

## DIN EN 13757-7



ICS 33.200; 35.100.10; 35.100.20; 91.140.50

Einsprüche bis 2023-09-14  
Vorgesehen als Ersatz für  
DIN EN 13757-7:2018-06

**Entwurf**

**Kommunikationssysteme für Zähler –  
Teil 7: Transport- und Sicherheitsdienste;  
Deutsche und Englische Fassung prEN 13757-7:2023**

Communication systems for meters –  
Part 7: Transport and security services;  
German and English version prEN 13757-7:2023

Systèmes de communication pour compteurs –  
Partie 7: Services de transport et de sécurité;  
Version allemande et anglaise prEN 13757-7:2023

**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2023-07-14 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 von DIN unter [www.din.de/go/entwuerfe](http://www.din.de/go/entwuerfe) bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de), sofern dort wiedergegeben;
- oder als Datei per E-Mail an [nhrs@din.de](mailto:nhrs@din.de) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter [www.din.de/go/stellungnahmen-norm-entwuerfe](http://www.din.de/go/stellungnahmen-norm-entwuerfe) oder für Stellungnahmen zu Norm-Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Heiz- und Raumlufttechnik sowie deren Sicherheit (NHRS), 10772 Berlin oder Am DIN-Platz, 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 190 Seiten

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

## Nationales Vorwort

Dieses Dokument (prEN 13757-7:2023) wurde vom Technischen Komitee CEN/TC 294 „Kommunikationssysteme für Zähler“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium 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).

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

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN ([www.din.de](http://www.din.de)) durch eine Suche nach der Dokumentennummer aufgerufen werden.

## Änderungen

Gegenüber DIN EN 13757-7:2018-06 wurden folgende Änderungen vorgenommen:

- a) Unterstützung von Sensorgeräten und Alarmgeräten;
- b) Reduzierung der Gerätetypen für thermische Energiezähler;
- c) Unterstützung von MBAL gemäß der neuen EN 13757-8;
- d) Einführung der Inhaltsdefinition für das Unterfeld Inhaltsindex im Feld Konfiguration;
- e) Anwendung eines separaten Nachrichtenzählers für jede in TPL verwendete Schlüssel-ID;
- f) Aktualisierung der SITP-Definition in Anhang A durch Hinzufügen von DSI 23h und Streichen von DSI 30h.

