

DIN EN 13757-7

ICS 33.200; 35.100.10; 35.100.20

Mit DIN EN 13757-3:2018-06
Ersatz für
DIN EN 13757-3:2013-08**Kommunikationssysteme für Zähler –
Teil 7: Transport- und Sicherheitsdienste;
Deutsche Fassung EN 13757-7:2018**Communication systems for meters –
Part 7: Transport and security services;
German version EN 13757-7:2018Systèmes de communication pour compteurs –
Partie 7: Services de transport et de sécurité;
Version allemande EN 13757-7:2018

Gesamtumfang 99 Seiten

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

Nationales Vorwort

Dieses Dokument (EN 13757-7:2018) wurde vom Technischen Komitee CEN/TC 294 „Kommunikationssysteme für Zähler“ erarbeitet, dessen Sekretariat von 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.

Änderungen

Gegenüber DIN EN 13757-3:2013-08 wurden folgende Änderungen vorgenommen:

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

Frühere Ausgaben

DIN EN 13757-3: 2005-02, 2013-08

Deutsche Fassung

Kommunikationssysteme für Zähler — Teil 7: Transport- und Sicherheitsdienste

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

Systèmes de communication pour compteurs —
Partie 7: Services de transport et de sécurité

Diese Europäische Norm wurde vom CEN am 8. Februar 2018 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

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

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

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

Inhalt

	Seite
Europäisches Vorwort.....	5
Einleitung	7
1 Anwendungsbereich.....	9
2 Normative Verweisungen	9
3 Begriffe	10
4 Abkürzungen und Symbole	12
4.1 Abkürzungen	12
4.2 Symbole	14
5 Schichtmodell	14
5.1 M-Bus-Schichten	14
5.2 Das CI-Feld-Prinzip	15
6 Authentifizierungs- und Fragmentierungs-Teilschicht (AFL)	20
6.1 Einleitung.....	20
6.2 Übersicht über die AFL-Struktur.....	21
6.3 Komponenten der AFL.....	21
6.3.1 AFL-Längenfeld (AFL.AFLL)	21
6.3.2 AFL-Fragmentierungskontrollfeld (AFL.FCL)	21
6.3.3 AFL-Nachrichtenkontrollfeld (AFL.MCL)	22
6.3.4 AFL-Schlüsselinformationsfeld (AFL.KI)	23
6.3.5 AFL-Nachrichtenzählerfeld (AFL.MCR)	23
6.3.6 AFL-MAC-Feld (AFL.MAC)	24
6.3.7 AFL-Nachrichtenlängenfeld (AFL.ML)	24
7 Transportschicht (TPL)	24
7.1 Einleitung.....	24
7.2 Struktur ohne TPL-Header.....	25
7.3 Struktur mit kurzem TPL-Header	25
7.4 Struktur mit langem TPL-Header	25
7.5 CI-Feld-abhängige Elemente.....	26
7.5.1 Identifikationsnummer	26
7.5.2 Identifikation des Herstellers	26
7.5.3 Versionsidentifikation.....	27
7.5.4 Identifikation des Gerätetyps.....	27
7.5.5 Zugriffsnummer.....	29
7.5.6 Statusbyte in Zählernachrichten	30
7.5.7 Statusbyte in Partnernachrichten	31
7.5.8 Konfigurationsfeld.....	32
7.6 Konfigurationsfeldabhängige Struktur	34
7.6.1 Allgemeines.....	34
7.6.2 Konfigurationsfelderweiterung	34
7.6.3 Optionale TPL-Header-Felder	34
7.6.4 Optionale TPL-Trailer-Felder.....	34
7.6.5 Teilverschlüsselung.....	35
7.7 Sicherheitsmodusspezifische TPL-Felder	35
7.7.1 Gemeinsame Teilfelder des Konfigurationsfelds und der Konfigurationsfelderweiterung.....	35

