	67
9.4.7	Schutzmechanismus AES-GCM-128 (Sicherheitsmodus 9)	69
9.4.8	Schutzmechanismus AES-CCM-128 (Sicherheitsmodus 10)	73
9.5	Reaktion auf einen Sicherheitsversagen	75
9.6	Schlüsselableitung	75
9.6.1	Allgemeines	75
9.6.2	Schlüsselableitungsfunktion A.....	75
9.7	Schlüsselaustausch	77
Anhang A (informativ)	Die Struktur höherer Protokollschichten	78
A.1	Allgemeines	78
A.2	Transport- und Anwendungsschicht ohne TPL-Header (ohne).....	78
A.3	Transport- und Anwendungsschicht mit kurzem TPL-Header	79
A.4	Transport- und Anwendungsschicht mit langem TPL-Header	79
A.5	Transportschicht ohne TPL-Header (keine Anwenderdaten).....	79
A.6	Transportschicht mit kurzem TPL-Header (keine Anwenderdaten).....	79
A.7	Transportschicht mit langem TPL-Header (keine Anwenderdaten).....	80

Anhang B (normativ) Übertragungsprotokoll für Sicherheitsinformationen	81
B.1 Einleitung	81
B.1.1 Allgemeines	81
B.1.2 Sicherheitsinformationen übertragen.....	81
B.1.3 Sicherheitsinformationen aktivieren.....	81
B.1.4 Sicherheitsinformationen deaktivieren.....	81
B.2 Protokolldefinitionen	82
B.2.1 Allgemeines	82
B.2.2 SITP-Struktur.....	82
B.2.3 Blockkontrollfeld.....	83
B.2.4 SITP-Befehle	83
B.2.5 SITP-Antworten.....	83
B.2.6 Wrapping.....	84
Anhang C (informativ) Beispiel eines Nachrichtenzählers.....	87
Literaturhinweise.....	90

Bilder

Bild 1 — Eingabe und Ausgabe für den GCM-Algorithmus.....	70
Bild C.1 — Kontrollfluss des Nachrichtenzählers (Teil 1).....	88
Bild C.2 — Kontrollfluss des Nachrichtenzählers (Teil 2).....	89

Tabellen

Tabelle 1 — Reihenfolge der M-Bus-Schicht.....	16
Tabelle 2 — Vom Master oder Slave verwendete Codes des CI-Felds	17
Tabelle 3 — Übersicht über alle AFL-Felder.....	23
Tabelle 4 — AFL-Fragmentierungskontrollfeld - Definitionen der Bitfelder	24
Tabelle 5 — AFL-Nachrichtenkontrollfeld - Definitionen der Bitfelder.....	25
Tabelle 6 — AT-Teilfeld von AFL.MCL.....	25
Tabelle 7 — AFL-Schlüsselinformationsfeld - Definitionen der Bitfelder	26
Tabelle 8 — AFL-Nachrichtenzählerfeld - Definitionen der Bitfelder.....	26
Tabelle 9 — AFL-Nachrichtenlängenfeld - Definitionen der Bitfelder.....	27
Tabelle 10 — Allgemeine Struktur der TPL.....	27
Tabelle 11 — Kurzer TPL-Header.....	28
Tabelle 12 — Langer TPL-Header.....	28
Tabelle 13 — Identifikation des Gerätetyps.....	29
Tabelle 14 — Kodierung des Statusfelds.....	33
Tabelle 15 — Mit dem Statusfeld kodierte Anwendungsfehler.....	33
Tabelle 16 — Bedeutung des Statusbytes für Partnernachrichten.....	34
Tabelle 17 — Bedeutung der Bits 0 bis 5 im Statusbyte für Partnernachrichten.....	35
Tabelle 18 — Allgemeine Definition der zwei obligatorischen Konfigurationsfeldbytes.....	35
Tabelle 19 — Definition der Modusbits im Konfigurationsfeld (Sicherheitsmodus).....	36

Tabelle 20 — TPL-Struktur einer geschützten Nachricht.....	36
Tabelle 21 — Inhalt der Zählernachricht.....	38
Tabelle 22 — Inhalt der Partnernachricht.....	39
Tabelle 23 — Zugänglichkeit eines Zählers.....	39
Tabelle 24 — Die Schlüssel-ID	40
Tabelle 25 — KDF-Auswahl	41
Tabelle 26 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 0	41
Tabelle 27 — Definition des Konfigurationsfelds für den Sicherheitsmodus 0.....	41
Tabelle 28 — Konfigurationsfeld und nachfolgende Felder mit den Sicherheitsmodi 2 und 3	42
Tabelle 29 — Definition des Konfigurationsfeldes für die Sicherheitsmodi 2 und 3.....	43
Tabelle 30 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 5	43
Tabelle 31 — Definition des Konfigurationsfelds für den Sicherheitsmodus 5.....	44
Tabelle 32 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 7	45
Tabelle 33 — Definition des Konfigurationsfelds für den Sicherheitsmodus 7.....	45
Tabelle 34 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 7	46
Tabelle 35 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 8	47
Tabelle 36 — Definition des Konfigurationsfelds für Modus 8	47
Tabelle 37 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 8.....	49
Tabelle 38 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 9	50
Tabelle 39 — Definition des Konfigurationsfelds für den Sicherheitsmodus 9.....	50
Tabelle 40 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 10.....	52
Tabelle 41 — Definition des Konfigurationsfelds für den Sicherheitsmodus 10	52
Tabelle 42 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 10	53
Tabelle 43 — Adressstruktur der Verbindungsschicht für Funk	54
Tabelle 44 — Struktur eines Datagramms für die Selektion eines Slaves	55
Tabelle 45 — Anwendungsschichtstruktur eines Datagramms für die erweiterte Selektion (Modus 1)	56
Tabelle 47 — Schutzmechanismen für die Ablesung des Zählers	64
Tabelle 48 — Initialisierungsvektor des Sicherheitsmodus 5.....	66
Tabelle 49 — Struktur des Initialisierungsvektors in Sicherheitsmodus 8	69
Tabelle 50 — Eingabe- und Ausgabeinformationen für die GCM-Funktionen.....	70
Tabelle 51 — Struktur des Initialisierungsvektors in Sicherheitsmodus 9	72
Tabelle 52 — Struktur der Nonce, N.....	74
Tabelle A.1 — Transport- und Anwendungsschicht ohne TPL-Header (ohne)	78
Tabelle A.2 — Transport- und Anwendungsschicht mit kurzem TPL-Header.....	79
Tabelle A.3 — Transport- und Anwendungsschicht mit langem TPL-Header	79
Tabelle A.4 — Transportschicht ohne TPL-Header	79
Tabelle A.5 — Transportschicht mit kurzem TPL-Header	79

Tabelle A.6 — Transportschicht mit langem TPL-Header.....	80
Tabelle B.1 — CI-Felder des Übertragungsprotokolls für Sicherheitsinformationen.....	82
Tabelle B.2 — Interne Blockstruktur des SITP	82
Tabelle B.3 — Blockkontrollfeld.....	83
Tabelle B.4 — Blockparameterstruktur der SITP-Befehle.....	83
Tabelle B.5 — Antwortstatusdefinition.....	84
Tabelle B.6 — Liste an Wrapped-Datenstrukturen.....	84
Tabelle B.7 — Wrapped-Datenstruktur 01h	85
Tabelle B.8 — Wrapped-Datenstruktur 02h	85

Europäisches Vorwort

Dieses Dokument (prEN 13757-7:2016) wurde vom Technischen Komitee CEN/TC 294 „Kommunikationssysteme für Zähler“ erarbeitet, dessen Sekretariat vom DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird zusammen mit prEN 13757-3:2016 EN 13757-3:2013 ersetzen.

Dieses Dokument wurde unter einem Normungsauftrag erarbeitet, den die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben, und unterstützt grundlegende Anforderungen EU-Richtlinien.

Die folgenden technischen Änderungen wurden in der vorliegenden Europäischen Norm aufgenommen:

- die neuen Sicherheitsmodi (vormals "Verschlüsselungsmodus") 7, 8, 9 und 10 wurden hinzugefügt, die verschlüsselte und authentifizierte Nachrichten unterstützen;
- Unterstützung der Schlüsselableitungsfunktion zur Erzeugung von flüchtigen Schlüsseln;
- eine neue Authentifizierungs- und Fragmentierungsschicht wurde eingeführt.

EN 13757 besteht aus folgenden Teilen:

- *Kommunikationssysteme für Zähler — Teil 1: Datenaustausch;*
- *Kommunikationssysteme für Zähler — Teil 2: Physical und Link Layer;*
- *Kommunikationssysteme für Zähler — Teil 3: Spezielle Anwendungsschicht;*
- *Kommunikationssysteme für Zähler und deren Fernablesung — Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRD-Band);*
- *Kommunikationssysteme für Zähler — Teil 5: Weitervermittlung für den drahtlosen M-Bus;*
- *Kommunikationssysteme für Zähler — Teil 6: Lokales Bussystem;*
- *Kommunikationssysteme für Zähler — Teil 7: Transport- und Sicherheitsdienste [In der Entwurfsstufe zum derzeitigen Zeitpunkt].*

Das vorliegende Dokument fällt unter das Mandat EU M/441 „Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability“, da es relevante Definitionen und Verfahren für die Zählerdatenübertragung auf Ebene der Anwendungsschicht bereitstellt. Das M/441-Mandat fördert die signifikante Entwicklung von Normen im Bereich Smart Metering.

Das vorliegende Dokument besteht in Übereinstimmung mit CEN/CLC/ETSI TR 50572 [4].

Einleitung

Dieser Europäische Norm-Entwurf gehört zu einer Reihe an Teilen der EN 13757, die Kommunikationssysteme für Zähler und deren Fernablesung abdeckt. EN 13757-1 enthält allgemeine Beschreibungen und ein Kommunikationsprotokoll. EN 13757-2 enthält eine Bitübertragungsschicht und eine Verbindungsschicht für Zweidraht-Zählerbusse (M-Bus). EN 13757-3 enthält eine genaue Beschreibung der Anwendungsprotokolle, insbesondere des M-Bus-Protokolls. EN 13757-4 beschreibt die drahtlose Kommunikation (oft drahtloser M-Bus oder wM-Bus genannt). EN 13757-5 beschreibt das drahtlose Netzwerk für die Verstärkung, Weitervermittlung und Lenkung für die verschiedenen Modi von EN 13757-4. EN 13757-6 beschreibt einen lokalen Zweidrahtbus für kurze Distanzen (Lo-Bus). prEN 13757-7 beschreibt den Transportmechanismus und die Sicherheitsverfahren für Daten.

Diese oberen M-Bus-Protokollschichten können mit verschiedenen Bitübertragungsschichten und mit Datenverbindungsschichten sowie Netzwerkschichten verwendet werden, die die Übertragung von binären transparenten Nachrichten von variabler Länge unterstützen. Häufig werden die Bitübertragungsschichten und die Verbindungsschichten von EN 13757-2 (Zweidraht) und EN 13757-4 (drahtlos) sowie EN 13757-5 (drahtlos mit Routingfunktion) oder die in EN 13757-1 beschriebenen Alternativen verwendet. Diese oberen M-Bus-Protokollschichten wurden für einen minimalen Batterieverbrauch der Zähler optimiert, um längere Batterielebensdauer der Zähler zu gewährleisten, insbesondere im Fall einer drahtlosen Kommunikation. Zweitens wurden sie für die Mindestnachrichtlänge optimiert, um die Belegung des drahtlosen Kanals und somit die Kollisionsrate zu minimieren. Drittens wurden sie für die Mindestanforderungen an den Zählerprozessor hinsichtlich der Anforderungen der RAM-Größe, der Codelänge und der Rechenleistung optimiert.

Eine Übersicht über Kommunikationssysteme für Zähler befindet sich in EN 13757-1, die ebenfalls weitere Definitionen enthält.

In dieser Norm liegt der Schwerpunkt auf der Zählerkommunikation. Der Zähler kommuniziert mit einem (oder manchmal mehreren) festen oder mobilen Kommunikationspartnern, die wiederum Teil eines privaten oder öffentlichen Netzwerks sind. Diese weiteren Kommunikationssysteme können dieselben oder andere Anwendungsschichtprotokolle, Sicherheits-, Privatsphäre-, Authentifizierungs- und Managementverfahren verwenden.

Um gängige Kommunikationssysteme für CEN-Zähler (z. B. Gaszähler, Wasserzähler, Wärmeenergie- und Heizkostenverteiler) und für Stromzähler zu vereinfachen, werden in dieser Norm gelegentlich Stromzähler erwähnt. All diese Referenzen dienen ausschließlich Informationszwecken und sind keine standardmäßigen Anforderungen. Die Definition der Kommunikationsstandards für Stromzähler (möglicherweise durch einen Bezug auf CEN-Normen) liegt weiterhin in der alleinigen Verantwortung von CENELEC.

Der Bediener eines Smart-Metering-Netzwerks muss das Netzwerk sichern, um den Datenschutz und die Privatsphäre der Daten des Konsumenten zu gewährleisten (siehe EG-Empfehlung C1342 (2012)). Die Sicherung eines Systems erfordert eine Sicherheitsrichtlinie, die im Allgemeinen sämtliche Einschränkungen von Funktionen, Informationsflüssen zwischen Funktionen, Zugriffen durch externe Systeme und Bedrohungen ansprechen sollte, einschließlich Software und Zugriff auf Daten von Dritten aus betrieblicher Sicht.

Die Sicherheitsrichtlinie steht unter der Verantwortung von Organisationen nach ihren Geschäftsvorgängen. Die Hauptelemente einer Sicherheitsrichtlinie bestimmen in Kombination mit Regeln die erreichte Gesamtsicherheit. Die Sicherheitsrichtlinie definiert Ziele und Elemente des durch die Betriebspolitik und die technischen Implementierungen des Sicherheitsdienstes zu unterstützenden Systems. Die Ein- und Ausführung der Sicherheitsrichtlinien liegt außerhalb des Anwendungsbereiches dieser Norm, sie bietet jedoch Sicherheitsdienste an, die diese Richtlinien bei der Einführung unterstützen.