**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

## **Inhalt**

|                                                                                                     | Seite |
|-----------------------------------------------------------------------------------------------------|-------|
| Europäisches Vorwort . . . . .                                                                      | 6     |
| Einleitung . . . . .                                                                                | 8     |
| 1 Anwendungsbereich . . . . .                                                                       | 10    |
| 2 Normative Verweisungen . . . . .                                                                  | 10    |
| 3 Begriffe . . . . .                                                                                | 10    |
| 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 . . . . .                                                                   | 16    |
| 6 Authentifizierungs- und Fragmentierungs-Teilschicht (AFL) . . . . .                               | 20    |
| 6.1 Einleitung . . . . .                                                                            | 20    |
| 6.2 Übersicht über die AFL-Struktur . . . . .                                                       | 21    |
| 6.3 Komponenten der AFL . . . . .                                                                   | 22    |
| 6.3.1 AFL-Längenfeld (AFL.AFL) . . . . .                                                            | 22    |
| 6.3.2 AFL-Fragmentierungskontrollfeld (AFL.FCL) . . . . .                                           | 22    |
| 6.3.3 AFL-Nachrichtenkontrollfeld (AFL.MCL) . . . . .                                               | 22    |
| 6.3.4 AFL-Schlüsselinformationsfeld (AFL.KI) . . . . .                                              | 23    |
| 6.3.5 AFL-Nachrichtenzählerfeld (AFL.MCR) . . . . .                                                 | 24    |
| 6.3.6 AFL-MAC-Feld (AFL.MAC) . . . . .                                                              | 24    |
| 6.3.7 AFL-Nachrichtenlängenfeld (AFL.ML) . . . . .                                                  | 24    |
| 7 Transportschicht (TPL) . . . . .                                                                  | 25    |
| 7.1 Einleitung . . . . .                                                                            | 25    |
| 7.2 Struktur ohne TPL-Header . . . . .                                                              | 25    |
| 7.3 Struktur mit kurzem TPL-Header . . . . .                                                        | 25    |
| 7.4 Struktur mit langem TPL-Header . . . . .                                                        | 26    |
| 7.5 CI-Feld-abhängige Elemente . . . . .                                                            | 26    |
| 7.5.1 Identifikationsnummer . . . . .                                                               | 26    |
| 7.5.2 Identifikation des Herstellers . . . . .                                                      | 27    |
| 7.5.3 Versionsidentifikation . . . . .                                                              | 27    |
| 7.5.4 Identifikation des Gerätetyps . . . . .                                                       | 27    |
| 7.5.5 Zugriffsnummer . . . . .                                                                      | 29    |
| 7.5.6 Statusbyte in Zählernachrichten . . . . .                                                     | 31    |
| 7.5.7 Statusbyte in Partnernachrichten . . . . .                                                    | 32    |
| 7.5.8 Konfigurationsfeld . . . . .                                                                  | 33    |
| 7.6 Konfigurationsfeldabhängige Struktur . . . . .                                                  | 34    |
| 7.6.1 Allgemeines . . . . .                                                                         | 34    |
| 7.6.2 Konfigurationsfelderweiterung . . . . .                                                       | 35    |
| 7.6.3 Optionale TPL-Header-Felder . . . . .                                                         | 35    |
| 7.6.4 Optionale TPL-Trailer-Felder . . . . .                                                        | 35    |
| 7.6.5 Teilverschlüsselung . . . . .                                                                 | 35    |
| 7.7 Sicherheitsmoduspezifische TPL-Felder . . . . .                                                 | 36    |
| 7.7.1 Gemeinsame Teilfelder des Konfigurationsfelds und der Konfigurationsfelderweiterung . . . . . | 36    |
| 7.7.2 Konfigurationsfeld des Sicherheitsmodus 0 . . . . .                                           | 39    |
| 7.7.3 Konfigurationsfeld der Sicherheitsmodi 2 und 3 . . . . .                                      | 40    |
| 7.7.4 Konfigurationsfeld des Sicherheitsmodus 5 . . . . .                                           | 41    |
| 7.7.5 Konfigurationsfeld des Sicherheitsmodus 7 . . . . .                                           | 42    |
| 7.7.6 Konfigurationsfeld des Sicherheitsmodus 8 . . . . .                                           | 44    |
| 7.7.7 Konfigurationsfeld des Sicherheitsmodus 9 . . . . .                                           | 47    |
| 7.7.8 Konfigurationsfeld des Sicherheitsmodus 10 . . . . .                                          | 49    |

|                     |                                                                                                   |    |
|---------------------|---------------------------------------------------------------------------------------------------|----|
| 8                   | Verwaltung der unteren Schichten                                                                  | 51 |
| 8.1                 | Allgemeines                                                                                       | 51 |
| 8.2                 | Setzen der Baudrate für die M-Bus-Verbindungsschicht nach EN 13757-2                              | 51 |
| 8.3                 | Adressstruktur bei Verwendung zusammen mit der drahtlosen Datenverbindungsschicht nach EN 13757-4 | 51 |
| 8.4                 | Selektion und Sekundäradressierung                                                                | 52 |
| 8.5                 | Generalisiertes Selektionsverfahren                                                               | 53 |
| 8.6                 | Suche nach installierten Slaves                                                                   | 54 |
| 8.6.1               | Primäradressen                                                                                    | 54 |
| 8.6.2               | Sekundäradressen                                                                                  | 54 |
| 8.6.3               | Verfahren der Platzhaltersuche                                                                    | 54 |
| 9                   | Sicherheitsdienste                                                                                | 55 |
| 9.1                 | Allgemeines                                                                                       | 55 |
| 9.2                 | Nachrichtenzähler                                                                                 | 56 |
| 9.2.1               | Überblick                                                                                         | 56 |
| 9.2.2               | Nachrichtenzähler $C_M$ , der vom Zähler übertragen wird                                          | 56 |
| 9.2.3               | Nachrichtenzähler $C_{CP}$ , der vom Kommunikationspartner übertragen wird                        | 57 |
| 9.2.4               | Nachrichtenzähler $C'_{CP}$ , der vom Zähler erhalten wird                                        | 57 |
| 9.2.5               | Nachrichtenzähler $C'_M$ und $C''_M$ , die vom Kommunikationspartner empfangen werden             | 57 |
| 9.3                 | Authentifizierungsverfahren in der AFL                                                            | 58 |
| 9.3.1               | Überblick                                                                                         | 58 |
| 9.3.2               | Authentifizierungsverfahren AES-CMAC-128                                                          | 58 |
| 9.3.3               | Authentifizierungsverfahren AES-GMAC-128                                                          | 59 |
| 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              | Liste der aktiven Schlüssel- und Schlüsselzählerinformation erhalten                              | 76 |
| A.2.11              | 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                                                                                    | 78 |
| A.7                 | Überblick über Datenstrukturen/Mechanismen                                                        | 78 |
| A.8                 | Datenstrukturen für Sicherheitsinformationen                                                      | 80 |