7.7.2	Konfigurationsfeld des Sicherheitsmodus 0.....	38
7.7.3	Konfigurationsfeld der Sicherheitsmodi 2 und 3.....	39
7.7.4	Konfigurationsfeld des Sicherheitsmodus 5.....	40
7.7.5	Konfigurationsfeld des Sicherheitsmodus 7.....	42
7.7.6	Konfigurationsfeld des Sicherheitsmodus 8.....	43
7.7.7	Konfigurationsfeld des Sicherheitsmodus 9.....	46
7.7.8	Konfigurationsfeld des Sicherheitsmodus 10	48
8	Verwaltung der unteren Schichten.....	50
8.1	Allgemeines	50
8.2	Setzen der Baudrate für die M-Bus-Verbindungsschicht nach EN 13757-2	50
8.3	Adressstruktur bei Verwendung zusammen mit der drahtlosen Datenverbindungsschicht nach EN 13757-4	50
8.4	Selektion und Sekundäradressierung	50
8.5	Generalisiertes Selektionsverfahren	52
8.6	Suche nach installierten Slaves.....	52
8.6.1	Primäradressen	52
8.6.2	Sekundäradressen	53
8.6.3	Verfahren der Platzhaltersuche	53
9	Sicherheitsdienste.....	53
9.1	Allgemeines	53
9.2	Nachrichtenzähler.....	55
9.2.1	Überblick.....	55
9.2.2	Nachrichtenzähler C_M , der vom Zähler übertragen wird	55
9.2.3	Nachrichtenzähler C_{CP} , der vom Kommunikationspartner übertragen wird.....	56
9.2.4	Nachrichtenzähler C'_{CP} , der vom Zähler erhalten wird	56
9.2.5	Nachrichtenzähler C'_M und C''_M , die vom Kommunikationspartner empfangen werden	57
9.3	Authentifizierungsverfahren in der AFL.....	57
9.3.1	Überblick.....	57
9.3.2	Authentifizierungsverfahren AES-CMAC-128.....	58
9.3.3	Authentifizierungsverfahren AES-GMAC-128	58
9.4	Verschlüsselungs- und Authentifizierungsverfahren in der TPL	59
9.4.1	Überblick über TPL-Schutzmechanismen	59
9.4.2	Herstellerspezifischer Schutzmechanismus (Sicherheitsmodus 1)	61
9.4.3	Schutzmechanismus DES-CBC (Sicherheitsmodus 2 und 3)	61
9.4.4	Schutzmechanismus AES-CBC-128 (Sicherheitsmodus 5)	62
9.4.5	Schutzmechanismus AES-CBC-128 (Sicherheitsmodus 7)	63
9.4.6	Schutzmechanismus AES-CTR-128 (Sicherheitsmodus 8)	64
9.4.7	Schutzmechanismus AES-GCM-128 (Sicherheitsmodus 9)	66
9.4.8	Schutzmechanismus AES-CCM-128 (Sicherheitsmodus 10)	69
9.5	Reaktion auf ein Sicherheitsversagen	71
9.6	Schlüsselableitung	72
9.6.1	Allgemeines	72
9.6.2	Schlüsselableitungsfunktion A.....	72
9.7	Schlüsselaustausch	73
Anhang A (normativ)	Übertragungsprotokoll für Sicherheitsinformationen.....	74
A.1	Einleitung.....	74
A.2	SITP-Dienste.....	74
A.2.1	Sicherheitsinformationen übertragen	74
A.2.2	Sicherheitsinformationen aktivieren	75
A.2.3	Sicherheitsinformationen deaktivieren	75
A.2.4	Sicherheitsinformationen zerstören.....	75
A.2.5	Kombinierte Aktivierung/Deaktivierung von Sicherheitsinformationen.....	75
A.2.6	Sicherheitsinformationen erzeugen	75

A.2.7	Sicherheitsinformationen erhalten.....	75
A.2.8	Liste aller Schlüsselinformation erhalten.....	75
A.2.9	Liste der aktiven Schlüsselinformation erhalten	75
A.2.10	Von Ende zu Ende gesicherte Anwendungsdaten übertragen.....	76
A.3	CI-Felder.....	76
A.4	SITP-Struktur.....	76
A.5	Blockkontrollfeld	77
A.6	Blockparameter	77
A.7	Überblick über Datenstrukturen/Mechanismen.....	78
A.8	Datenstrukturen für Sicherheitsinformationen	80
A.8.1	Allgemeines.....	80
A.8.2	Datenstruktur 00 _h	80
A.8.3	Datenstruktur 01 _h	80
A.8.4	Datenstruktur 02 _h	81
A.8.5	Datenstruktur 03 _h	81
A.8.6	Datenstruktur 20 _h	82
A.8.7	Datenstruktur 21 _h	83
A.8.8	Datenstruktur 22 _h	84
A.9	Datenstrukturen für gesicherte Anwendungsdaten.....	85
A.9.1	Allgemeines.....	85
A.9.2	Datenstruktur 30 _h – AES-Schlüssel-Wrap.....	86
A.9.3	Datenstruktur 31 _h – HMAC-SHA256	87
A.9.4	Datenstruktur 32 _h und 33 _h – CMAC.....	88
A.9.5	Datenstruktur 34 _h – AES-GCM	89
A.9.6	Datenstruktur 35 _h – AES-GMAC.....	90
A.9.7	Datenstruktur 36 _h und 37 _h – AES-CCM	91
	Anhang B (informativ) Beispiel eines Nachrichtenzählers.....	93
	Literaturhinweise.....	97

Europäisches Vorwort

Dieses Dokument (EN 13757-7:2018) wurde vom Technischen Komitee CEN/TC 294 „Kommunikationssysteme für Zähler“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Oktober 2018, und etwaige entgegenstehende nationale Normen müssen bis Oktober 2018 zurückgezogen werden.

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

Dieses Dokument ersetzt zusammen mit EN 13757-3:2018 und CEN/TR 17167:2018 EN 13757-3:2013.