Ein Sicherheitskonzept bezieht sich hauptsächlich auf ein *architektonisches* Modell, das Datenflüsse zwischen rollenbasierten Datenverarbeitungsfunktionen darstellt. Anforderungen für das Sicherheitskonzept ergeben sich aus den Gesamtsicherheitszielen in Kombination mit den abgeleiteten Sicherheitsdiensten und bewährten Methoden. Die vorgelegte Norm bietet einen Satz an Sicherheitsdiensten, der das Design eines sicheren Systems ermöglicht, das mit hoher Wahrscheinlichkeit während der Lebensdauer des Zählers Angriffen standhält.

Die Beschränkung auf symmetrische Verschlüsselungsverfahren für die Datenübertragung ermöglicht energie- und speichereffiziente Lösungen. Dies ist vorteilhaft für dauerhaft batteriebetriebene Zähler. Außerdem wird die Integration unidirektionaler Zählerkommunikationen ermöglicht. Dienstleistungen wie die Schlüsselableitung und die Schlüsselverteilung lösen den Konflikt zwischen der kurzen Lebensdauer der Schlüssel und der langen Lebensdauer eines Zählers.

1 Anwendungsbereich

Dieser vorliegende Europäische Norm-Entwurf spezifiziert die Transport- und Sicherheitsdienste für Kommunikationssysteme für Zähler und deren Fernablesung.

Dieser vorliegende Europäische Norm-Entwurf spezifiziert sichere Kommunikationsfähigkeiten nach Design und unterstützt den Aufbau einer sicheren Systemarchitektur.

Dieser vorliegende Europäische Norm-Entwurf gilt für den Schutz der Verbraucherdaten zur Gewährleistung der Privatsphäre.

Dieser vorliegende Europäische Norm-Entwurf soll mit den in EN 13757-2, EN 13757-3, EN 13757-4, EN 13757-5 und EN 13757-6 festgelegten Spezifikationen der unteren Schicht verwendet werden.

2 Normative Verweisungen

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

EN 13757-1, *Kommunikationssysteme für Zähler — Teil 1: Datenaustausch*

EN 13757-2, *Kommunikationssysteme für Zähler und deren Fernablesung — Teil 2: Physical und Link Layer*

prEN 13757-3:2016, *Kommunikationssysteme für Zähler — Spezielle Anwendungsschicht*

EN 13757-4:2013, *Kommunikationssysteme für Zähler und deren Fernablesung — Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRD-Band)*

EN 13757-5, *Kommunikationssysteme für Zähler — Teil 5: Weitervermittlung für den drahtlosen M-Bus*

EN 62056-5-3:2014, *Datenkommunikation der elektrischen Energiemessung — DLMS/COSEM — Teil 5-3: DLMS/ COSEM-Anwendungsschicht (IEC 62056-5-3:2013)*

EN 62056-21, *Messung der elektrischen Energie — Zählerstandsübertragung, Tarif- und Laststeuerung — Teil 21: Datenübertragung für festen und mobilen Anschluss (IEC 62056-21)*

EN 62056-61, *Messung der elektrischen Energie — Zählerstandsübertragung, Tarif- und Laststeuerung — Teil 61: Object identification system (OBIS) (IEC 62056-61)*

ISO 8372, *Information processing — Modes of operation for a 64-bit block cipher algorithm*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

NIST/SP 800-38A:2001-12, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*

NIST/SP 800-38B:2005-05, *Recommendation for Block Cipher Modes of Operation: CMAC Mode for Authentication*

NIST/SP 800-38C:2004-05, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*

NIST/SP 800-38D:2007-11, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

NIST/SP 800-38F:2012-12, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

Authentifizierung

Eigenschaft, dass Daten von ihrer angeblichen Quelle stammen

[QUELLE: NIST/SP 800-38F:2012-12, NIST/SP 800-38C:2004-05]

3.2

Byte

Oktett von Bits

3.3

Vertraulichkeit

Eigenschaft, dass Informationen nicht für unautorisierte Personen, Entitäten oder Prozesse verfügbar oder öffentlich gemacht werden

[QUELLE: ISO 7498-2:1989]

3.4

Integrität

Datenintegrität

Eigenschaft, dass Daten nicht auf unberechtigte Weise geändert oder zerstört wurden

[QUELLE: ISO 7498-2:1989]

3.5

Datagramm

Dateneinheit, die von einer Quelle an ein Ziel übertragen wird

Anmerkung 1 zum Begriff: In älteren Ausgaben von prEN 13757-3 wurde das Datagramm als Telegramm bezeichnet.

3.6

Flüchtiger Schlüssel

Schlüssel der zum Verschlüsseln oder Entschlüsseln einer einzigen Nachricht oder einer Sitzung, welche in dem System flüchtig sind

3.7

Fragment

Datagramm einer fragmentierten Nachricht

3.8

Hex-ASCII

Als ASCII-Zeichen verschlüsselte Zahlen mit Basis 16 ("0"- "9", "A"- "F")

[QUELLE: ANSI X9 TR-31:2010]

3.9

Initialisierungsvektor

Zahl, die als Startpunkt für die Verschlüsselung von Datensequenzen verwendet wird, um die Sicherheit durch die Einrichtung zusätzlicher kryptographischer Abweichungen zu erhöhen und kryptographische Ausrüstungen zu synchronisieren

3.10

Schlüsselkomponente

einer von mindestens zwei Parametern mit den Merkmalen (z. B. Format, Zufälligkeit) eines kryptographischen Schlüssels, der mit einem oder mehreren ähnlichen Parametern kombiniert wird, um einen kryptographischen Schlüssel zu formen

[QUELLE: EN ISO 11568-3:1996]

3.11

Schlüsselableitung

Methode, mit der eine (potenziell große) Anzahl an Schlüsseln aus einem einzelnen anfänglichen Schlüssel und nicht geheimen variablen Daten erzeugt ("abgeleitet") wird, wobei jeder daraus resultierende Schlüssel einen nicht umkehrbaren Prozess verwendet

3.12

Schlüssel verschlüsselnder Schlüssel

KEK (en: key-encrypting key)

kryptographischer Schlüssel, der für die Verschlüsselung oder Entschlüsselung von anderen Schlüsseln verwendet wird

[QUELLE: NIST/SP 800-57 Part 1:2012-07]

3.13

Schlüssel-Wrapping-Schlüssel

symmetrischer Schlüssel, der die Wrapping- und Unwrapping-Funktionen eines Schlüssel-Wrapping-Mechanismus festlegt

3.14

Schlüssel-Wrapping-Mechanismus

durch einen symmetrischen Schlüssel authentifizierter Verschlüsselungsmechanismus, der die kryptographischen Schlüssel und andere spezialisierte Daten schützen soll

3.15

Nachricht

funktionale Gruppe von Daten, die von der Quelle an das Ziel übertragen werden

Anmerkung 1 zum Begriff: Eine Nachricht kann aus einem oder mehreren Datagrammen bestehen.

3.16

persistenter Schlüssel

kryptographischer Schlüssel, der über einen längeren Zeitraum hinweg behalten werden muss

3.17

Pseudozufallsfunktion

Prozess, der verwendet werden kann, um eine Ausgabe aus einem zufälligen Startwert zur Initialisierung eines Zufallszahlengenerators und einer Datenvariable zu erzeugen, damit die Ausgabe rechnerisch von einer komplett zufälligen Ausgabe unterschieden werden kann

Anmerkung 1 zum Begriff: Siehe NIST/SP 800-108:2009-10.

3.18

Wiedergabeschutz

Erkennung der (versuchten) Wiederholung einer Nachricht zu einem späteren Zeitpunkt

3.19

sicheres kryptographisches Gerät

Gerät, das eine sichere Speicherung für geheime Informationen wie Schlüssel sowie Sicherheitsdienste basierend auf diesen geheimen Informationen bereitstellt

[QUELLE: EN ISO 11568-3:1996]

3.20

Schutzmechanismus

Betriebsmodus eines (symmetrischen) kryptographischen Algorithmus

Anmerkung 1 zum Begriff: Der Sicherheitsmechanismus wird vom Sicherheitsmodus identifiziert.

3.21

Sicherheitsmodus

Modusnummer im Konfigurationsfeld, die einen Satz angewandter Sicherheitsmechanismen identifiziert

3.22

Sicherheitsdienst

Authentifizierung, Vertraulichkeit und Datenintegrität

Anmerkung 1 zum Begriff: Sicherheitsdienste werden von Schutzmechanismen bereitgestellt.

3.23

Teilschicht

Untergliederung einer Schicht

[QUELLE: EN ISO/IEC 7498-1:1995]

3.24

Transport-Masterschlüssel

TMK (en: Transport Master Key)

Schlüssel verschlüsselnder Schlüssel zur Übertragung eines Masterzählerschlüssels auf den Zähler

4 Abkürzungen und Symbole

4.1 Abkürzungen

ACC-DMD	Access Demand	Zugriffsbedarf
ACC-NR	Access – No Reply	Zugriff – Keine Antwort
ACK	Acknowledge	Quittieren [EN 13757-2/EN 13757-4]
AES	Advanced Encryption Standard	Advanced Encryption Standard
AFL	Authentication and Fragmentation Sublayer	Authentifizierungs- und Fragmentierungs-Teilschicht
APDU	Application Protocol Data Unit	Dateneinheit des Anwendungsprotokolls
APL	Application Layer	Anwendungsschicht
ASCII	American Standard Code for Information Interchange	
BCD	Binary Coded Decimal Numbers	Binär kodierte Dezimalzahlen

CBC	Cipher Block Chaining; (AES mode of operation) Cipher Block Chaining (AES-Betriebsmodus)
CCM	Counter mode encryption algorithm with CBC-MAC (AES mode of operation) Verschlüsselungsalgorithmus des Zählermodus mit CBC-MAC (AES-Betriebsmodus)
CF	Configuration field Konfigurationsfeld
CFE	Configuration Field Extension Konfigurationsfelderweiterung
CI	Control Information field Steuerinformationsfeld
CMAC	Cipher-based MAC [NIST/SP 800-38B] Chiffre-basierter MAC [NIST/SP 800-38B]
CMD	Command Befehl
CNF-IR	Confirm Installation Request Installationsanforderung bestätigen
CTR	Counter mode encryption algorithm (AES mode of operation) Verschlüsselungsalgorithmus des Zählermodus (AES-Betriebsmodus)
DES	Data Encryption Standard Data Encryption Standard
DIF	Data Information Field Dateninformationsfeld
DIFE	Data Information Field Extensions Dateninformationsfeld-Erweiterungen
DLL	Data Link Layer Datenverbindungsschicht
DLMS	Device Language Message Specification Device Language Message Specification
ELL	Extended Link Layer Erweiterte Verbindungsschicht
GCM	Galois/Counter Mode, an algorithm for authenticated encryption with associated data (AES mode of operation) Galois-/Zählermodus, ein Algorithmus für die authentifizierte Verschlüsselung mit zugehörigen Daten (AES-Betriebsmodus)
GMAC	a specialization of GCM for generating a message authentication code (MAC) on data that is not encrypted eine Spezialisierung des GCM zur Erzeugung eines Nachrichtenauthentifizierungscodes (en: Message Authentication Code, MAC) für nicht verschlüsselte Daten
IV	Initialisation Vector Initialisierungsvektor
KEK	Key-encrypting key Schlüssel verschlüsselnder Schlüssel
LSB	Least significant byte Niedrigstwertiges Byte
LSBit	Least significant bit Niedrigstwertiges Bit
MAC	Message Authentication Code Nachrichtenauthentifizierungscode ANMERKUNG MAC wird in anderen Normen auch als Akronym für Media Access Control (Medienzugriffskontrolle) für die Datenkommunikation in der Bitübertragungsschicht verwendet
MDH	Manufacturer Data Header Hersteller-Datenkopf

MK	Message Key (persistent)	Nachrichtenschlüssel (persistent)
MSB	Most significant byte	Höchstwertiges Byte
MSBit	Most significant bit	Höchstwertiges Bit
NWL	Network Layer	Netzwerkschicht
OBIS	Object Identification System (EN 62056-61)	
REQ-UD	Request User Data (Class 1 or 2)	Nutzerdaten anfordern (Klasse 1 oder 2) [EN 13757-2/EN 13757-4]
RSP-UD	Respond User Data [EN 13757-2/EN 13757-4]	Mit Nutzerdaten antworten [EN 13757-2/EN 13757-4]
RSSI	Received Signal Strength Indicator	Anzeiger für die Signalstärke des empfangenen Signals
SITP	Security Information Transfer Protocol	Übertragungsprotokoll für Sicherheitsinformationen
SM-CG	Smart Meter Co-ordination Group	Gemeinsame Arbeitsgruppe Smart Meter Co ordination Group
SND-IR	Send Installation Request	Installationsanforderung senden [EN 13757-4]
SND-NKE	Send Link Reset	Verbindungsrücksetzung senden [EN 13757-2/EN 13757-4]
SND-NR	Send – No Reply	Senden – Keine Antwort [EN 13757-4]
SND-UD	Send User Data	Nutzerdaten senden [EN 13757-2/EN 13757-4]
TPDU	Transport Protocol Data Unit	Transportprotokolldateneinheit
TPL	Transport Layer	Transportschicht
VIF	Value Information Field	Wertinformationsfeld
VIFE	Value Information Field Extensions	Wertinformationsfeld-Erweiterung

4.2 Symbole

Hexadezimalzahlen sind durch ein nachgestelltes „h“ gekennzeichnet.

Binärzahlen sind durch ein nachgestelltes „b“ gekennzeichnet.

Dezimalzahlen besitzen kein Suffix.

Die Verkettung der Felder ist durch das Symbol "||" gekennzeichnet. Z. B. 12h || 34 h ergibt 1 234 h.

5 Schichtmodell

5.1 M-Bus-Schichten

Der M-Bus deckt verschiedene Kommunikationsschichten ab. Die Bitübertragungsschicht und die Datenverbindungsschicht sind für alle Arten an Kommunikationen obligatorisch. Die Struktur dieser zwei

Schichten hängt vom Kommunikationsmedium (drahtgebundener M-Bus (EN 13757-2) und lokaler Bus (EN 13757-6) oder drahtloser M-Bus ab (EN 13757-4 und EN 13757-5)).