|                              |                                                                  |           |
|------------------------------|------------------------------------------------------------------|-----------|
| <b>A.8.1</b>                 | <b>Allgemeines</b>                                               | <b>80</b> |
| <b>A.8.2</b>                 | <b>Datenstruktur 00<sub>h</sub></b>                              | <b>80</b> |
| <b>A.8.3</b>                 | <b>Datenstruktur 01<sub>h</sub></b>                              | <b>81</b> |
| <b>A.8.4</b>                 | <b>Datenstruktur 02<sub>h</sub></b>                              | <b>81</b> |
| <b>A.8.5</b>                 | <b>Datenstruktur 03<sub>h</sub></b>                              | <b>82</b> |
| <b>A.8.6</b>                 | <b>Datenstruktur 20<sub>h</sub></b>                              | <b>83</b> |
| <b>A.8.7</b>                 | <b>Datenstruktur 21<sub>h</sub></b>                              | <b>83</b> |
| <b>A.8.8</b>                 | <b>Datenstruktur 22<sub>h</sub></b>                              | <b>84</b> |
| <b>A.8.9</b>                 | <b>Datenstruktur 23<sub>h</sub></b>                              | <b>85</b> |
| <b>A.9</b>                   | <b>Datenstrukturen für gesicherte Anwendungsdaten</b>            | <b>85</b> |
| <b>A.9.1</b>                 | <b>Allgemeines</b>                                               | <b>85</b> |
| <b>A.9.2</b>                 | <b>Datenstruktur 30<sub>h</sub> — AES-Schlüssel-Wrap</b>         | <b>87</b> |
| <b>A.9.3</b>                 | <b>Datenstruktur 31<sub>h</sub> — HMAC-SHA256</b>                | <b>87</b> |
| <b>A.9.4</b>                 | <b>Datenstruktur 32<sub>h</sub> und 33<sub>h</sub> — CMAC</b>    | <b>88</b> |
| <b>A.9.5</b>                 | <b>Datenstruktur 34<sub>h</sub> — AES-GCM</b>                    | <b>89</b> |
| <b>A.9.6</b>                 | <b>Datenstruktur 35<sub>h</sub> — AES-GMAC</b>                   | <b>90</b> |
| <b>A.9.7</b>                 | <b>Datenstruktur 36<sub>h</sub> und 37<sub>h</sub> — AES-CCM</b> | <b>91</b> |
| <b>Anhang B (informativ)</b> | <b>Beispiel eines Nachrichtenzählers</b>                         | <b>93</b> |
| <b>Literaturhinweise</b>     |                                                                  | <b>96</b> |

## **Bilder**

|                 |                                                      |           |
|-----------------|------------------------------------------------------|-----------|
| <b>Bild 1</b>   | <b>Eingabe und Ausgabe für den GCM-Algorithmus</b>   | <b>66</b> |
| <b>Bild B.1</b> | <b>Kontrollfluss des Nachrichtenzählers (Teil 1)</b> | <b>94</b> |
| <b>Bild B.2</b> | <b>Kontrollfluss des Nachrichtenzählers (Teil 2)</b> | <b>95</b> |