Dieses Dokument wurde unter einem Normungsauftrag erarbeitet, den die Europäische Kommission und die Europäische Freihandelszone dem CEN erteilt haben.

Die folgenden wesentlichen technischen Änderungen wurden in dieser neuen Fassung der 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 derzeit aus folgenden Teilen:

- *Kommunikationssysteme für Zähler — Teil 1: Datenaustausch;*
- *Kommunikationssysteme für Zähler — Teil 2: Drahtgebundene M-Bus-Kommunikation;*
- *Kommunikationssysteme für Zähler — Teil 3: Anwendungsprotokolle;*
- *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;*
- *CEN/TR 17167:2018, Kommunikationssysteme für Zähler — Begleitender Technischer Bericht zu EN 13757-2, -3 und -7, Beispiele und ergänzende Informationen.*

Das vorliegende Dokument fällt unter den Normungsauftrag EU M/441 „Normungsauftrag an CEN, CENELEC und ETSI auf dem Gebiet der Messgeräte mit dem Ziel der Entwicklung einer offenen Architektur für Verbrauchszähler unter Einbeziehung von Interoperabilität ermöglichenden Kommunikationsprotokollen“, da es relevante Definitionen und Verfahren für die Zählerdatenübertragung auf Ebene der Anwendungsschicht bereitstellt. Der M/441-Normungsauftrag fördert die signifikante Entwicklung von Normen im Bereich intelligenter Messsysteme.

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

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Diese Europäische Norm gehört zur Normenreihe EN 13757, die Kommunikationssysteme für Zähler 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 Funk 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). EN 13757-7 beschreibt den Transportmechanismus und die Sicherheitsverfahren für Daten. Der Technische Bericht CEN/TR 17167 enthält informative Anhänge von EN 13757-2, EN 13757-3 und EN 13757-7.

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 (Funk) sowie EN 13757-5 (Funk 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 eine längere Batterielebensdauer der Zähler sicherzustellen, insbesondere im Fall einer drahtlosen Kommunikation. Zweitens wurden sie für eine minimale Nachrichtenlänge 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 zudem 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 sein können. Diese weiteren Kommunikationssysteme können dieselben oder andere Anwendungsschichtprotokolle, Sicherheits-, Datenschutz-, Authentifizierungs- und Managementverfahren verwenden.

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

ANMERKUNG 1 CEN/TR 17167:2018, Anhang C, legt fest, wie Teile dieser Norm und der Normen EN 13757-2 und EN 13757-4 zur Implementierung von Funktionalitäten intelligenter Zähler verwendet werden können. Ähnliche Funktionalitäten können auch mithilfe anderer Bitübertragungsschichten und Verbindungsschichten implementiert werden.

ANMERKUNG 2 Für weitere Informationen zu Installationsverfahren und deren Integration in Zählerverwaltungssysteme siehe CEN/TR 17167:2018, Anhang D.

Der Bediener eines Smart-Metering-Netzwerks muss das Netzwerk sichern, um den Datenschutz und die Privatsphäre der Daten des Konsumenten sicherzustellen (siehe EG-Empfehlung C1342 (2012)). Die Absicherung eines Systems erfordert eine Sicherheitsrichtlinie, die im Allgemeinen alle Funktionseinschränkungen, den Informationsfluss zwischen Funktionen, den Zugriff durch externe Systeme

und Bedrohungen organisatorisch behandeln sollte, einschließlich Software und den Zugriff auf Daten durch Dritte.

Die Sicherheitsrichtlinie unterliegt der Verantwortung von Organisationen entsprechend ihrer Geschäftsprozesse. Die Hauptelemente einer Sicherheitsrichtlinie bestimmen in Kombination mit Regeln die allgemeine Sicherheit, die erreicht wird. Die Sicherheitsrichtlinie definiert Ziele und Elemente des Systems, die durch organisatorische Richtlinien und technische Implementierungen der Sicherheitsdienste unterstützt werden sollen. Das Einrichten und Ausführen von Sicherheitsrichtlinien liegt außerhalb des Anwendungsbereiches dieser Norm, welche jedoch Sicherheitsdienste bietet, die diese Richtlinien unterstützen, wenn sie implementiert werden.

Ein Sicherheitskonzept bezieht sich hauptsächlich auf ein *architektonisches* Modell, das Datenflüsse zwischen rollenbasierten Datenverarbeitungsfunktionen darstellt. Anforderungen an 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

Diese vorliegende Europäische Norm legt die Transport- und Sicherheitsdienste für Kommunikationssysteme für Zähler fest.

Diese vorliegende Europäische Norm legt sichere Kommunikationsfähigkeiten nach Design fest und unterstützt den Aufbau einer sicheren Systemarchitektur.

Diese vorliegende Europäische Norm gilt für den Schutz der Verbraucherdaten zur Sicherung der Privatsphäre.

Es ist vorgesehen, dass diese Europäische Norm 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 wird.