Das Vorhandensein der anderen Schichten hängt von Folgendem ab:

- Kommunikationsmedium (drahtgebundener/drahtloser M-Bus, Funkmodus),
- Nachrichtentyp (z. B. REQ-UD2 oder RSP-UD),
- Nachrichtenlänge (Fragmentierung erforderlich),
- ausgewählter Sicherheitsmodustyp.

Tabelle 1 zeigt die gültigen Schichten, ihre Reihenfolge und den damit verbundenen Teil dieser Normenreihe an, in der sie beschrieben werden. Die oberen Protokollschichten AFL, TPL und APL werden in dieser Norm spezifiziert.

Tabelle 1 — Reihenfolge der M-Bus-Schicht

Abkürzung	Schicht	An-gegeben durch CI-Feld	Entsprechen-der Teil dieser Normenreihe	Farb-codes	OSI-Modell Schicht
APL (en: Application Layer)	Anwendungsschicht	a	EN 13757-1/ prEN 13757-3/ EN 13757-5	Orange	Anwendung
TPL (en: Transport Layer)	Transportschicht	Ja	prEN 13757-3/ EN 13757-4	Grün	Präsentation Sitzung Transport
AFL (en: Authentication and Fragmentation Sublayer)	Authentifizierungs- und Fragmentierungs- Teilschicht	Ja	prEN 13757-3	Lila	
NWL (en: Network Layer)	Netzwerkschicht	Ja	EN 13757-5	Pink	Netzwerk
ELL (en: Extended Link Layer)	Erweiterte Verbindungsschicht	Ja	EN 13757-4	Blau	Daten- verbindung
DLL (en: Data Link Layer)	Datenverbindungs- schicht	Nein	EN 13757-2/ EN 13757-4/ EN 13757-5	Hellblau	
PHY (en: Physical Layer)	Bitübertragungs- schicht	Nein	EN 13757-2/ EN 13757-4/ EN 13757-5/ EN 13757-6	Hellgelb	Physikalisch
^a Die APL wird nicht von einem zugeordneten CI-Feld eingeführt, sondern vom CI-Feld der TPL angegeben.					

ANMERKUNG Die Beziehung zwischen den M-Bus-Schichten und den OSI-Schichten ist keine Eins-zu-Eins-Beziehung. Die OSI-Datenverbindungsschicht wird von zwei M-Bus-Schichten bereitgestellt (DLL und ELL). Die Funktionalität der OSI-Schichten 4 bis 6 wird von den M-Bus-Schichten AFL und TPL dargestellt.

5.2 Das CI-Feld-Prinzip

Alle Schichten zwischen der DLL und der APL werden von einem CI-Feld eingeführt (Steuerinformationsfeld). Diese CI-Felder geben die Struktur der folgenden Schichten an.

Die Schichten ELL und NWL nutzen eine feste Struktur. Deshalb informiert das CI-Feld indirekt über die Länge der zugehörigen Schichten und die Startposition des nächsten Felds. Die AFL verfügt über eine variable Struktur. Sie gibt die Länge dieser Schicht mithilfe eines zugehörigen Längenfelds an.

Die Transportschicht und die Anwendungsschicht nutzen ein geteiltes CI-Feld. Aus diesem Grund muss eine Transportschicht vorhanden sein, wenn die Anwendungsschicht in einer Nachricht verwendet wird. Die kürzeste Transportschicht (kein Header) besteht nur aus diesem CI-Feld. Das CI-Feld der Transportschicht gibt das verwendete Anwendungsprotokoll (wie M-Bus-Daten, DLMS-Daten oder Alarmprotokolle), den Ursprung der Nachricht (Master-Befehl oder Slave-Antwort) und die feste Kopfstruktur des TPL-Headers an. Hinter diesem CI-Feld folgt kein anderes CI-Feld.

Die Länge der APL wird durch die Nachrichtenlänge gegeben, die durch die Länge der anderen bestehenden Schichten reduziert wird.

Zu Einzelheiten der CI-Feld-spezifischen Datenrahmen(en: frame)-Struktur siehe Anhang A.

Tabelle 2 — Vom Master oder Slave verwendete Codes des CI-Felds

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
00 _h -1F _h	Reserviert für DLMS-basierte Anwendungen	APL (en: Application Layer)	keine	DLMS (siehe EN 13757-1)
20 _h -4F _h	Reserviert			
50 _h	Anwendungsrücksetzung oder -auswahl an Gerät	APL (en: Application Layer)	keine	Anwendungsauswahl; siehe prEN 13757-3:2016, 5.3
51 _h	Befehl an Gerät (voller M-Bus-Datenrahmen)	APL (en: Application Layer)	keine	M-Bus (nicht für drahtlos); Siehe prEN 13757-3:2016, 5.2
52 _h	Auswahl des Geräts		keine	Management Siehe 8.4
53 _h	Anwendungsrücksetzung oder -auswahl an Gerät	APL (en: Application Layer)	Lang	Anwendungsauswahl; siehe prEN 13757-3:2016, 5.3
54 _h	Anfrage der ausgewählten Anwendung an das Gerät	APL (en: Application Layer)	keine	Anwendungsauswahl; siehe prEN 13757-3:2016, 5.3
55 _h	Anfrage der ausgewählten Anwendung an das Gerät	APL (en: Application Layer)	Lang	Anwendungsauswahl; siehe prEN 13757-3:2016, 5.3
56 _h -59 _h	Reserviert			

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
5A _h	Befehl an Gerät (voller M-Bus-Datenrahmen)	APL (en: Application Layer)	Kurz	M-Bus; Siehe prEN 13757-3:2016, 4.2
5B _h	Befehl an Gerät (voller M-Bus-Datenrahmen)	APL (en: Application Layer)	Lang	M-Bus; Siehe prEN 13757-3:2016, 4.2
5C _h	Aktion Synchronisieren	APL (en: Application Layer)	keine	Siehe prEN 13757-3:2016, 4.8
5D _h - 5E _h	Reserviert			
5F _h	Spezifische Nutzung ^b	APL (en: Application Layer)	Lang	ANMERKUNG Siehe Literaturhinweis [12].
60 _h	Befehl an Gerät	APL (en: Application Layer)	Lang	DLMS/COSEM mit OBIS-Identifikator (siehe EN 13757-1 und EN 62056-5-3) ^a
61 _h	Befehl an Gerät	APL (en: Application Layer)	Kurz	DLMS/COSEM mit OBIS-Identifikator (siehe EN 13757-1 und EN 62056-5-3) ^a
62 _h - 63 _h	Reserviert			
64 _h	Befehl an Gerät	APL (en: Application Layer)	Lang	Reserviert für Beschreiber von Werten des Typs OBIS ^a
65 _h	Befehl an Gerät	APL (en: Application Layer)	Kurz	Reserviert für Beschreiber von Werten des Typs OBIS ^a
66 _h	Antwort bezüglich der ausgewählten Anwendung vom Gerät	APL (en: Application Layer)	keine	Anwendungsauswahl; siehe prEN 13757-3:2016, 4.3
67 _h	Antwort bezüglich der ausgewählten Anwendung vom Gerät	APL (en: Application Layer)	Kurz	Anwendungsauswahl; siehe prEN 13757-3:2016, 4.3
68 _h	Antwort bezüglich der ausgewählten Anwendung vom Gerät	APL (en: Application Layer)	Lang	Anwendungsauswahl; siehe prEN 13757-3:2016, 4.3
69 _h	Antwort vom Gerät (M-Bus- Formatrahmen)	APL (en: Application Layer)	keine	M-Bus; siehe prEN 13757-3:2016, 4.2, Anhang G
6A _h	Antwort vom Gerät (M-Bus- Formatrahmen)	APL (en: Application Layer)	Kurz	M-Bus; siehe prEN 13757-3:2016, 4.2, Anhang G

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
6B _h	Antwort vom Gerät (M-Bus-Formatrahmen)	APL (en: Application Layer)	Lang	M-Bus; Siehe prEN 13757-3:2016, 4.2, Anhang G
6C _h	Zeitsynchronisierung zum Gerät	APL (en: Application Layer)	Lang	Siehe prEN 13757-3:2016, 4.4
6D _h	Zeitsynchronisierung zum Gerät	APL (en: Application Layer)	Lang	Siehe prEN 13757-3:2016, 4.4
6D _h	Zeitsynchronisierung zum Gerät	APL (en: Application Layer)	Lang	Siehe prEN 13757-3:2016, 4.4
6E _h	Anwendungsfehler vom Gerät	APL (en: Application Layer)	Kurz	Siehe prEN 13757-3:2016, 4.6
6F _h	Anwendungsfehler vom Gerät	APL (en: Application Layer)	Lang	Siehe prEN 13757-3:2016, 4.6
70 _h	Anwendungsfehler vom Gerät	APL (en: Application Layer)	keine	Siehe prEN 13757-3:2016, 4.6
71 _h	Alarm vom Gerät	APL (en: Application Layer)	keine	Siehe prEN 13757-3:2016, 4.5
72 _h	Antwort vom Gerät (voller M-Bus-Datenrahmen)	APL (en: Application Layer)	Lang	M-Bus; siehe prEN 13757-3:2016, 4.2
73 _h	Antwort vom Gerät (M-Bus-Kompaktrahmen)	APL (en: Application Layer)	Lang	M-Bus; siehe prEN 13757-3:2016, 4.2, Anhang G
74 _h	Alarm vom Gerät	APL (en: Application Layer)	Kurz	Siehe prEN 13757-3:2016, 4.5
75 _h	Alarm vom Gerät	APL (en: Application Layer)	Lang	Siehe prEN 13757-3:2016, 4.5
76 _h - 77 _h	Reserviert			
78 _h	Antwort vom Gerät (voller M-Bus-Datenrahmen)	APL (en: Application Layer)	keine	M-Bus; Siehe prEN 13757-3:2016, 4.2
79 _h	Antwort vom Gerät (M-Bus-Kompaktrahmen)	APL (en: Application Layer)	keine	M-Bus; siehe prEN 13757-3:2016, 4.2, Anhang G

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
7A _h	Antwort vom Gerät (voller M-Bus-Datenrahmen)	APL (en: Application Layer)	Kurz	M-Bus; Siehe prEN 13757-3:2016, 4.2
7B _h	Antwort vom Gerät (M-Bus-Kompaktrahmen)	APL (en: Application Layer)	Kurz	M-Bus; siehe prEN 13757-3:2016, Anhang G und prEN 13757-3:2016, 4.2
7C _h	Antwort vom Gerät	APL (en: Application Layer)	Lang	DLMS/COSEM mit OBIS-Identifikator (siehe EN 13757-1 und EN 62056-5-3) ^a
7D _h	Antwort vom Gerät	APL (en: Application Layer)	Kurz	DLMS/COSEM mit OBIS-Identifikator (siehe EN 13757-1 und EN 62056-5-3) ^a
7E _h	Antwort vom Gerät	APL (en: Application Layer)	Lang	Reserviert für Beschreiber von Werten des Typs OBIS ^a
7F _h	Antwort vom Gerät	APL (en: Application Layer)	Kurz	Reserviert für Beschreiber von Werten des Typs OBIS ^a
80 _h	Transportschicht zum Gerät (ohne APL)	TPL (en: Transport Layer)	Lang	Siehe EN 13757-4
81 _h	Netzwerkschichtdaten	NWL (en: Network Layer)		Siehe EN 13757-5
82 _h	Reserviert			Siehe EN 13757-4, EN 13757-5
83 _h	Netzwerkmanagementdaten zum Gerät	APL (en: Application Layer)	keine	Siehe EN 13757-5
84 _h	Transportschicht zum Gerät (M-Bus-Kompaktrahmen erwartet)	TPL (en: Transport Layer)	Lang	Siehe prEN 13757-3:2016, Anhang G
85 _h	Transportschicht zum Gerät (M-Bus-Formatrahmen erwartet)	TPL (en: Transport Layer)	Lang	Siehe prEN 13757-3:2016, Anhang G
86 _h - 88 _h	Reserviert			Siehe EN 13757-4, EN 13757-5
89 _h	Netzwerkmanagementdaten vom Gerät	NWL (en: Network Layer)	keine	Siehe EN 13757-5
8A _h	Transportschicht vom Gerät (ohne APL)	TPL (en: Transport Layer)	Kurz	Siehe EN 13757-4
8B _h	Transportschicht vom Gerät	TPL (en: Transport Layer)	Lang	Siehe EN 13757-4

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
	(ohne APL)	Transport Layer)		
8C _h - 8F _h	Erweiterte Verbindungsschicht	ELL (en: Extended Link Layer)		Siehe EN 13757-4
90 _h	Authentifizierungs- und Fragmentierungs-Teilschicht	AFL (en: Authentication and Fragmentation Sublayer)		Siehe Abschnitt 0
91 _h	Reserviert			
92 _h - 97 _h	Reserviert			Siehe EN 13757-4, EN 13757-5
98 _h - 9D _h	Reserviert			
9E _h	Spezifische Nutzung ^b	APL (en: Application Layer)	Kurz	ANMERKUNG Siehe Literaturhinweis [12]
9F _h	Spezifische Nutzung ^b	APL (en: Application Layer)	Lang	ANMERKUNG Siehe Literaturhinweis [12].
A0 _h - B7 _h	Herstellerspezifisch	APL (en: Application Layer)		Siehe prEN 13757-3:2016, 4.9
B8 _h	Baudrate auf 300 Baud setzen	APL (en: Application Layer)	keine	Managmement der unteren Schichten; Siehe 8.2
B9 _h	Baudrate auf 600 Baud setzen	APL (en: Application Layer)	keine	Managmement der unteren Schichten; Siehe 8.2
BA _h	Baudrate auf 1 200 Baud setzen	APL (en: Application Layer)	keine	Managmement der unteren Schichten; Siehe 8.2
BB _h	Baudrate auf 2 400 Baud setzen	APL (en: Application Layer)	keine	Managmement der unteren Schichten; Siehe 8.2
BC _h	Baudrate auf 4 800 Baud setzen	APL (en: Application Layer)	keine	Managmement der unteren Schichten; Siehe 8.2
BD _h	Baudrate auf 9 600 Baud setzen	APL (en: Application Layer)	keine	Managmement der unteren Schichten; Siehe 8.2
BE _h	Baudrate auf 19 200 Baud	APL (en:	keine	Managmement der unteren Schichten;