## **Tabellen**

|                   |                                                                               |           |
|-------------------|-------------------------------------------------------------------------------|-----------|
| <b>Tabelle 1</b>  | <b>Reihenfolge der M-Bus-Schicht</b>                                          | <b>16</b> |
| <b>Tabelle 2</b>  | <b>Vom Master oder Slave verwendete Codes des CI-Felds</b>                    | <b>17</b> |
| <b>Tabelle 3</b>  | <b>Übersicht über alle AFL-Felder</b>                                         | <b>21</b> |
| <b>Tabelle 4</b>  | <b>AFL-Fragmentierungskontrollfeld — Definitionen der Bitfelder</b>           | <b>22</b> |
| <b>Tabelle 5</b>  | <b>AFL-Nachrichtenkontrollfeld — Definitionen der Bitfelder</b>               | <b>22</b> |
| <b>Tabelle 6</b>  | <b>AT-Teilfeld von AFL.MCL</b>                                                | <b>23</b> |
| <b>Tabelle 7</b>  | <b>AFL-Schlüsselinformationfeld — Definitionen der Bitfelder</b>              | <b>23</b> |
| <b>Tabelle 8</b>  | <b>AFL-Nachrichtenzählerfeld — Definitionen der Bitfelder</b>                 | <b>24</b> |
| <b>Tabelle 9</b>  | <b>AFL-Nachrichtenzählervorgangfeld — Definitionen der Bitfelder</b>          | <b>25</b> |
| <b>Tabelle 10</b> | <b>Allgemeine Struktur der TPL</b>                                            | <b>25</b> |
| <b>Tabelle 11</b> | <b>Kurzer TPL-Header</b>                                                      | <b>26</b> |
| <b>Tabelle 12</b> | <b>Langer TPL-Header</b>                                                      | <b>26</b> |
| <b>Tabelle 13</b> | <b>Identifikation des Gerätetyps</b>                                          | <b>27</b> |
| <b>Tabelle 14</b> | <b>Kodierung des Statusfelds</b>                                              | <b>31</b> |
| <b>Tabelle 15</b> | <b>Mit dem Statusfeld kodierte Anwendungsfehler</b>                           | <b>31</b> |
| <b>Tabelle 16</b> | <b>Bedeutung des Statusbytes für Partnernachrichten</b>                       | <b>32</b> |
| <b>Tabelle 17</b> | <b>Bedeutung der Bits 0 bis 5 im Statusbyte für Partnernachrichten</b>        | <b>32</b> |
| <b>Tabelle 18</b> | <b>Allgemeine Definition der zwei obligatorischen Konfigurationsfeldbytes</b> | <b>33</b> |
| <b>Tabelle 19</b> | <b>Definition der Modusbits im Konfigurationsfeld (Sicherheitsmodus)</b>      | <b>34</b> |
| <b>Tabelle 20</b> | <b>TPL-Struktur einer geschützten Nachricht</b>                               | <b>34</b> |
| <b>Tabelle 21</b> | <b>Inhalt der Zählernachricht</b>                                             | <b>36</b> |
| <b>Tabelle 22</b> | <b>Inhalt der Partnernachricht</b>                                            | <b>36</b> |
| <b>Tabelle 23</b> | <b>Verwendung von Inhaltsindexbits</b>                                        | <b>37</b> |
| <b>Tabelle 24</b> | <b>Zugänglichkeit eines Geräts</b>                                            | <b>37</b> |
| <b>Tabelle 25</b> | <b>Schlüssel-ID</b>                                                           | <b>38</b> |