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 — Teil 2: Drahtgebundene M-Bus-Kommunikation*

EN 13757-3:2018, *Kommunikationssysteme für Zähler — Teil 3: Anwendungsprotokolle*

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*

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

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 Anwendungsdaten
vom Messprozess verwendete und/oder erzeugte Daten wie Registerwerte, Tarife und Umrechnungsfaktoren oder zur Kontrolle des Messprozesses beziehungsweise der Ausgabe oder für zusätzlicher Informationen verwendete Daten

3.2 Anwendungsprotokoll
Protokoll für die Kodierung der Anwendungsdaten

Anmerkung 1 zum Begriff: Anwendungsprotokolle werden in EN 13757-3 festgelegt.

3.3 Authentifizierung
Eigenschaft, dass Daten von ihrer angeblichen Quelle stammen

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

3.4 Byte
Oktett von Bits

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

[QUELLE: ISO 7498-2:1989]

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

[QUELLE: ISO 7498-2:1989]

3.7 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.

3.8 flüchtiger Schlüssel
Schlüssel zum Verschlüsseln oder Entschlüsseln einer einzigen Nachricht für eine begrenzte Zeit oder eine begrenzte Datenmenge

3.9 Fragment
Datagramm einer fragmentierten Nachricht

3.10

Hex-ASCII

als ASCII-Zeichen verschlüsselte Zahlen mit Basis 16 („0“bis„9“, „A“bis„F“)

[QUELLE: ANSI X9 TR-31:2010]

3.11

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

3.12

Schlüsselzähler

im Übertragungsprotokoll für Sicherheitsinformationen verwendeter eindeutiger Zähler zur Identifizierung gesicherter von Ende zu Ende übertragener Befehle und Antworten

3.13

Schlüsselableitung

Methode, mit der eine (potentiell 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

3.14

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.

3.15

Nachrichtenzähler

in der AFL oder TPL verwendeter eindeutiger Zähler zur Identifizierung einer gesicherten Nachricht

3.16

persistenter Schlüssel

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

3.17

Schutzmechanismus

Betriebsmodus eines (symmetrischen) kryptographischen Algorithmus

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

3.18

Sicherheitsmodus

Modusnummer im Konfigurationsfeld, die einen Satz angewandter Sicherheitsmechanismen identifiziert

3.19

Sicherheitsdienst

Authentifizierung, Vertraulichkeit und Datenintegrität

Anmerkung 1 zum Begriff: Sicherheitsdienste werden von Schutzmechanismen bereitgestellt.

3.20

Teilschicht

Untergliederung einer Schicht

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

3.21

TPL-Füllung

in der TPL hinzugefügte Füllbytes zur Auffüllung von Anwendungsdaten auf die angeforderte Größe für eine Blockchiffrierung

3.22

Wrapper-Schlüssel

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

3.23

Wrapping-Mechanismus

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

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
BCF	Block control field of SITP structure, coding the usage of command or response	Blockkontrollfeld der SITP-Struktur, Kodierung der Nutzung von Befehl bzw. Antwort
BID	Block identification number of SITP structure	Blockidentifikationsnummer der SITP-Struktur
BL	Block length of SITP structure	Blocklänge der SITP-Struktur
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	Chiffre-basierter MAC [NIST/SP 800-38B]
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
DLL	Data Link Layer	Datenverbindungsschicht
DLMS	Device Language Message Specification	Device Language Message Specification
DSI	Data structure identifier, part of block parameter structure inside SITP	Datenstrukturidentifikator, Teil der Blockparameterstruktur innerhalb des SITP
DSH	Data structure header, part of block parameter structure inside SITP	Header der Datenstruktur, Teil der Blockparameterstruktur innerhalb des SITP
DSH1	Byte one of DSH	Byte eins des DSH
DSH2	Byte two of DSH	Byte zwei des DSH
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
ICV	Integrity check value, part of a wrapped data structure in SITP	Integritätsüberprüfungswert, Teil einer Wrapped-Datenstruktur im SITP
IV	Initialisation Vector	Initialisierungsvektor
LSB	Least significant byte	Niedrigstwertiges Byte
LSBit	Least significant bit	Niedrigstwertiges Bit
MAC	Message Authentication Code	Nachrichtenauthentifizierungscode
ANMERKUNG MAC ist in anderen Normen auch das Akronym für Steuerung für Medienzugriff (en: Media Access Control) für die Datenkommunikation an der physischen Schicht.		
MK	Message Key (persistent)	Nachrichtenschlüssel (persistent)
MLI	Message Length Indicator, part of a wrapped data structure in SITP	Nachrichtenlängenidentifikator, Teil einer Wrapped-Datenstruktur im SITP
MSB	Most significant byte	Höchstwertiges Byte
MSBit	Most significant bit	Höchstwertiges Bit
NWL	Network Layer	Netzwerkschicht
OBIS	Object Identification System	Object Identification System

		(EN 62056-61)
PID	Protocol identifier field, part of wrapped data structure in SITP	Protokollidentifikatorfeld, Teil einer Wrapped-Datenstruktur im SITP
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	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
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]
SND-UD2	Send User Data 2	Nutzerdaten senden 2 [EN 13757-2/EN 13757-4]
SND-UD3	Send User Data 3 [EN 13757-4]	Nutzerdaten senden 3 [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. 12_h || 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 Funk M-Bus ab [EN 13757-4 und EN 13757-5]).