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
	setzen	Application Layer)		Siehe 8.2
BF _h	Baudrate auf 38 400 Baud setzen	APL (en: Application Layer)	keine	Management der unteren Schichten; Siehe 8.2
C0 _h	Befehl an Gerät	APL (en: Application Layer)	Lang	Image-Übertragung; siehe prEN 13757-3:2016, Anhang I
C1 _h	Antwort vom Gerät	APL (en: Application Layer)	Kurz	Image-Übertragung; siehe prEN 13757-3:2016, Anhang I
C2 _h	Antwort vom Gerät	APL (en: Application Layer)	Lang	Image-Übertragung; siehe prEN 13757-3:2016, Anhang I
C3 _h	Befehl an Gerät	APL (en: Application Layer)	Lang	Sicherheitsinformationenübertragung; siehe Anhang B
C4 _h	Antwort vom Gerät	APL (en: Application Layer)	Kurz	Sicherheitsinformationenübertragung; siehe Anhang B
C5 _h	Antwort vom Gerät	APL (en: Application Layer)	Lang	Sicherheitsinformationenübertragung; siehe Anhang B
C6 _h -FF _h	Reserviert			
ANMERKUNG Alle SND-UD-Datagramme sind in der Datenverbindungsschicht zu quittieren, selbst wenn die Funktion dieser CI-Felder nicht implementiert ist.				
^a Die Anwendungsprotokolle beinhalten ebenfalls OBIS-Kennungen. Im M-Bus Anwendungsprotokoll sind diese OBIS Kennungen nicht enthalten, können aber nachträglich hinzugefügt werden. Anhang H ist zu verwenden, um die OBIS Kennungen aus den M-Bus Daten, prEN 13757-3:2016, zu generieren. ^b Siehe Referenz in den Literaturhinweisen zur Verwendung dieses Modus zum Zeitpunkt der Veröffentlichung dieser Norm.				

6 Authentifizierungs- und Fragmentierungs-Teilschicht (AFL, en: Authentication and Fragmentation Sublayer)

6.1 Einleitung

Die AFL ist als Teil der Transportschicht anzusehen. Dieser Abschnitt erklärt die Nutzung der Authentifizierungs- und Fragmentierungs-Teilschicht (AFL) in Kombination mit den anderen Schichten und Sicherheitsmodi.

Die Authentifizierungs- und Fragmentierungs-Teilschicht bietet die folgenden drei essentiellen Dienstleistungen:

- Fragmentierung langer Nachrichten in mehreren Datagrammen

- einen Nachrichtenauthentifizierungscode (MAC) zum Nachweis der Authentifizierung der TPL und APL
- einen Nachrichtenzähler, der eine sicherheitsrelevante Nachrichtenidentifizierung bietet, die für die Schlüsselableitungsfunktion verwendet werden darf (siehe 9.6.1).

Diese optionale Schicht muss angewandt werden, wenn mindestens eine dieser Dienstleistungen erforderlich ist.

ANMERKUNG Nachrichtenauthentifizierungscode (MAC) und Nachrichtenzähler können ebenfalls von Sicherheitsmechanismen in der Transportschicht bereitgestellt werden.

Eine Fragmentierung ist erforderlich, wenn große Nachrichten, wie beispielsweise Softwareupdates, transportiert werden. Die AFL ist in einen Abschnitt pro Fragment und einen Abschnitt für die gesamte Nachricht unterteilt. Die Position der AFL im M-Bus-Schichtmodell ist in Tabelle 1.

Im Allgemeinen dürfen zwei alternative, von MAC unterstützte Nachrichtenauthentifizierungs- und Integritätskapazitäten in der AFL angewandt werden.

- individuelle Fragmentauthentifizierung durch einen MAC (dies kapselt die Authentifizierung der Fragmente als schichtspezifische Protokolldateneinheiten ein),
- Authentifizierung der Gesamtnachricht durch einen MAC (dies kombiniert den Fragmenttransport mit der Authentifizierung einer Anwendungsprotokolldateneinheit).

Der MAC-Dienst (siehe 9.4.5.2) schützt alle obigen Schichten der AFL während der Übertragung. Deshalb sind in den höheren Schichten keine Änderungen möglich, sobald der MAC berechnet wurde.

Um die Authentifizierung der APDUs mit anderen Kommunikationspartnern über den medienabhängigen Transport hinaus zu gewährleisten, ist ein zusätzlicher MAC-Dienst in der Anwendungsschicht anwendbar.

6.2 Übersicht über die AFL-Struktur

Eine Nachricht besteht aus einem oder mehreren Fragmenten. Jedes Fragment muss in einem Daten Verbindungsschichtdatenrahmen transportiert werden. Die schattierten Tabelle 3 sind in jedem Fragment vorhanden. Die anderen Felder sind optional.

Tabelle 3 — Übersicht über alle AFL-Felder

Größe (Bytes)	Feldname	Beschreibung
1	CI	Zeigt an, dass eine Authentifizierungs- und Fragmentierungs-Teilschicht folgt.
1	AFL	AFL-Länge
2	FCL	Fragmentierungs-Kontrollfeld
1	MCL	Fragmentierungs-Kontrollfeld ^a
2	KI	Schlüsselinformationfeld ^a
4	MCR	Nachrichtenzählerfeld ^a
N ^b	MAC	Nachrichtenauthentifizierungscode ^a
2	ML	Nachrichtenlängenfeld ^a

Größe (Bytes)	Feldname	Beschreibung
^a		Dies ist ein optionales Feld. Ihre Aufnahme wird durch das Fragmentierungskontrollfeld definiert, das in 6.3.2 spezifiziert wird.
^b		Die Länge des MAC hängt vom AT-Teilfeld in AFL.MCL ab.

Alle AFL-Felder mit mehreren Bytes, außer des AFL.MAC, müssen mit dem niedrigstwertigen Byte an erster Stelle übertragen werden (Little Endian).

6.3 Komponenten der AFL

6.3.1 AFL-Längenfeld (AFL.AFLL)

Dieses Feld beschreibt die Anzahl aller Bytes innerhalb der AFL, außer dem AFL.AFLL-Feld selbst.

Das AFL.AFLL-Feld gehört nicht zu den durch MAC geschützten Daten.

6.3.2 AFL-Fragmentierungskontrollfeld (AFL.FCL)

Das Fragmentierungskontrollfeld zeigt das Vorhandensein der folgenden Felder im aktuellen Fragment an.

Das AFL.FCL-Feld (siehe Tabelle 4) gehört nicht zu den durch MAC geschützten Daten.

Tabelle 4 — AFL-Fragmentierungskontrollfeld – Definitionen der Bitfelder

Bit	Feldname	Beschreibung
15	RES	Reserviert (standardmäßig 0 _b)
14	MF	Mehr Fragmente 0 _b Dies ist das letzte Fragment 1 _b Mehr Fragmente folgen
13	MCLP	In diesem Fragment ist eine Nachrichtenkontrolle vorhanden
12	MLP	In diesem Fragment ist eine Nachrichtenlänge vorhanden
11	MCRP	In diesem Fragment ist ein Nachrichtenzähler vorhanden
10	MACP	In diesem Fragment ist ein MAC vorhanden
9	KIP	In diesem Fragment sind Schlüsselinformationen vorhanden
8	RES	Reserviert (standardmäßig 0 _b)
7 bis 0	FID	Fragment-ID

Die Fragment-ID wird zur Identifizierung jedes einzelnen Fragments einer langen Nachricht verwendet. Die FID muss für das erste Fragment einer fragmentierten Nachricht auf 1 gesetzt werden. Die FID muss mit jedem Fragment schrittweise erhöht werden. Die FID darf niemals überlaufen. Für unfragmentierte Nachrichten muss die FID auf 0 gesetzt werden.

6.3.3 AFL-Nachrichtenkontrollfeld (AFL.MCL)

Das AFL-Nachrichtenkontrollfeld zeigt das Vorhandensein der folgenden Felder in einem Fragment der Nachricht an (siehe Tabelle 5).

Tabelle 5 — AFL-Nachrichtenkontrollfeld - Definitionen der Bitfelder

Bit	Feldname	Beschreibung
7	RES	Reserviert (standardmäßig 0 _b)
6	MLMP	In dieser Nachricht ist eine Nachrichtenlänge vorhanden
5	MCMP	In dieser Nachricht ist ein Nachrichtenzähler vorhanden
4	KIMP	In dieser Nachricht sind Schlüsselinformationen vorhanden
3	AT	Authentifizierungstyp (siehe Tabelle 6)
2		
1		

Die Bits 4 bis 7 im AFL.MCL-Feld definiert das Vorhandensein von zusätzlichen Feldern in der Nachricht. Das Feld ist vorhanden, wenn das Bit eingestellt ist.

Tabelle 6 beschreibt die Nutzung des AT-Teilfelds.

Wenn das AFL.MCL-Feld genutzt wird, muss es stets im ersten Fragment vorhanden sein. Es darf nicht in einem der folgenden Fragmente derselben Nachricht vorhanden sein.

Tabelle 6 — AT-Teilfeld von AFL.MCL

Wert	Authentifizierungstyp	Länge des Authentifizierungs-codes
	Keine Authentifizierung	
1...2	Reserviert	
3	AES-CMAC-128	2 Bytes
4	AES-CMAC-128	4 Bytes
5	AES-CMAC-128	8 Bytes
6	AES-CMAC-128	12 Bytes
7	AES-CMAC-128	16 Bytes
8	AES-GMAC-128	12 Bytes
9...15	Reserviert	

Die Norm erlaubt verschiedene Niveaus der Integritätsstärke, z. B. durch Auswahl der Authentifizierungstagslänge. Das Niveau muss je nach Anwendungstyp ausgewählt werden (z. B. Übertragung des Verbrauchswerts, Schaltbefehle, Softwareupdate, usw.).

6.3.4 AFL-Schlüsselinformationsfeld (AFL.KI)

Das Schlüsselinformationsfeld (siehe Tabelle 7) ermöglicht es dem Empfänger einer Nachricht, den zugehörigen Authentifizierungsschlüssel zu identifizieren.

Tabelle 7 — AFL-Schlüsselinformationfeld – Definitionen der Bitfelder

Bit	Feldname	Beschreibung
15 bis 8	Schlüsselversion	Die Schlüsselversion identifiziert die angewandte Schlüsselversion, wie in 7.7.1 spezifiziert.
7 bis 6	RES	Reserviert (standardmäßig 0 _b)
5 bis 4	KDF-Auswahl	Die KDF-Auswahl identifiziert die angewandte Schlüsselableitungsfunktion, wie in Tabelle 25 spezifiziert.
3 bis 0	Schlüssel-ID	Die Schlüssel-ID identifiziert den angewandten Schlüssel, wie in Tabelle 24 spezifiziert.

Im Fall einer individuellen Fragmentauthentifizierung muss der Nachrichtenschlüssel für alle Fragmente der Nachricht angewandt werden. Wenn keine KI vorliegt, müssen die Werte des Konfigurationsfelds in der TPL für die Schlüsselauswahl verwendet werden.

6.3.5 AFL-Nachrichtenzählerfeld (AFL.MCR)

Tabelle 8 — AFL-Nachrichtenzählerfeld - Definitionen der Bitfelder

Bits	Feldname	Beschreibung
31 bis 0	C	AFL-Nachrichtenzähler dieser Nachricht. Siehe 9.2 für nähere Angaben.

Das Vorhandensein des abgelegten AFL.MCR hängt vom ausgewählten Sicherheitsmodus ab. Siehe 9.4 für nähere Angaben.

Wenn das Nachrichtenzählerfeld genutzt wird, muss das AFL.MCR-Feld stets im ersten Fragment vorhanden sein. Es darf nicht in einem der folgenden Fragmente derselben Nachricht vorhanden sein.

6.3.6 AFL-MAC-Feld (AFL.MAC)

Die Länge des MAC-Felds hängt von der ausgewählten Option im AT-Teilfeld ab, das durch das AFL.MCL-Feld angezeigt wird.

Wenn das MAC-Feld genutzt wird, muss das AFL.MAC-Feld im Fall einer

- individuellen Fragmentauthentifizierung: in jedem Fragment;
- Nachrichtenauthentifizierung: nur im letzten Fragment einer Nachricht vorhanden sein.

Abweichend von der üblichen Übertragungsreihenfolge für Felder mit mehreren Bytes im M-Bus muss das MSB des MAC als erstes Byte und das LSB als letztes Byte übertragen werden. Für Einzelheiten zur Verwendung des MAC siehe 9.3.

6.3.7 AFL-Nachrichtenlängenfeld (AFL.ML)

Das Feld AFL.ML (siehe Tabelle 9) gibt die Anzahl an Bytes nach dem AFL.ML bis zum Ende der nicht fragmentierten Nachricht an (ausschließlich der Verbindungsschichtfelder wie CRC oder Prüfsumme).

Die Nachrichtenlänge muss berechnet werden, bevor die Nachricht in mehrere Fragmente aufgeteilt wird.

Tabelle 9 — AFL-Nachrichtenlängenfeld - Definitionen der Bitfelder

Bits	Feldname	Beschreibung
15 bis 0	ML	Die Nachrichtenlänge erlaubt eine Länge von höchstens 64 kBytes. Die Nachrichtenlänge enthält die Summe aller Fragmente (beginnend ab TPL) für eine Nachricht. Sie umfasst keine DLL-, ELL- oder AFL-Felder.

ANMERKUNG 1 Die Nachrichtenlänge wird außerdem durch die maximale Anzahl der Fragment-IDs begrenzt (255).

ANMERKUNG 2 Nicht alle Empfänger können aufgrund der beschränkten Nachrichtenpuffergröße solch lange Nachrichten erhalten.