|                                                                                                       |    |
|-------------------------------------------------------------------------------------------------------|----|
| Tabelle 26 — KDF-Auswahl . . . . .                                                                    | 39 |
| Tabelle 27 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 0 . . . . .          | 39 |
| Tabelle 28 — Definition des Konfigurationsfelds für den Sicherheitsmodus 0 . . . . .                  | 39 |
| Tabelle 29 — Konfigurationsfeld und nachfolgende Felder mit den Sicherheitsmodi 2 und 3 . . . . .     | 40 |
| Tabelle 30 — Definition des Konfigurationsfelds für die Sicherheitsmodi 2 und 3 . . . . .             | 40 |
| Tabelle 31 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 5 . . . . .          | 41 |
| Tabelle 32 — Definition des Konfigurationsfelds für den Sicherheitsmodus 5 . . . . .                  | 41 |
| Tabelle 33 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 7 . . . . .          | 42 |
| Tabelle 34 — Definition des Konfigurationsfelds für den Sicherheitsmodus 7 . . . . .                  | 42 |
| Tabelle 35 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 7 . . . . .        | 43 |
| Tabelle 36 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 8 . . . . .          | 44 |
| Tabelle 37 — Definition des Konfigurationsfelds für Modus 8 . . . . .                                 | 45 |
| Tabelle 38 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 8 . . . . .        | 46 |
| Tabelle 39 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 9 . . . . .          | 47 |
| Tabelle 40 — Definition des Konfigurationsfelds für den Sicherheitsmodus 9 . . . . .                  | 48 |
| Tabelle 41 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 10 . . . . .         | 49 |
| Tabelle 42 — Definition des Konfigurationsfelds für den Sicherheitsmodus 10 . . . . .                 | 49 |
| Tabelle 43 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 10 . . . . .       | 50 |
| Tabelle 44 — Adressstruktur der Verbindungsschicht für Funk . . . . .                                 | 51 |
| Tabelle 45 — Struktur eines Datagramms für die Selektion eines Slaves . . . . .                       | 52 |
| Tabelle 46 — Anwendungsschichtstruktur eines Datagramms für die erweiterte Selektion . . . . .        | 53 |
| Tabelle 47 — Sicherheitsdienste und Sicherheitsziele . . . . .                                        | 55 |
| Tabelle 48 — Schutzmechanismen für die Ablesung des Zählers . . . . .                                 | 60 |
| Tabelle 49 — Initialisierungsvektor des Sicherheitsmodus 5 . . . . .                                  | 62 |
| Tabelle 50 — Struktur des Initialisierungsvektors in Sicherheitsmodus 8 . . . . .                     | 65 |
| Tabelle 51 — Eingabe- und Ausgabeinformationen für die GCM-Funktionen . . . . .                       | 66 |
| Tabelle 52 — Struktur des Initialisierungsvektors in Sicherheitsmodus 9 . . . . .                     | 69 |
| Tabelle 53 — Struktur der Nonce N . . . . .                                                           | 71 |
| Tabelle 54 — Konstante DC für die Schlüsselableitung . . . . .                                        | 72 |
| Tabelle A.1 — CI-Felder des Übertragungsprotokolls für Sicherheitsinformationen . . . . .             | 76 |
| Tabelle A.2 — Interne Blockstruktur des SITP . . . . .                                                | 76 |
| Tabelle A.3 — Blockkontrollfeld . . . . .                                                             | 77 |
| Tabelle A.4 — Blockparameterstruktur . . . . .                                                        | 78 |
| Tabelle A.5 — Liste der SITP-Datenstrukturen/Mechanismen . . . . .                                    | 79 |
| Tabelle A.6 — DSH-Inhalt von DSI 00 <sub>h</sub> . . . . .                                            | 80 |
| Tabelle A.7 — Wrapped-Datenstruktur 01 <sub>h</sub> . . . . .                                         | 81 |
| Tabelle A.8 — Wrapped-Datenstruktur 02 <sub>h</sub> . . . . .                                         | 81 |
| Tabelle A.9 — Wrapped-Datenstruktur 03 <sub>h</sub> . . . . .                                         | 82 |
| Tabelle A.10 — Optionen für Wrapped-Datenstruktur 03 <sub>h</sub> . . . . .                           | 82 |
| Tabelle A.11 — Datenstruktur 20 <sub>h</sub> für alle von einem Wrapper umhüllten Schlüssel . . . . . | 83 |
| Tabelle A.12 — Datenstruktur 21 <sub>h</sub> für aktiven Schlüssel . . . . .                          | 84 |
| Tabelle A.13 — Statusantwortstruktur . . . . .                                                        | 84 |
| Tabelle A.14 — Definition des Statusantwortbytes . . . . .                                            | 84 |
| Tabelle A.15 — Datenstruktur 23 <sub>h</sub> für aktiven Schlüsselzähler . . . . .                    | 85 |
| Tabelle A.16 — Liste der unterstützten PIDs . . . . .                                                 | 87 |
| Tabelle A.17 — Datenstruktur 31 <sub>h</sub> . . . . .                                                | 87 |
| Tabelle A.18 — Auswahl von Datenstruktur 32 <sub>h</sub> und 33 <sub>h</sub> . . . . .                | 88 |
| Tabelle A.19 — Datenstruktur 32 <sub>h</sub> und 33 <sub>h</sub> . . . . .                            | 88 |
| Tabelle A.20 — Datenstruktur 34 <sub>h</sub> . . . . .                                                | 89 |
| Tabelle A.21 — Struktur von IV bei AES-GCM . . . . .                                                  | 89 |
| Tabelle A.22 — Datenstruktur 35 <sub>h</sub> . . . . .                                                | 90 |
| Tabelle A.23 — Struktur von IV bei AES-GMAC . . . . .                                                 | 91 |
| Tabelle A.24 — Auswahl von Datenstruktur 36 <sub>h</sub> und 37 <sub>h</sub> . . . . .                | 91 |
| Tabelle A.25 — Wrapped-Datenstruktur 36 <sub>h</sub> und 37 <sub>h</sub> . . . . .                    | 91 |
| Tabelle A.26 — Struktur der CCM-Nonce bei AES-GMAC . . . . .                                          | 92 |