Das Vorhandensein der anderen Schichten hängt von Folgendem ab:

- Kommunikationsmedium (drahtgebundener/Funk 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 festgelegt.

Tabelle 1 — Reihenfolge der M-Bus-Schicht

Abkürzung	Schicht	Angegeben durch CI-Feld	Entsprechender Teil dieser Normenreihe	Farb-codes ^b	OSI-Model Schicht
APL	Anwendungsschicht	a	EN 13757-1/ EN 13757-3/ EN 13757	Orange	Anwendung Präsentation
TPL (en: Transport Layer)	Transportschicht	Ja	EN 13757-7/ EN 13757	Grün	Sitzung Transport
AFL (en: Authentication and Fragmentation Sublayer)	Authentifizierungs- und Fragmentierungs-Teilschicht	Ja	EN 13757-7	Lila	
NWL (en: Network Layer)	Netzwerkschicht	Ja	EN 13757-5	Pink	Netzwerk
ELL (en: Extended Link Layer)	Erweiterte Verbindungsschicht	Ja	EN 13757-4	Blau	Datenverbindung
DLL (en: Data Link Layer)	Datenverbindungsschicht	Nein	EN 13757-2/ EN 13757/ EN 13757-5	Hellblau	
PHY (en: Physical Layer)	Bitübertragungsschicht	Nein	EN 13757-2/ EN 13757/ EN 13757-5/ EN 13757	Hellgelb	Physikalisch
^a Die APL wird nicht von einem zugeordneten CI-Feld eingeführt, sondern vom CI-Feld der TPL angegeben. ^b Diese Farbcodes werden in Beispiele aus CEN/TR 17167 angewandt.					

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 und 5 wird von den M-Bus-Schichten AFL und TPL dargestellt. Die Funktionalität der OSI-Schichten 6 und 7 wird von den M-Bus-Schichten APL dargestellt.

5.2 Das CI-Feld-Prinzip

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

Die Schichten ELL und NWL geben keine bestimmte Längeninformation an. Daher muss die Struktur dieser Schichten vom CI-Feld abgeleitet werden. Siehe EN 13757-4 oder EN 13757-5 für die Spezifikation der Länge der entsprechenden Schichten und der Startposition der nächsten Schicht.

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.

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

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
00 _h bis 1F _h	Reserviert für DLMS-basierte Anwendungen	APL	keine	DLMS (siehe EN 13757-1)
20 _h bis 4F _h	Reserviert			
50 _h	Anwendungsrücksetzung oder -auswahl an Gerät	APL	keine	Anwendungsauswahl; nach EN 13757-3:2018, Abschnitt 7
51 _h	Befehl an Gerät (voller M-Bus-Datenrahmen)	APL	keine	M-Bus (nicht für drahtlos); nach EN 13757-3:2018, Abschnitt 6
52 _h	Auswahl des Geräts		keine	Management, siehe 8.4
53 _h	Anwendungsrücksetzung oder -auswahl an Gerät	APL	Lang	Anwendungsauswahl; nach EN 13757-3:2018, Abschnitt 7
54 _h	Anfrage der ausgewählten Anwendung an das Gerät	APL	keine	Anwendungsauswahl; nach EN 13757-3:2018, Abschnitt 7
55 _h	Anfrage der ausgewählten Anwendung an das Gerät	APL	Lang	Anwendungsauswahl; nach EN 13757-3:2018, Abschnitt 7
56 _h bis 59 _h	Reserviert			
5A _h	Befehl an Gerät (voller M-Bus-Datenrahmen)	APL	Kurz	M-Bus; nach EN 13757-3:2018, Abschnitt 6
5B _h	Befehl an Gerät (voller M-Bus-Datenrahmen)	APL	Lang	M-Bus; nach EN 13757-3:2018, Abschnitt 6
5C _h	Aktion synchronisieren	APL	keine	nach EN 13757-3:2018, Abschnitt 12
5D _h bis 5E _h	Reserviert			
5F _h	Spezifische Nutzung ^b	TPL	Lang	ANMERKUNG Siehe Literaturhinweis [8].
60 _h	Befehl an Gerät	APL	Lang	DLMS/COSEM mit OBIS-Identifikator (nach EN 13757-1 und EN 62056-5-3) ^a
61 _h	Befehl an Gerät	APL	Kurz	DLMS/COSEM mit OBIS-Identifikator (nach EN 13757-1 und