Das AFL.ML-Nachrichtenlängenfeld darf nur im ersten Fragment einer fragmentierten Nachricht vorhanden sein, um die Gesamtnachrichtenlänge anzuzeigen. Für nicht fragmentierte Nachrichten kann das AFL.ML-Feld deaktiviert werden.

7 Transportschicht (TPL)

7.1 Einleitung

Tabelle 10 zeigt eine allgemeine TPL-Struktur einer Nachricht mit einer integrierten APL. Tabelle 2 (siehe 5.2) zeigt die entsprechenden CI-Felder, die die TPL mit einem der möglichen TPL-Köpfe einführen (markiert durch "ohne", "kurz" oder "lang").

Tabelle 10 — Allgemeine Struktur der TPL

CI-Feld	TPL-Header	APL-Daten	TPL-Trailer (optional)
1 Byte	Ohne Header Kurzer Header Langer Header	Variable Anzahl	Variable Anzahl

Bei Verwendung eines langen Datenkopfes ist die Zähleradresse in diesem Header enthalten, während sich die vom Hersteller zugewiesene eindeutige Verbindungsschichtadresse unterscheiden kann (jedoch trotzdem innerhalb der gemeinsamen universell eindeutigen Adressstruktur liegt). Dadurch kann z. B. ein Drahtbus-zu-Funk-Konverter die unterstützte Zähleradresse im langen Datenkopf und seine eigene Adresse in der Funkdatenverbindungsschicht liefern. Für einen einfachen Zähler (der keinen zusätzlichen Konverter benötigt) ist der kurze Header ausreichend.

Wenn nichts anderes angegeben wird, müssen TPL-Felder mit mehreren Bytes diese mit dem niedrigstwertigen Byte an erster Stelle übertragen (Little Endian).

7.2 Struktur ohne TPL-Header

Diese Struktur besitzt keinen TPL-Header. Das erste Byte, das nach dem CI-Feld folgt, ist der Beginn der Anwendungsdaten. Übertragungseigenschaften wie Verschlüsselung, Zugriffsnummer oder eine zusätzliche Zähleradresse werden von dieser Datenstruktur nicht unterstützt.

Diese Struktur kann gemeinsam mit der erweiterten Verbindungsschicht nach EN 13757-4 verwendet werden.

7.3 Struktur mit kurzem TPL-Header

Die ersten 4 Bytes nach dem CI-Feld sind stets vorhanden. Dem Konfigurationsfeld darf je nach ausgewähltem Sicherheitsmodus im Konfigurationsfeld eine Konfigurationsfelderweiterung folgen. Danach

folgen optionale TPL-Header-Felder, die vom Sicherheitsmodus abhängen und im Konfigurationsfeld (siehe Tabelle 19 in 7.5.8) oder aus den Kontrollbits des Konfigurationsfelds bzw. der Konfigurationsfelderweiterung (siehe Tabelle 11) ausgewählt werden. Einzelheiten siehe 7.6.

Tabelle 11 — Kurzer TPL-Header

CI-abhängige Felder			CF-abhängige Felder	
Zugriffsnr.	Status	Konfigurationsfeld (en: Configuration Field, CF)	Konfigurationsfelderweiterung (en: Configuration Field Extension, CFE)	Optionale TPL-Header-Felder
1 Byte	1 Byte	2 Byte	0 bis n Bytes	0 bis n Bytes

Der kurze Datenkopf wird für Systeme verwendet, die die Bitübertragungsschicht und die Verbindungsschicht für Funk-M Bus-Kommunikation unterstützen (siehe EN 13757-4). In dieser Norm enthält die Verbindungsschichtadresse die Informationsfelder des Herstellers, die Identifikationsnummer, die Version und den Gerätetyp. Wenn die Zähleradresse mit der Verbindungsschichtadresse identisch ist oder die Zähleradresse von der sekundären Adresse ausgewählt wurde (siehe 8.4), dürfen die 8 Bytes der Zähleradresse von der Transportschicht ausgelassen werden.

7.4 Struktur mit langem TPL-Header

Die ersten 12 Bytes nach dem CI-Feld sind stets vorhanden. Dem Konfigurationsfeld darf je nach ausgewähltem Sicherheitsmodus im Konfigurationsfeld eine Konfigurationsfelderweiterung folgen. Danach folgen optionale TPL-Header-Felder, die vom Sicherheitsmodus abhängen und im Konfigurationsfeld (siehe Tabelle 19 in 7.5.8) oder aus den Kontrollbits des Konfigurationsfelds bzw. der Konfigurationsfelderweiterung (siehe Tabelle 12) ausgewählt werden. Einzelheiten siehe 7.6.

Tabelle 12 — Langer TPL-Header

CI-abhängige Felder							CF-abhängige Felder	
Ident.-Nr.	Hersteller	Version	Gerätetyp	Zugriffsnr.	Status	Konfigurationsfeld (en: Configuration Field, CF)	Konfigurationsfelderweiterung (en: Configuration Field Extension, CFE)	Opt. TPL-Header-Felder
4 Byte	2 Byte	1 Byte	1 Byte	1 Byte	1 Byte	2 Byte	0 bis n Byte	0 bis n Byte

Die Adressfelder des langen TPL-Headers enthalten unabhängig von der Übertragungsrichtung stets die Adresse des Zählers. Bei einer Funkkommunikation nach EN 13757-4 muss der lange TPL-Header verwendet werden, wenn sich die Verbindungsschichtadresse von der Zähleradresse unterscheidet.

7.5 CI-Feld-abhängige Elemente

7.5.1 Identifikationsnummer

Die Identifikationsnummer ist entweder eine bestimmte Fabrikationsnummer oder eine vom Kunden änderbare Nummer, die mit 8 BCD-gepackten Ziffern (4 Bytes) kodiert ist und daher von 00000001 bis

99999999 reicht. Während der Fertigung kann eine eindeutige Nummer voreingestellt werden, die anschließend jedoch geändert werden darf, besonders, wenn zusätzlich eine eindeutige und nicht änderbare Fabrikationsnummer (siehe auch 8.5) bereitgestellt wird.

Ein Fh an einer beliebigen Stelle der Identifikationsnummer ist als Platzhalter zu interpretieren. Ein Platzhalter kann eine beliebige Zahl mit einem Wert von 0 bis 9 ersetzen. Eine Identifikationsnummer von beispielsweise 112233FF spricht alle Zähler mit Identifikationsnummern von 11223300 bis 11223399 an. Platzhalter werden vom Kommunikationspartner verwendet, um eine Gruppe von Zählern anzusprechen. Ein Zähler muss die Adresse mit Platzhaltern akzeptieren, wenn sie mit seiner eigenen Adresse übereinstimmt.

7.5.2 Identifikation des Herstellers

Das Feld Hersteller ist als vorzeichenlose Binärzahl mit 2 Bytes kodiert. Diese Hersteller-ID wird aus dem ASCII-Code der Hersteller-ID nach EN 62056-21 (drei Großbuchstaben) nach folgender Gleichung berechnet:

$$\begin{aligned} \text{Man. Hersteller-ID [ASCII (1. Buchstabe)} & - 64] \times 32 \times 32 \\ & [\text{ASCII (2. Buchstabe)} - 64] \times 32 \\ & [\text{ASCII (3. Buchstabe)} - 64] \end{aligned} \quad (1)$$

ANMERKUNG Verwaltet werden diese aus drei Buchstaben bestehenden Hersteller-IDs nach EN 62056-21 von der der britischen DLMS User Association (<http://www.dlms.com/flag>).

Ein FFh ist als Platzhalter zu interpretieren. Ein Platzhalter kann durch einen Wert von 00h bis FEh ersetzt werden. Eine Herstelleridentifikation FFFFh spricht den Zähler unabhängig von seiner eigenen Herstelleridentifikation an. Platzhalter werden vom Kommunikationspartner verwendet, um eine Gruppe von Zählern anzusprechen. Ein Zähler muss die Adresse mit Platzhaltern akzeptieren, wenn sie mit seiner eigenen Adresse übereinstimmt.

7.5.3 Versionsidentifikation

Das Versionsfeld gibt die Generation bzw. Version des Geräts an und ist vom Hersteller abhängig. Es kann verwendet werden, um sicherzustellen, dass die Identifikationsnummer in jeder Versionsnummer eindeutig ist.

Der Wert FFh ist als Platzhalter zu interpretieren. Ein Platzhalter kann durch einen Wert von 00h bis FEh ersetzt werden. Platzhalter werden vom Kommunikationspartner verwendet, um eine Gruppe von Zählern anzusprechen. Ein Zähler muss die Adresse mit Platzhaltern akzeptieren, wenn sie mit seiner eigenen Adresse übereinstimmt.

7.5.4 Identifikation des Gerätetyps

Der Gerätetyp ist wie in Tabelle 13 angegeben kodiert.

Tabelle 13 — Identifikation des Gerätetyps

Gerätetyp (ehemals Medium)	Binärcode Bit 7...0	Hexadezimal- code
Sonstige	0000 0000	00
Ölzähler	0000 0001	01
Stromzähler	0000 0010	02
Gaszähler	0000 0011	03
Wärmezähler	0000 0100	04
Dampfzähler	0000 0101	05
Warmwasserzähler (30 °C ... 90 °C) ^e	0000 0110	06

Gerätetyp (ehemals Medium)	Binär-code Bit 7...0	Hexadezimal- code
Wasserzähler ^e	0000 0111	07
Heizkostenverteiler	0000 1000	08
Druckluft	0000 1001	09
Kältezähler (Volumen, das am Rücklauftemperatúrausgang gemessen wird)	0000 1010	0A
Kältezähler (Volumen gemessen bei Vorlauftemperatur: Vorlauf)	0000 1011	0B
Wärmezähler (Volumen gemessen bei Vorlauftemperatur: Vorlauf)	0000 1100	0C
Kombinierte Wärme-/Kältezähler	0000 1101	0D
Bestandteile des Busses/Systems	0000 1110	0E
Unbekannter Gerätetyp	0000 1111	0F
Bewässerungswasserzähler ^d	0001 0000	10
Wasserdatenlogger	0001 0001	11
Gasdatenlogger	0001 0010	12
Gaskonverter	0001 0011	13
Wärmewert	0001 0100	14
Heißwasserzähler ($\geq 90\text{ °C}$) ^d	0001 0101	15
Kaltwasserzähler ^e	0001 0110	16
Doppelregister-Wasserzähler (heiß/kalt) ^{a, e}	0001 0111	17
Druckmesser	0001 1000	18
A/D-Umwandler	0001 1001	19
Rauchmelder	0001 1010	1A
Raumsensor (z. B. Temperatur oder Feuchte)	0001 1011	1B
Gasmelder	0001 1100	1C
Reserviert für Sensoren		1D bis 1F
Trennschalter (Elektrizität)	0010 0000	20
Ventil (Gas oder Wasser)	0010 0001	21
Reserviert für Schalteinrichtungen		22 bis 24
Kundeneinheit (Anzeigegerät)	0010 0101	25
Reserviert für Endkundengeräte		26 bis 27
Abwasserzähler ^d	0010 1000	28
Abfall	0010 1001	29
Reserviert für Kohlenstoffdioxid	0010 1010	2A
Reserviert für Zähler für Umweltbelastungsmessung (Environmental Meter)		2B bis 2F

Gerätetyp (ehemals Medium)	Binärcode Bit 7...0	Hexadezimal- code
Servicewerkzeug	0011 0000	30
Kommunikationssteuergeräte (Gateway)	0011 0001	31
Unidirektionaler Repeater	0011 0010	32
Bidirektionaler Repeater	0011 0011	33
Reserviert für Systemgeräte		34 bis 35
Funkumsetzer (systemseitig) ^b	0011 0110	36
Funkumsetzer (zählerseitig) ^c	0011 0111	37
Busumsetzer (zählerseitig) ^c		
Reserviert für Systemgeräte		38 bis 3F
Reserviert		40 bis FE
Platzhalter	1111 1111	FF
^a Ein derartiger Zähler erfasst den Wasserdurchfluss oberhalb einer Grenztemperatur in einem separaten Register mit einer entsprechenden Tarif-ID. ^b Ein systemseitiger Funkumsetzer arbeitet als Funk-Master und Bus-Slave. ^c Ein zählerseitiger Funkumsetzer arbeitet als Slave wie ein Zähler. ^d Dieser Gerätetyp muss für nicht trinkbares Wasser/Industriewasser verwendet werden. ^e Dieser Gerätetyp muss für Trinkwasser verwendet werden.		

Ein FFh ist als Platzhalter zu interpretieren. Ein Platzhalter kann durch einen Wert von 00h bis FEh ersetzt werden. Platzhalter werden vom Kommunikationspartner verwendet, um eine Gruppe von Zählern anzusprechen. Ein Zähler muss die Adresse mit Platzhaltern akzeptieren, wenn sie mit seiner eigenen Adresse übereinstimmt.

7.5.5 Zugriffsnummer

7.5.5.1 Überblick

Die Zugriffsnummer ist Teil des festen Headers. Sie wird vom Protokoll der erweiterten Verbindungsschicht, der Transportschicht oder Anwendungsschicht verwendet. Sie ist als eine 1-Byte-lange vorzeichenlose Binärzahl kodiert. Ursprünglich wurde sie aufgenommen, um den drahtgebundenen M-Bus nach EN 13757-2 zu unterstützen, und sie signalisiert dem Nutzer, dass sein Zähler mittels des nach dem Pull-Prinzip funktionierenden Ableseverfahrens nach EN 13757-2 ausgelesen wurde. Diese Funktion unterstützt die Erkennung unerwünschter häufiger Auslesungen. Für den typischerweise nach dem Push-Prinzip funktionierenden häufigen Sendebetrieb von auf EN 13757-4 basierenden Funkgeräten ist diese Anwendung jedoch nicht mehr sinnvoll. Die annehmbare maximale Auslese- oder Übertragungshäufigkeit unterliegt entweder rechtlichen Bestimmungen oder wird vertraglich zwischen der auslesenden Organisation und dem Verbraucher festgelegt. Für Geräte nach EN 13757-4 muss die Zugriffsnummer zur klaren Angabe eines neuen Datagramms sowohl bei gepushten als auch bei angeforderten Daten streng nach den Regeln der Inkrementierung vergeben werden. Bei den durch den Partner erzeugten Datagrammen ist die Implementierung dank weniger strenger Generierungsregeln einfacher. Die Erkennungsregeln sind für Zähler und Partner identisch, d. h. ein Datagramm mit identischer Zugriffsnummer gilt als Wiederholung eines identischen, bereits zuvor empfangenen Datagramms und ist zu ignorieren. Alle Datagramme mit einer sich vom zuletzt empfangenen Datagramm unterscheidenden Zugriffsnummer werden als neues Datendatagramm betrachtet. „Neue Daten“ bedeutet dabei, dass die Zähleranwendung neuere Messwerte bereitstellt als im letzten (alten) Datendatagramm.

Diese verbindungsschichtorientierte Funktion reicht nicht aus, um von einer Anwendung stammende Nachrichten eindeutig zu identifizieren. Wenn eine Anwendung eine derartige eindeutige Identifizierung einer Nachricht erfordert, darf diese Nachricht um einen Datensatz mit VIF = FDh,08 h (eindeutige Nachrichtenidentifikation) und einer Datenlänge von mindestens 4 Byte ergänzt werden.

Wenn sowohl erweiterte Verbindungsschicht als auch Transportschicht vorhanden sind, wird die Zugriffsnummer der erweiterten Verbindungsschicht für die Taktung von synchronen Übertragungen verwendet, während die in der Transportschicht enthaltene Zugriffsnummer zur Kennzeichnung neuer Daten verwendet wird.

7.5.5.2 Erzeugen der Zugriffsnummer bei durch den Zähler eingeleiteten Datagrammen

Wenn ein Zähler ein Datagramm erzeugt (SND-NR, SND-IR, ACC-DMD oder ACC-NR; siehe EN 13757-4:2013, 11.5.4)), wird die Zugriffsnummer vor oder nach jeder neuen Übertragung des Zählers um eins inkrementiert (Modulo 256).

Wenn der Zähler die synchronisierte Übertragung für batteriebetriebene Empfänger (vgl. EN 13757-4) unterstützt, darf die Zugriffsnummer nur mit jeder synchronen Übertragung um genau eins erhöht werden. Bei jeder asynchronen Übertragung zwischen zwei synchronen Datagrammen muss der Zähler die Zugriffsnummer der letzten synchronen Übertragung verwenden. Um die Erkennung eines Null-Verbrauchs zu verhindern, wird empfohlen, dem Nachrichteninhalte einen Zeitstempel oder einen Aufwärtszähler (VIFE „Eindeutige Nachrichtenidentifikation“) hinzuzufügen, wenn im Zeitraum zwischen zwei synchronen Übertragungen eine oder mehrere asynchrone Übertragungen stattfinden. Falls eine solche asynchrone Übertragung neue Daten enthält, darf die erweiterte Verbindungsschicht für die Trennung der Anzeige der synchronen Übertragung von der Anzeige der neuen Daten genutzt werden.

Nachdem der Zähler eingeschaltet wurde, muss der Wert seiner Zugriffsnummer durch einen zufällig gewählten Anfangswert von 0 bis 255 eingestellt werden. Die Zugriffsnummer des Zählers darf nicht rücksetzbar sein.

Wenn das Datagramm eine Antwort auf ein Datagramm des Kommunikationspartners ist (d. h. ACK, RSP-UD oder sonstiges), dann wiederholt die Zugriffsnummer die empfangene Zugriffsnummer des Kommunikationspartners. In allen anderen Fällen wird die Zugriffsnummer des Zählers verwendet.

Vom Zähler initiierte Datagramme sind nach der Norm für den drahtgebundenen M-Bus (vgl. EN 13757-2) nicht zulässig.

7.5.5.3 Erzeugen der Zugriffsnummer bei durch den Partner erzeugten Datagrammen

Erzeugt der Kommunikationspartner ein drahtloses Datagramm (SND-UD, SND-NKE, REQ-UD1, REQ-UD2; siehe EN 13757-4:2013, 11.5.4)), so muss jedes Datagramm innerhalb von 300 s oder innerhalb des Mehrfachzugriffszyklus (en: frequent access cycle) nach EN 13757-4 einen anderen Wert der Zugriffsanzahl verwenden. Zur Erfüllung dieser Anforderung wird eine einfache Inkrementierung empfohlen. Sendet der Partner eine Antwort an den Zähler (d. h. ACK oder CNF-IR mit CI-Feld), so wiederholt die übertragene Zugriffsnummer des Partners die empfangene Zugriffsnummer des Zählers. Nach dem Einschalten des Kommunikationspartners ist dessen Wert nicht definiert, es wird jedoch ein Anfangswert von Null empfohlen.

Bei der drahtgebundenen Kommunikation nach EN 13757-2 muss der Zähler seine eigene Zugriffsnummer vor oder nach jeder Antwort (RSP-UD) an den Kommunikationspartner erhöhen. Sendet der Kommunikationspartner (M Bus-Master) eine Zugriffsnummer (z. B. mit einer SND_UD), so darf diese vom Zähler ignoriert werden.

ANMERKUNG Im Fall von verschlüsselten Befehlen stellt der Kommunikationspartner eine Zugriffsnummer zur Verfügung.

7.5.6 Statusbyte in Zählernachrichten

Tabelle 14 beschreibt die Nutzung jedes Bits im Statusbyte.

Tabelle 14 — Kodierung des Statusfelds

Bit	Bedeutung mit gesetztem Bit	Bedeutung mit nicht gesetztem Bit
7	Herstellerspezifisch	Herstellerspezifisch
6	Herstellerspezifisch	Herstellerspezifisch
5	Herstellerspezifisch	Herstellerspezifisch
4	Vorübergehender Fehler	Kein vorübergehender Fehler
3	Dauerhafter Fehler	Kein dauerhafter Fehler
2	Energieversorgung niedrig	Energieversorgung in Ordnung
1, 0	Siehe	Siehe

Tabelle 15 — Mit dem Statusfeld kodierte Anwendungsfehler

Statusbits 1 und 0	Anwendungsstatus
0 0	Kein Fehler
0 1	Anwendung beschäftigt
1 0	Beliebiger Anwendungsfehler
1 1	Ungewöhnlicher Zustand/Alarm

Die Statusbits sind in folgender Bedeutung zu verwenden:

Energiereserve niedrig	Warnung – Das Bit „Energiereserve niedrig“ wird nur gesetzt, um eine Unterbrechung der externen Energieversorgung oder das Ende der Batterielebensdauer zu signalisieren.
Permanenter Fehler	Ausfall – Das Bit „Permanenter Fehler“ wird nur gesetzt, wenn der Zähler einen schweren Gerätefehler (der eine Service-Aktion erfordert) signalisiert. Der Fehler kann nur durch eine Service-Aktion zurückgesetzt werden.
Temporärer Fehler	Warnung – Das Bit „Temporärer Fehler“ wird nur gesetzt, wenn der Zähler einen geringfügigen Fehlerzustand signalisiert (der keine unmittelbare Service-Aktion erfordert). Dieser Fehlerzustand darf später wieder verschwinden.
Beliebiger Anwendungsfehler	Dieses Bit ist zu verwenden, um einen Fehler während der Interpretation oder der Ausführung eines empfangenen Befehls mitzuteilen, z. B. wenn eine nicht entschlüsselbare Nachricht empfangen wurde. Der Zähler kann mithilfe des Anwendungsfehlerprotokolls in der nächsten Zählerantwort Einzelheiten über den aufgetretenen Anwendungsfehler zur Verfügung stellen (siehe prEN 13757-3:2016, 5.6).

Ungewöhnliche Zustände

Dieses Bit ist zu verwenden, wenn eine ordnungsgemäß funktionierende Anwendung ein ungewöhnliches Verhalten, z. B. bei einem Wasserzähler einen anhaltenden Wasserfluss, erkennt.

Weitere Angaben bezüglich des Fehlerzustands des Zählers können im M-Bus-Anwendungsprotokoll der Zählerantwort bereitgestellt werden (siehe prEN 13757-3:2016, Anhang E).

7.5.7 Statusbyte in Partnernachrichten

Informationen über Signalpegel beim Kommunikationspartner dürfen im Statusbyte in der Partnernachricht an den Zähler zurückgeschickt werden (siehe Tabelle 16). Dies ermöglicht die Durchführung der Kontrolle der RF-Übertragungsleistung vom Zähler während der Installation und des Betriebs.

Ein Feedback des RSSI kann während der Installation des Zählers nützlich sein. Informationen zur Verbindungsqualität sind für die Bewertung verschiedener Funkverbindungen zwischen einem Zähler und unterschiedlichen Partnern hilfreich. Darüber hinaus wird der Wert auch dazu verwendet, um einem Installationsdienstwerkzeug die Verbindungsqualität zu signalisieren.

Im Fall von Umgebungsgeräuschen ist der RSSI keine gute Basis für einen Leistungsanpassungsalgorithmus. Eine Messung des überschüssigen Rauschabstands oder der Verbindungsgrenze kann beim Betrieb nützlicher sein. Die Verbindungsgrenze drückt den Rauschabstand aus, während ein ausreichender Geräuschpegel für die Demodulation beibehalten wird (im Ermessen des Empfängers). Dadurch kann der Zähler eine eigenständige Leistungsniveaueinstellung durchführen, ohne von den Informationen über den erforderlichen Mindestauschabstand im Empfänger beim Kommunikationspartner abhängig zu sein.

Aus diesem Grund sollte der Kommunikationspartner eine gültige Verbindungsgrenze oder zumindest einen gültigen RSSI-Wert unterstützen.

Der Zähler darf seine Ausgangsleistung basierend auf der Verbindungsgrenze anpassen, aber der Zähler sollte über einen automatisierten Ausnahmebehandlungsmechanismus verfügen (um die RF-Übertragungsleistung auf einen Standardwert einzustellen), falls er über einen längeren Zeitraum hinweg keine Informationen vom Kommunikationspartner erhält.

Tabelle 16 — Bedeutung des Statusbytes für Partnernachrichten

Bit-Nr.	Wert und Bedeutung	
7	1:	Dieser Inhalt des Statusbytes ist für eine zukünftige Verwendung reserviert
	0:	Das Statusbyte enthält Signalpegelinformationen, die in den folgenden Bits spezifiziert werden
6	0:	Der Inhalt stellt den zuletzt erhaltenen RSSI-Wert für einen Empfang von diesem Zähler dar
	1:	Der Inhalt stellt die Verbindungsgrenze für den letzten Empfang von diesem Zähler dar
5..0	0..63:	Vorzeichenloser Integer. Die Zahl für den empfangenen Pegel muss, wie in Tabelle 17 dargestellt, gehandhabt werden

Tabelle 17 — Bedeutung der Bits 0 bis 5 im Statusbyte für Partnernachrichten

Typ	Wert und Bedeutung	
RSSI	0:	Kein RSSI-Wert vorhanden oder drahtgebundene Kommunikation
	1:	Der Empfangspegel liegt bei -128 dBm oder weniger
	2..62:	Der Empfangspegel wird als $-130 + (2 \times \text{RSSI-Wert})$ dBm berechnet Der Pegel liegt im Bereich -126 dBm bis - 6 dBm
	63:	Der Empfangspegel liegt bei -4 dBm oder höher
Verbindungs- grenze	0:	Keine Informationen zur Verbindungsgrenze vorhanden oder drahtgebundene Kommunikation
	1:	Die Verbindungsgrenze liegt bei -10 dB oder weniger
	2..62:	Die Verbindungsgrenze wird als $(-11 + \text{Verbindungsgrenzwert})$ dB berechnet Der Pegel liegt im Bereich -9 dB bis + 51dB
	63:	Die Verbindungsgrenze liegt bei + 52 dB oder höher

Der Wert „0“ in Bits 0 bis 5 bedeutet entweder, dass der Partner keine RSSI-Werte bereitstellt, oder, dass der Partner bislang keine Nachricht vom Zähler empfangen hat.

7.5.8 Konfigurationsfeld

Das Konfigurationsfeld (CF) besteht aus zwei Bytes und enthält Informationen über den angewandten Sicherheitsmodus. Dieser Sicherheitsmodus definiert:

- angewandten Satz an Schutzmechanismen;
- Inhalt anderer Bits im Konfigurationsfeld;
- Vorhandensein, Länge und Inhalt der Konfigurationsfelderweiterung (CFE);
- Nummer, Länge und Inhalt der optionalen TPL-Header-/Trailer-Felder nach dem Konfigurationsfeld bzw. der Konfigurationsfelderweiterung.

Tabelle 18 zeigt, wo die Sicherheitsmodusbits zu finden sind. Das Entschlüsseln anderer Bits (mit "X" gekennzeichnet) hängt vom ausgewählten Sicherheitsmodus ab (siehe 7.7).

Tabelle 18 — Allgemeine Definition der zwei obligatorischen Konfigurationsfeldbytes

MS Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LS Bit 0
Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch	Sicherheitsmodusbit 4	Sicherheitsmodusbit 3	Sicherheitsmodusbit 2	Sicherheitsmodusbit 1	Sicherheitsmodusbit 0	Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch	Sicherheitsmodus- spezifisch
X	X	X	M	M	M	M	M	X	X	X	X	X	X	X	X

Der Feldsicherheitsmodus im Konfigurationsfeld ermöglicht die Auswahl eines Schutzmechanismus zum Schutz der Nachricht. Tabelle 19 bietet eine Liste der verfügbaren Schutzmechanismen. Der Schutzmechanismus der Transportschicht ist in 9.4 beschrieben.