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
				EN 62056-5-3) ^a
62 _h bis 63 _h	Reserviert			
64 _h	Befehl an Gerät	APL	Lang	Reserviert für Beschreiber von Werten des Typs OBIS ^a
65 _h	Befehl an Gerät	APL	Kurz	Reserviert für Beschreiber von Werten des Typs OBIS ^a
66 _h	Antwort bezüglich der ausgewählten Anwendung vom Gerät	APL	keine	Anwendungsauswahl; nach EN 13757-3:2018, Abschnitt 7
67 _h	Antwort bezüglich der ausgewählten Anwendung vom Gerät	APL	Kurz	Anwendungsauswahl; nach EN 13757-3:2018, Abschnitt 7
68 _h	Antwort bezüglich der ausgewählten Anwendung vom Gerät	APL	Lang	Anwendungsauswahl; nach EN 13757-3:2018, Abschnitt 7
69 _h	Antwort vom Gerät (M-Bus-Formatrahmen)	APL	keine	M-Bus; nach EN 13757-3:2018, 6, Anhang G
6A _h	Antwort vom Gerät (M-Bus-Formatrahmen)	APL	Kurz	M-Bus; nach EN 13757-3:2018, Anhang G
6B _h	Antwort vom Gerät (M-Bus-Formatrahmen)	APL	Lang	M-Bus; nach EN 13757-3:2018, Anhang G
6C _h	Zeitsynchronisierung zum Gerät	APL	Lang	nach EN 13757-3:2018, Abschnitt 8
6D _h	Zeitsynchronisierung zum Gerät	APL	Lang	nach EN 13757-3:2018, Abschnitt 8
6E _h	Anwendungsfehler vom Gerät	APL	Kurz	nach EN 13757-3:2018, Abschnitt 10
6F _h	Anwendungsfehler vom Gerät	APL	Lang	nach EN 13757-3:2018, Abschnitt 10
70 _h	Anwendungsfehler vom Gerät	APL	keine	nach EN 13757-3:2018, Abschnitt 10
71 _h	Alarm vom Gerät	APL	keine	nach EN 13757-3:2018, Abschnitt 9
72 _h	Antwort vom Gerät (voller M-Bus-Datenrahmen)	APL	Lang	M-Bus; nach EN 13757-3:2018, Abschnitt 6
73 _h	Antwort vom Gerät (M-Bus-Kompaktrahmen)	APL	Lang	M-Bus; nach EN 13757-3:2018, Abschnitt 6, Anhang G
74 _h	Alarm vom Gerät	APL	Kurz	nach EN 13757-3:2018, Abschnitt 9
75 _h	Alarm vom Gerät	APL	Lang	nach EN 13757-3:2018, Abschnitt 9
76 _h bis 77 _h	Reserviert			
78 _h	Antwort vom Gerät (voller M-Bus-Datenrahmen)	APL	keine	M-Bus; nach EN 13757-3:2018, Abschnitt 6
79 _h	Antwort vom Gerät (M-Bus-Kompaktrahmen)	APL	keine	M-Bus; nach EN 13757-3:2018, Abschnitt 6, Anhang G

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
7A _h	Antwort vom Gerät (voller M-Bus-Datenrahmen)	APL	Kurz	M-Bus; nach EN 13757-3:2018, Abschnitt 6
7B _h	Antwort vom Gerät (M-Bus-Kompaktrahmen)	APL	Kurz	M-Bus; nach EN 13757-3:2018, Anhang G und EN 13757-3:2018, Abschnitt 6
7C _h	Antwort vom Gerät	APL	Lang	DLMS/COSEM mit OBIS-Identifikator (nach EN 13757-1 und EN 62056-5-3) ^a
7D _h	Antwort vom Gerät	APL	Kurz	DLMS/COSEM mit OBIS-Identifikator (nach EN 13757-1 und EN 62056-5-3) ^a
7E _h	Antwort vom Gerät	APL	Lang	Reserviert für Beschreiber von Werten des Typs OBIS ^a
7F _h	Antwort vom Gerät	APL	Kurz	Reserviert für Beschreiber von Werten des Typs OBIS ^a
80 _h	Transportschicht zum Gerät (ohne APL)	TPL	Lang	Nach EN 13757-4
81 _h	Netzwerkschichtdaten	NWL		Nach EN 13757-5
82 _h	Netzwerkmanagementdaten zum Gerät	APL	Lang	Nach EN 13757-4 und EN 13757-5
83 _h	Netzwerkmanagementdaten zum Gerät	APL	keine	Nach EN 13757-4 und EN 13757-5
84 _h	Transportschicht zum Gerät (M-Bus-Kompaktrahmen erwartet)	TPL	Lang	Nach EN 13757-3:2018, Anhang G
85 _h	Transportschicht zum Gerät (M-Bus-Formatrahmen erwartet)	TPL	Lang	Nach EN 13757-3:2018, Anhang G
86 _h	Reserviert für erweiterte Verbindungsschicht	ELL		Nach EN 13757-4
87 _h	Netzwerkmanagementdaten vom Gerät	APL	Lang	Nach EN 13757-4, EN 13757-5
88 _h	Netzwerkmanagementdaten vom Gerät	APL	Kurz	Nach EN 13757-4, EN 13757-5
89 _h	Netzwerkmanagementdaten vom Gerät	APL	keine	Nach EN 13757-4, EN 13757-5
8A _h	Transportschicht vom Gerät (ohne APL)	TPL	Kurz	Nach EN 13757-4
8B _h	Transportschicht vom Gerät (ohne APL)	TPL	Lang	Nach EN 13757-4
8C _h bis 8F _h	Erweiterte Verbindungsschicht	ELL		Nach EN 13757-4