Tabelle 19 — Definition der Modusbits im Konfigurationsfeld (Sicherheitsmodus)

Sicherheitsmodus	Eigenschaften	Referenz
0	Keine Verschlüsselung angewendet	-
1	Herstellerspezifische Nutzung	9.4.2
2	DES; IV=0 (veraltet)	9.4.3
3	DES; IV≠0 (veraltet)	9.4.3
4	Spezifische Nutzung ^a	ANMERKUNG Siehe Literaturhinweis [6].
5	AES-CBC-128; IV≠0	9.4.4
6	Reserviert für zukünftige Nutzung	-
7	AES-CBC-128; IV=0	9.4.5
8	AES-CTR-128; CMAC	9.4.6
9	AES-GCM-128	9.4.7
10	AES-CCM-128	9.4.8
11	Reserviert für zukünftige Nutzung	-
12	Reserviert für zukünftige Nutzung	-
13	Spezifische Nutzung ^a	ANMERKUNG Siehe Literaturhinweis [8].
14	Reserviert für zukünftige Nutzung	-
15	Spezifische Nutzung ^a	ANMERKUNG Siehe Literaturhinweis [7].
16-31	Reserviert für zukünftige Nutzung	-

^a Siehe Referenz in den Literaturhinweisen zur Verwendung dieses Modus zum Zeitpunkt der Veröffentlichung dieser Norm

7.6 Konfigurationsfeld-abhängige Struktur

7.6.1 Allgemeines

Tabelle 20 — TPL-Struktur einer geschützten Nachricht

CI-Feld	TPL-Header			APL (en: Application Layer)		TPL-Trailer
	CI-abhängige Felder (siehe 7.3 und 7.4)	Konfigurationsfelderweiterung	Optionale TPL-Header-Felder	Verschlüsselte Anwendungsdaten	Nicht verschlüsselte Anwendungsdaten	Optionales TPL-Trailerfeld

Wenn ein kurzer oder langer TPL-Header angewandt wird, gibt es stets ein Konfigurationsfeld. Hinter dem Konfigurationsfeld und vor den Anwendungsdaten dürfen sich eine Konfigurationsfelderweiterung und zusätzliche optionale TPL-Header-Felder befinden. Außerdem dürfen sich optionale TPL-Trailer-Felder hinter den Anwendungsdaten befinden. Das Vorhandensein dieser Felder wird vom Konfigurationsfeld und der Konfigurationsfelderweiterung gesteuert.

Alle Felder vor dem Konfigurationsfeld, das Konfigurationsfeld selbst und die Konfigurationsfelderweiterung sind stets unverschlüsselt. Je nach ausgewähltem Sicherheitsmodus dürfen optionale TPL-Header-/Trailer-Felder verschlüsselt sein. Anwendungsdaten können verschlüsselt, unverschlüsselt oder teilverschlüsselt sein. Im Falle einer Teilverschlüsselung werden die verschlüsselten Daten stets vor den unverschlüsselten Daten übertragen (siehe 7.6.5).

Die Länge der gesicherten Daten ist entweder im Konfigurationsfeld oder in den optionalen TPL-Header-Feldern kodiert. Die Berechnung der Länge der verschlüsselten Daten hängt vom Sicherheitsmodus ab.

7.6.2 Konfigurationsfelderweiterung

Die Konfigurationsfelderweiterung ist eine optionale Komponente der TPL. Das Vorhandensein und der Inhalt hängen vom im Konfigurationsfeld ausgewählten Sicherheitsmodus ab.

Es enthält einen Satz an kontrollierenden Bits für sicherheitsrelevante Parameter wie Schlüssel-IDs, KDF-Funktionsdefinitionen und gibt Informationen über das Vorhandensein der folgenden optionalen TPL-Header- und TPL-Trailer-Felder.

7.6.3 Optionale TPL-Header-Felder

Die optionalen TPL-Header-Felder nach dem Konfigurationsfeld oder den Konfigurationsfelderweiterungen sind optionale Komponenten der TPL. Das Vorhandensein und die Größe hängen von den kontrollierenden Bits (einschließlich der Sicherheitsmodusbits) im Konfigurationsfeld oder den Konfigurationsfelderweiterungen ab.

Optionale TPL-Header-Felder enthalten sicherheitsrelevante Parameter, wie z. B. Zähler, Zeitstempel oder Längeninformationen über gesicherte Daten.

7.6.4 Optionale TPL-Trailer-Felder

Die optionalen TPL-Trailer-Felder nach der Anwendungsschicht sind optionale Komponenten, die sich am Ende der Nachricht befinden. Das Vorhandensein und die Länge werden von kontrollierenden Bits im Konfigurationsfeld bzw. der Konfigurationsfelderweiterung vordefiniert.

Zusammen mit dem TPL-Header umschließt der TPL-Trailer die Anwendungsdaten einer Nachricht. Er enthält sicherheitsrelevante Parameter wie Authentifizierungs-Tags und Zeitstempel.

7.6.5 Teilverschlüsselung

Wenn die Anzahl verschlüsselter Bytes kleiner ist als die gesamte Länge der Anwendungsdaten, dann folgen auf die verschlüsselten Daten unverschlüsselte Daten. Die Grenze zwischen verschlüsselten und nicht verschlüsselten Daten darf nicht in einem Datenpunkt liegen. Wenn nötig müssen die ungenutzten Bytes im verschlüsselten Teil durch Füllbytes aufgefüllt werden.

Einige Sicherheitsmodi spezifizieren die Anzahl an verschlüsselten Bytes oder Blöcken mithilfe der N-Bits des Konfigurationsfelds. Wenn alle N-Bits auf 1 gesetzt sind (z. B. NNNNNNNN = 1111111_b), wird spezifiziert, dass die Teilverschlüsselung deaktiviert ist und keine unverschlüsselten Daten nach den verschlüsselten Daten folgen. Dies resultiert in der Möglichkeit, sehr große fragmentierte Nachrichten zu

verschlüsseln. Wenn alle N-Bits auf 0_b gesetzt sind, folgen keine verschlüsselten Daten. Dies ist hilfreich, wenn die Nachricht unverschlüsselt, aber dennoch authentifiziert übertragen werden soll.

Für die korrekte Ablesung des unverschlüsselten Teils einer teilverschlüsselten Nachricht muss die Kopfstruktur des angewandten Sicherheitsmodus dem Empfänger der Nachricht bekannt sein.

ANMERKUNG 1 Einige Sicherheitsmodi fügen nach den optional unverschlüsselten Daten sicherheitsbezogene Felder hinzu (wie ein Authentifizierungs-Tag). Die Felder und Nummern der verbundenen Bytes werden durch den Header der Transportschicht angezeigt.

ANMERKUNG 2 Das Hinzufügen von verschlüsselten oder unverschlüsselten Daten von einem anderen Gerät (z. B. Repeater-Latenzzeit) zu einer authentifizierten Nachricht ist nicht realisierbar, da die Authentifizierung sonst fehlschlägt.

7.7 Sicherheitsmodus-spezifische TPL-Felder

7.7.1 Gemeinsame Teilfelder des Konfigurationsfelds und der Konfigurationsfelderweiterung

Abgesehen von der Sicherheitsmodusangabe definiert das Konfigurationsfeld zusätzliche modusspezifische Teilfelder. Dieser Abschnitt gibt die Teilfelder des Konfigurationsfelds an, das von mehreren Sicherheitsmodi geteilt wird (siehe 7.7.2 bis 7.7.8).

Teilfelder H und R: Nachrichtenwiederholung

Bit H und Bit R des Konfigurationsfeldes sind für die Verwendung in wiederholten Nachrichten reserviert, siehe EN 13757-5. Ein Zähler muss in einer übertragenen Nachricht immer $H = 0_b$ und $R = 0_b$ setzen. Der Zähler darf diese Bits in einer empfangenen Nachricht ignorieren.

Diese Bits sind für die drahtlose M-Bus-Kommunikation reserviert. Für die Kommunikation auf dem drahtgebundenen M-Bus müssen die Bits H und R auf "0" gesetzt werden. Einige Sicherheitsmodi können gelten, wenn dieser Dienst ELL verwendet wird (vgl. EN 13757-4).

Teilfeld CC: Nachrichteninhalt

Die Bits CC werden zur Beschreibung des Inhalts der Nachricht verwendet. Die Definition unterscheidet zwischen einer Zähler- und einer Partnernachricht (vgl. Tabelle 21 und Tabelle 22).

Tabelle 21 — Inhalt der Zählernachricht

Bit C_H	Bit C_L	Inhalte der Nachricht
0	0	Normdatennachricht
0	1	Reserviert für Nachrichtenpriorisierung
1	0	Statische Nachricht (bestehend aus Parameter, OBIS-Definitionen und sonstigen Daten, die nicht häufig verändert werden).
1	1	Reserviert für zukünftige Erweiterungen

Tabelle 22 — Inhalt der Partnernachricht

Bit C_H	Bit C_L	Inhalt der Datenpunktauthentifizierung
0	0	Normbefehlsnachricht
0	1	Reserviert für Befehlspriorisierung
1	0	Reserviert
1	1	Reserviert für zukünftige Erweiterungen

Teilfeld III: Inhaltsindex

Dieses Feld wird verwendet, um zwischen mehreren Zählerdatenrahmen mit unterschiedlichem Inhalt, aber mit demselben Inhaltsfeldwert "CC" zu unterscheiden. Mit diesem Feld kann ein Empfänger Datenrahmen mit unterschiedlichem Inhalt identifizieren und speichern oder filtern, ohne die Anwendungsdaten entschlüsseln zu müssen.

Für Sender, die diese optionale Funktion nicht unterstützen, muss dieses Feld stets auf 0 gesetzt werden. Empfänger, die diese optionale Funktion nicht unterstützen, müssen dieses Feld ignorieren.

Dieses Feld spezifiziert nicht den tatsächlichen Inhalt, das beste Vorgehen wäre die Nutzung des niedrigsten Wertes für die am häufigsten übertragenen Datenrahmen.

Teilfelder B, A und S: Verbindungszugriffskontrolle

Bit S wird zur Deklaration einer synchronisierten Übertragung verwendet. Wenn die Übertragungstaktung (vorhersagbare Übertragungszeit) die Anforderungen an eine synchrone Übertragung nach EN 13757-4 erfüllt, muss diese Übertragung durch Setzen von Bit S gekennzeichnet werden. Andernfalls muss das Bit S stets 0 sein. Einige Sicherheitsmodi können gelten, wenn dieser Dienst ELL verwendet (vgl. EN 13757-4).

Die Konfigurationsfeldbits A und B (Zugänglichkeit (en: Accessibility) und Bidirektionale Kommunikation) werden entsprechend Tabelle 23 zur Zugriffskontrolle für den Zähler verwendet.

Tabelle 23 — Zugänglichkeit eines Zählers

Bit B	Bit A	Zugänglichkeit eines drahtlosen Zählers
0	0	Zähler/Aktor stellt kein Zugriffsfenster bereit (unidirektionaler Zähler)
0	1	Zähler unterstützt allgemein den bidirektionalen Zugriff, nach dieser Übertragung gibt es jedoch kein Zugriffsfenster mehr
1	0	Zähler stellt nur unmittelbar nach dieser Übertragung ein kurzes Zugriffsfenster bereit
1	1	Zähler stellt unbegrenzten Zugriff bereit (mindestens bis zur nächsten Übertragung)

Einige Sicherheitsmodi können gelten, wenn dieser Dienst ELL verwendet (vgl. EN 13757-4).

Diese Bits sind für die drahtlose M-Bus-Kommunikation reserviert. Für die Kommunikation auf dem drahtgebundenen M-Bus müssen die Bits B, A und S auf "0" gesetzt werden.

Teilfeld KKKK: Schlüssel-ID

Die Schlüssel-ID (KKKK) wird verwendet, um den angewandten Schlüssel für diese Nachricht zu identifizieren. Tabelle 24 zeigt die Struktur der Schlüssel-ID-Liste.

Tabelle 24 — Die Schlüssel-ID

Schlüssel-ID	K	K	K	K	Verschlüsselung oder Authentifizierungsschlüssel
00	0	0	0	0	Anwenderschlüssel 0
01	0	0	0	1	Anwenderschlüssel 1
02	0	0	1	0	Anwenderschlüssel 2
03	0	0	1	1	Anwenderschlüssel 3
04	0	1	0	0	Anwenderschlüssel 4
05	0	1	0	1	Anwenderschlüssel 5
06	0	1	1	0	Anwenderschlüssel 6
07	0	1	1	1	Anwenderschlüssel 7
08	1	0	0	0	Anwenderschlüssel 8
09	1	0	0	1	Anwenderschlüssel 9
10	1	0	1	0	Anwenderschlüssel 10
11	1	0	1	1	Anwenderschlüssel 11
12	1	1	0	0	Anwenderschlüssel 12
13	1	1	0	1	Anwenderschlüssel 13
14	1	1	1	0	Anwenderschlüssel 14
15	1	1	1	1	Anwenderschlüssel 15

Im Fall von abgeleiteten flüchtigen Schlüsseln muss die Schlüssel-ID des persistenten Schlüssels (in KDF angewandt) verwendet werden.

Teilfeld V: Version (und Schlüssel-Versionsfeld)

Die Bitversion (V) aktiviert das Schlüssel-Versionsfeld. Das Schlüssel-Versionsfeld ist nur dann im TPL-Header vorhanden (siehe 7.7.5 bis 7.7.8), wenn das Versionsbit gesetzt wurde. Wenn das Schlüssel-Versionsfeld vorhanden ist, identifiziert es die angewandte Version des Schlüssels mit der entsprechenden Schlüssel-ID.

Das Schlüssel-Versionsfeld wird verwendet, um Schlüssel mit derselben Schlüssel-ID zu trennen (und für selben Zweck verwendet). Ein neuer Schlüssel sollte eine höhere Versionsnummer als ein älterer Schlüssel besitzen. Eine gültige Schlüsselversion liegt im Bereich von 1 bis 254. Der Wert 0 signalisiert, dass das Schlüssel-Versionsfeld nicht verwendet wird. Der Wert 255 ist für eine besondere Nutzung reserviert.

Im Fall von abgeleiteten flüchtigen Schlüsseln muss die Schlüssel-Version des persistenten Schlüssels (in KDF angewandt) verwendet werden.

ANMERKUNG Der Zähler verfügt normalerweise nur über einen kleinen Satz an Schlüsseln.