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
90 _h	Authentifizierungs- und Fragmentierungs-Teilschicht	AFL		Nach Abschnitt 6
91 _h	Reserviert			
92 _h bis 97 _h	Reserviert			Nach EN 13757-4, EN 13757-5
98 _h bis 9D _h	Reserviert			
9E _h	Spezifische Nutzung ^b	TPL	Kurz	ANMERKUNG Siehe Literaturhinweis [8].
9F _h	Spezifische Nutzung ^b	TPL	Lang	ANMERKUNG Siehe Literaturhinweis [8].
A0 _h bis B7 _h	Herstellerspezifisch	APL		Nach EN 13757-3:2018, 13
B8 _h	Baudrate auf 300 Baud setzen	APL	keine	Management der unteren Schichten; nach 8.2
B9 _h	Baudrate auf 600 Baud setzen	APL	keine	Management der unteren Schichten; nach 8.2
BA _h	Baudrate auf 1 200 Baud setzen	APL	keine	Management der unteren Schichten; nach 8.2
BB _h	Baudrate auf 2 400 Baud setzen	APL	keine	Management der unteren Schichten; nach 8.2
BC _h	Baudrate auf 4 800 Baud setzen	APL	keine	Management der unteren Schichten; nach 8.2
BD _h	Baudrate auf 9 600 Baud setzen	APL	keine	Management der unteren Schichten; nach 8.2
BE _h	Baudrate auf 19 200 Baud setzen	APL	keine	Management der unteren Schichten; nach 8.2
BF _h	Baudrate auf 38 400 Baud setzen	APL	keine	Management der unteren Schichten; nach 8.2
C0 _h	Befehl an Gerät	APL	Lang	Image-Übertragung; nach EN 13757-3:2018, Anhang I
C1 _h	Antwort vom Gerät	APL	Kurz	Image-Übertragung; nach EN 13757-3:2018, Anhang I
C2 _h	Antwort vom Gerät	APL	Lang	Image-Übertragung; nach EN 13757-3:2018, Anhang I
C3 _h	Befehl an Gerät	APL	Lang	Sicherheitsinformationenübertragung; nach Anhang A
C4 _h	Antwort vom Gerät	APL	Kurz	Sicherheitsinformationenübertragung; nach Anhang A
C5 _h	Antwort vom Gerät	APL	Lang	Sicherheitsinformationenübertragung; nach Anhang A
C6 _h bis FF _h	Reserviert			

CI-Feld	Richtung	Schicht	TPL-Header	Protokoll der höheren Schicht
ANMERKUNG Alle SND-DU-Datagramme werden in der Daten Verbindungsschicht zu quittiert, 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. EN 13757-3:2018, Anhang H ist zu verwenden, um die OBIS-Kennungen aus den M-Bus-Daten zu generieren.			
b	Für spezifische nationale Implementierungen verwendet. Siehe Referenz in den Literaturhinweisen zur Verwendung dieses CI-Felds zum Zeitpunkt der Veröffentlichung dieser Norm.			

6 Authentifizierungs- und Fragmentierungs-Teilschicht (AFL)

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 je Fragment und einen Abschnitt für die gesamte Nachricht unterteilt. Die Position der AFL im M-Bus-Schichtmodell ist in Tabelle 1 dargestellt.

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 Protokoll dateneinheiten ein);
- Authentifizierung der Gesamtnachricht durch einen MAC (dies kombiniert den Fragmenttransport mit der Authentifizierung einer Anwendungsprotokoll dateneinheit).

Der MAC-Dienst (siehe 9.3) 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 sicherzustellen, 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 Datenverbindungsschichtdatagramm transportiert werden. Die schattierten Felder von 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	Schlüsselinformationsfeld ^a
4	MCR	Nachrichtenzählerfeld ^a
N ^b	MAC	Nachrichtenauthentifizierungscode ^a
2	ML	Nachrichtenlängenfeld ^a
^a Dies ist ein optionales Feld. Ihre Aufnahme wird durch das Fragmentierungskontrollfeld definiert, das in 6.3.2 festgelegt wird. ^b Die Länge des MAC hängt vom AT-Teilfeld in AFL.MCL ab.		