Teilfeld DD: KDF-Auswahl

Die KDF-Auswahl (DD) identifiziert die angewandte Schlüsselableitungsfunktion (KDF), falls vorhanden. Tabelle 25 zeigt die möglichen Werte dieses Teilfelds an.

Tabelle 25 — KDF-Auswahl

KDF	D	D	Angewandte Schlüsselableitungsfunktion
-	0	0	Persistenter Schlüssel ^a
A	0	1	Schlüsselableitungsfunktion A (siehe 9.6.1)
B	1	0	Reserviert
C	1	1	Reserviert

^a Keine Schlüsselableitung - gespeicherter Schlüssel wird direkt für die Verschlüsselung oder Authentifizierung verwendet

7.7.2 Konfigurationsfeld des Sicherheitsmodus 0

Tabelle 26 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 0.

Tabelle 26 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 0

Feld-name	Konfig. Feld (siehe Tabelle 27)	Nicht verschlüsselte Anwendungsdaten
Länge	2	..

Tabelle 27 — Definition des Konfigurationsfelds für den Sicherheitsmodus 0

MSBit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSBit 0
Bidirektionale Kommunikation	Zugänglichkeit	Synchronisiert	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Reserviert	Reserviert	Reserviert	Reserviert	Inhalt der Nachricht	Inhalt der Nachricht	Repeater-Zugriff	Hop-Zähler
B	A	S	M	M	M	M	M	0	0	0	0	C	C	R	H

Bit 0: Hop-Zähler "H"

- Dieses Bit ist spezifiziert in 7.7.1

Bit 1: Repeater-Zugriff "R"

- Dieses Bit ist spezifiziert in 7.7.1

Bit 2 bis Bit 3: Inhalt der Nachricht "CC"

- Diese Bits sind definiert in Tabelle 21 und
- Tabelle 22 (siehe 7.7.1)

Bit 4 bis Bit 7: Reserviert mit Wert gleich 0_b

Bit 8 bis Bit 12: Sicherheitsmodus "MMMM"

- Für die Spezifikation der Modi (siehe Tabelle 19)
- Modus 0 wird angegeben durch MMMMM= 00000_b

Bit 13: Synchronisierungsbit "S"

- Dieses Bit ist spezifiziert in 7.7.1

Bit 14: Zugänglichkeitsbit "A"

- Dieses Bit ist spezifiziert in 7.7.1

Bit 15: Bidirektionales Bit "B"

- Dieses Bit ist spezifiziert in 7.7.1

7.7.3 Konfigurationsfeld der Sicherheitsmodi 2 und 3

Tabelle 28 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle der Sicherheitsmodi 2 und 3

Tabelle 28 — Konfigurationsfeld und nachfolgende Felder mit den Sicherheitsmodi 2 und 3

Feld-name	Konfig. Feld (siehe Tabelle 29)	Verschlüsselte Anwendungsdaten	Nicht verschlüsselte Anwendungsdaten (optional)
Länge	2	NNNNNNNN	..

Tabelle 29 — Definition des Konfigurationsfeldes für die Sicherheitsmodi 2 und 3

MS Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSB it 0
Reserviert	Reserviert	Reserviert	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Anzahl an verschl. Bytes	Anzahl an verschl. Bytes	Anzahl an verschl. Bytes	Anzahl an verschl. Bytes	Anzahl an verschl. Bytes	Anzahl an verschl. Bytes	Anzahl an verschl. Bytes	Anzahl an verschl. Bytes
0	0	0	M	M	M	M	M	N	N	N	N	N	N	N	N

Bit 0 bis Bit 7: Länge "NNNNNNNN"

- Anzahl an Bytes der verschlüsselten Daten (e. g. NNNNNNNN = 00010000_b entspricht 32 Bytes; siehe auch 7.6.5.)

Bit 8 bis Bit 12: Sicherheitsmodus "MMMMM"

- Für die Spezifikation der Sicherheitsmodi (siehe Tabelle 19)
- Modus 2 wird angegeben durch MMMMM = 00010_b
- Modus 3 wird angegeben durch MMMMM = 00011_b

Bit 13 bis Bit 15: Reserviert mit Wert gleich 0_b

Siehe 9.4.3 für Einzelheiten über diese Sicherheitsmodi.

7.7.4 Konfigurationsfeld des Sicherheitsmodus 5

Tabelle 30 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 5.

Tabelle 30 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 5

Feld- name	Konfig. Feld (siehe Tabelle 31)	Entschlüsselungsverifizierung (verschlüsselt)	Verschlüsselte Anwendungsdaten	Nicht verschlüsselte Anwendungsdaten (optional)
Länge	2	2	16*NNNN - 2	::

Tabelle 31 — Definition des Konfigurationsfelds für den Sicherheitsmodus 5

MS Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LS Bit 0
Bidirektionale Kommunikation	Zugänglichkeit	Synchronisiert	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Anzahl an verschl. Blöcken	Anzahl an verschl. Blöcken	Anzahl an verschl. Blöcken	Anzahl an verschl. Blöcken	Inhalt der Nachricht	Inhalt der Nachricht	Repeater-Zugriff	Hop-Zähler
B	A	S	M	M	M	M	M	N	N	N	N	C	C	R	H

Für die Kommunikation auf dem drahtlosen M-Bus müssen die Bits wie folgt verwendet werden:

Bit 0: Hop-Zähler "H"

- Dieses Bit ist spezifiziert in 7.7.1

Bit 1: Repeater-Zugriff "R"

- Dieses Bit ist spezifiziert in 7.7.1

Bit 2 bis Bit 3: Inhalt der Nachricht "CC"

- Diese Bits sind definiert in Tabelle 21 und
- Tabelle 22 (siehe 7.7.1)

Bit 4 bis Bit 7: Länge "NNNN"

- Länge der verschlüsselten Daten, in Blocks von jeweils 16 Bytes angegeben (e. g. NNNN = 0010_b entspricht 32 Bytes; siehe auch 7.6.5)

Bit 8 bis Bit 12: Sicherheitsmodus "MMMM"

- Für die Spezifikation der Modi (siehe Tabelle 19)
- Modus 5 wird angegeben durch MMMMM = 00101_b

Bit 13: Synchronisierungsbit "S"

- Dieses Bit ist spezifiziert in 7.7.1

Bit 14: Zugänglichkeitsbit "A"

- Dieses Bit ist spezifiziert in 7.7.1

Bit 15: Bidirektionales Bit "B"

- Dieses Bit ist spezifiziert in 7.7.1

Siehe 9.4.4 für Einzelheiten über diese Sicherheitsmodi.

7.7.5 Konfigurationsfeld des Sicherheitsmodus 7

Tabelle 32 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 7.

Tabelle 32 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 7

Feld-name	Konfig.feld (siehe Tabelle 33)	Konfig.felderweiterung (siehe Tabelle 34)	Schlüsselversion	Nachrichtenzähler (optional)	Entschlüsselungsverifizierung (verschlüsselt)	Verschlüsselte Anwendungsdaten	Nicht verschlüsselte Anwendungsdaten (optional)
Länge	2	1	(1)	(4)	2	16*NNNN - 2	..

Tabelle 33 — Definition des Konfigurationsfelds für den Sicherheitsmodus 7

MSBit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSBit 0
Inhalt der Nachricht	Inhalt der Nachricht	Zählergröße	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Sicherheitsmodus	Anzahl an verschl. Blöcken	Anzahl an verschl. Blöcken	Anzahl an verschl. Blöcken	Anzahl an verschl. Blöcken	Inhaltsindex	Inhaltsindex	Inhaltsindex	Inhaltsindex
C	C	Z	M	M	M	M	M	N	N	N	N	I	I	I	I

Bit 0 bis Bit 3: Inhaltsindex "IIII"

- Inhaltsindex wie spezifiziert in 7.7.1.

Bit 4 bis Bit 7: Länge "NNNN"

- Länge der verschlüsselten Daten, in Blocks von jeweils 16 Bytes angegeben (e.g. NNNN = 0010_b entspricht 32 Bytes; siehe auch 7.6.5.)

Bit 8 bis Bit 12: Sicherheitsmodus "MMMMM"

- Für die Spezifikation der Sicherheitsmodi (siehe Tabelle 19)
- Modus 7 wird angegeben durch MMMMM = 00111_b

Bit 13: Zählergröße "Z"

- Dieses Bit definiert die Größe des Zählers in TPL
- Zählergrößenbit entspricht 0_b: Zählergröße ist 0 Byte (nicht vorhanden)
- Zählergrößenbit entspricht 1_b: Zählergröße ist 4 Byte (vorhanden)

Bit 14 bis Bit 15: Inhalt der Nachricht "CC"

Diese Bits sind definiert in Tabelle 21 und

Tabelle 22 (siehe 7.7.1)

Tabelle 34 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 7

MSBit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LSBit 0
Reserviert	Version	KDF-Auswahl	KDF-Auswahl	Schlüssel-ID	Schlüssel-ID	Schlüssel-ID	Schlüssel-ID
0 _b	V	D	D	K	K	K	K

Bit 0 bis Bit 3: Schlüssel-ID "KKKK"

- Schlüssel-ID, wie in Tabelle 24 spezifiziert (siehe 7.7.1)

Bit 4 bis Bit 5: KDF-Auswahl "DD"

- Selektor für die Schlüsselabweichungsfunktion, wie in Tabelle 25 spezifiziert (siehe 7.7.1)

Bit 6: Version "V"

- Versionsbit entspricht 0_b: das Feld Schlüssel-Version ist nicht vorhanden (0 Byte)
- Versionsbit entspricht 1_b: das Feld Schlüssel-Version ist vorhanden (1 Byte) (siehe 7.7.1)

Bit 7: Reserviert mit Wert gleich 0_b

Siehe 9.4.5 für Einzelheiten über diesen Sicherheitsmodus.

7.7.6 Konfigurationsfeld des Sicherheitsmodus 8

Tabelle 35 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 8.

Tabelle 35 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 8

Feld-name	Konfig. Feld (siehe Tabelle 36)	Konfig. felderweiterung (optional) (siehe Tabelle 37)	Schlüsselversion	Länge[E] (optional)	Nachrichtenzähler	Verschlüsselte Anwendungsdaten	Nicht verschlüsselte Anwendungsdaten (optional)	Authentifizierungs-Tag 1	Übertragungszeitstempel (optional)	Authentifizierungs-Tag 2 (optional)
Länge	2	(1)	(1)	(1)	2/3/4	Länge (E)	...	4	(3)	(2)

Abweichend von der gängigen Übertragungsreihenfolge von Feldern mit mehreren Bytes müssen das Authentifizierungs-Tag 1 und das Authentifizierungs-Tag 2 mit dem MSB an erster Stelle übertragen werden.

ANMERKUNG 1 Das Authentifizierungs-Tag 1 (MAC_1) und 2 (MAC_2) und der Übertragungszeitstempel befinden sich am Ende der Nachricht. Wenn der Übertragungszeitstempel aktiviert ist, ist auch der Authentifizierungs-Tag 2 aktiviert, um das Feld des Übertragungszeitstempels zu authentifizieren.

ANMERKUNG 2 Alle optionalen Felder des TPL-Headers und des TPL-Trailers werden unverschlüsselt übertragen.

Tabelle 36 — Definition des Konfigurationsfelds für Modus 8

MS Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	LS Bit 0
CFE	KDF-Auswahl	KDF-Auswahl	Modus	Modus	Modus	Modus	Modus	Len E Bit	Authentifizierungs-Tag2 und Übertragungszeitstempel	Zählergröße	Zählergröße	Schlüssel-ID	Schlüssel-ID	Schlüssel-ID	Schlüssel-ID
X	D	D	M	M	M	M	M	E	O	Z	Z	K	K	K	K

Bit 0 bis Bit 3: Schlüssel-ID "KKKK"

— Schlüssel-ID, wie in Tabelle 24 spezifiziert (siehe 7.7.1)

Bit 4 bis Bit 5: Zählergröße "ZZ"

- Zählergrößenbits entsprechen 00_b : reserviert
- Zählergrößenbits entsprechen 01_b : Das nachfolgende Zählerfeld ist 2 Bytes groß
- Zählergrößenbits entsprechen 10_b : Das nachfolgende Zählerfeld ist 3 Bytes groß
- Zählergrößenbits entsprechen 11_b : Das nachfolgende Zählerfeld ist 4 Bytes groß

Bit 6: Authentifizierungs-Tag2 und Übertragungszeitstempel "0"

- Bit Authentifizierungs-Tag2 und Übertragungszeitstempel entsprechen 0_b :
Das Authentifizierungs-Tag 2 und der Übertragungszeitstempel sind nicht vorhanden (0 Byte)
- Bit Authentifizierungs-Tag2 und Übertragungszeitstempel entsprechen 1_b :
Das Authentifizierungs-Tag 2 ist vorhanden (2 Bytes) und der Übertragungszeitstempel ist vorhanden (3 Bytes)

Bit 7: Len E Bit "E"

- Len E Bit entspricht 0_b : das Feld Länge[E] ist nicht vorhanden (0 Byte)
(Es sind keine unverschlüsselten Anwendungsdaten nach den verschlüsselten Anwendungsdaten vorhanden.)
- Len E Bit entspricht 1_b : das Feld Länge[E] ist vorhanden (1 Byte)
(Das Feld Länge[E] ist als vorzeichenloser Integer kodiert. Dies ermöglicht eine maximale Länge von 255 Bytes an verschlüsselten Anwendungsdaten.)

Bit 8 bis Bit 12: Sicherheitsmodus "MMMMM"

- Für die Spezifikation der Sicherheitsmodi (siehe Tabelle 19)
- Modus 8 wird angegeben durch MMMMM = 01000_b

Bit 13 bis Bit 14: KDF-Auswahl "DD"

- Selektor für die Schlüsselabweichungsfunktion, wie in Tabelle 25 spezifiziert (siehe 7.7.1)

Bit 15: CFE 'X'

- CFE-Bit 0 Die Konfigurationsfelderweiterung ist nicht vorhanden (0 Byte)
- CFE-Bit 1 Die Konfigurationsfelderweiterung ist vorhanden (1 Byte); siehe Tabelle 35