Alle AFL-Felder mit mehreren Bytes außer 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.AFL)

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

Das AFL.AFL-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 ^a

Bit	Feldname	Beschreibung
12	MLP	In diesem Fragment ist eine Nachrichtenlänge vorhanden ^a
11	MCRP	In diesem Fragment ist ein Nachrichtenzähler vorhanden ^a
10	MACP	In diesem Fragment ist ein MAC vorhanden ^a
9	KIP	In diesem Fragment sind Schlüsselinformationen vorhanden ^a
8	RES	Reserviert (standardmäßig 0 _b)
7 bis 0	FID	Fragment-ID
^a 0 = Feld ist nicht vorhanden; 1 = Feld ist vorhanden		

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 ^a
5	MCMP	In dieser Nachricht ist ein Nachrichtenzähler vorhanden ^a
4	KIMP	In dieser Nachricht sind Schlüsselinformationen vorhanden ^a
3	AT	Authentifizierungstyp (siehe Tabelle 6)
2		
1		
0		
^a 0 = Feld ist nicht vorhanden; 1 = Feld ist vorhanden		

Die Bits 4 bis 7 im AFL.MCL-Feld definieren das Vorhandensein von zusätzlichen Feldern in der Nachricht.

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 Authentifizierungscodes
0	Keine Authentifizierung	
1 bis 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 bis 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-Schlüsselinformationfeld (AFL.KI)

Das Schlüsselinformationfeld (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 festgelegt.
7 bis 6	RES	Reserviert (standardmäßig 0 _b)
5 bis 4	KDF-Auswahl	Die KDF-Auswahl identifiziert die angewandte Schlüsselableitungsfunktion, wie in Tabelle 25 festgelegt.
3 bis 0	Schlüssel-ID	Die Schlüssel-ID identifiziert den angewandten Schlüssel, wie in Tabelle 24 festgelegt.

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.

Wenn kein AFL.MCR vorliegt, müssen die Werte des Nachrichtenzählerfelds in der TPL für den AFL.MCR verwendet werden.

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 vorhanden sein im Fall einer

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

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-Header 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 TPL-Headers ist die Zähleradresse in diesem Header enthalten. Diese Zähleradresse darf sich von der vom Hersteller zugewiesene eindeutige Verbindungsschichtadresse unterscheiden. 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 TPL-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 7.5.8, Tabelle 19) 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	
Zugriffs-nr.	Status	Konfigurationsfeld (CF)	Konfigurationsfelderweiterung (CFE)	Optionale TPL-Header-Felder
1 Byte	1 Byte	2 Bytes	0 bis n Bytes	0 bis n Bytes

Der kurze TPL-Header 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

7.5.8, Tabelle 19) 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 (CF)	Konfigurationsfelderweiterung (CFE)	Opt. TPL-Header-Felder
4 Bytes	2 Bytes	1 Byte	1 Byte	1 Byte	1 Byte	2 Bytes	0 bis n Bytes	0 bis n Bytes

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 kann, besonders, wenn zusätzlich eine eindeutige und nicht änderbare Fabrikationsnummer (siehe auch 8.5) bereitgestellt wird.

Ein F_h 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. 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:

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

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

Ein FF_h ist als Platzhalter zu interpretieren. Ein Platzhalter kann jeden Wert von 00_h bis FE_h ersetzen. Eine Herstelleridentifikation $FFFF_h$ 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 FF_h ist als Platzhalter zu interpretieren. Ein Platzhalter kann durch einen Wert von 00_h bis FE_h 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	Hexadezimalcode
Sonstige	0000 0000	00
Ölzähler	0000 0001	01
Elektrizitätszähler	0000 0010	02
Gaszähler	0000 0011	03
Wärmeenergiezähler — Wärme (Volumen, das am Rücklauftemperaturausgang gemessen wird)	0000 0100	04
Dampfzähler	0000 0101	05
Warmwasserzähler (30 °C ... 90 °C) ^e	0000 0110	06
Wasserzähler ^e	0000 0111	07
Heizkostenverteiler	0000 1000	08
Druckluft	0000 1001	09
Wärmeenergiezähler — Kühlung (Volumen, das am Rücklauftemperaturausgang gemessen wird)	0000 1010	0A
Wärmeenergiezähler — Kühlung (Volumen gemessen bei Vorlauftemperatur: Vorlauf)	0000 1011	0B
Wärmeenergiezähler — Wärme (Volumen gemessen bei Vorlauftemperatur: Vorlauf)	0000 1100	0C
Wärmeenergiezähler — Wärme und Kühlung kombiniert	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 (≥ 90 °C) ^d	0001 0101	15
Kaltwasserzähler ^e	0001 0110	16

Gerätetyp (ehemals Medium)	Binärcode Bit 7...0	Hexadezimalcode
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 (en: environmental meter)		2B bis 2F
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	0011 1000	38
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 FF_h ist als Platzhalter zu interpretieren. Ein Platzhalter kann durch einen Wert von 00_h bis FE_h 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.