## Europäisches Vorwort

Dieses Dokument (prEN 13757-7:2023) wurde vom Technischen Komitee CEN/TC 294 „Kommunikationssysteme für Zähler“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN 13757-7:2018 ersetzen.

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission und die Europäische Freihandelsassoziation CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinie(n).

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.

EN 13757-7:2023 enthält gegenüber EN 13757-7:2018 folgende wesentliche technischen Änderungen:

- Unterstützung von Sensorgeräten und Warnmeldern;
- Verringerung der Gerätetypen für Wärmeenergiezähler;
- Unterstützung von MBAL nach neuer Norm EN 13757-8;
- Einführung der Inhaltsdefinition für das Unterfeld Inhaltsindex im Konfigurationsfeld;
- Anwendung eines separaten Nachrichtenzählers für jede in der TPL verwendete Schlüssel-ID;
- Aktualisierung der SITP-Definition in Anhang A, z. B. Ergänzung von DSI 23h und Streichung von DSI 30h.

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*

- *Kommunikationssysteme für Zähler — Teil 8: Anpassungsschicht*<sup>1</sup>
- *CEN/TR 17167, Kommunikationssysteme für Zähler — Begleitender Technischer Bericht zu EN 13757-2, EN 13757-3 und EN 13757-7, Beispiele und ergänzende Informationen.*

Das vorliegende Dokument wird in Verbindung mit CEN/CLC/ETSI/TR 50572 [4] verwendet.

---

1 In Bearbeitung.

## Einleitung

Dieses Dokument ist Teil der Normenreihe EN 13757, die Kommunikationssysteme für Zähler behandelt. 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 (häufig als Funk-M-Bus oder wM-Bus bezeichnete) Funkkommunikation. EN 13757-5 beschreibt das für die Wiederholung, Weitervermittlung und das Routing für die in EN 13757-4 beschriebenen Modi zu nutzende Funknetz. EN 13757-6 beschreibt einen für Kurzstrecken zu verwendenden lokal begrenzten Zweidraht-Bus (Lo-Bus). EN 13757-7 beschreibt Transportmechanismen und 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 (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 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.

Ein Überblick über Kommunikationssysteme für Zähler wird in EN 13757-1 gegeben, die auch weitere Definitionen enthält.

Dieses Dokument konzentriert sich auf die Zählerkommunikation. Der Zähler kommuniziert mit einem (oder manchmal mehreren) festen oder mobilen Kommunikationspartnern, die wiederum Teil eines privaten oder öffentlichen Netzwerks sein könnten. Diese weiteren Kommunikationssysteme könnten 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 dieses Dokument 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 17167:2023<sup>1</sup>, 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 17167:2023<sup>1</sup>, 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 die-

ses Dokuments, welches 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

Dieses Dokument legt die Transport- und Sicherheitsdienste für Kommunikationssysteme für Zähler und Fernablesungen für Zähler fest.

Dieses Dokument legt sichere Kommunikationsfähigkeiten nach Design fest und unterstützt den Aufbau einer sicheren Systemarchitektur.

Dieses Dokument gilt für den Schutz der Verbraucherdaten zur Sicherung der Privatsphäre.

Dieses Dokument soll mit den in den relevanten Teilen der Normenreihe EN 13757 festgelegten Spezifikationen der unteren Schicht verwendet werden.

## 2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 13757-2, *Kommunikationssysteme für Zähler — Teil 2: Drahtgebundene M-Bus-Kommunikation*

EN 13757-3:2023, *Kommunikationssysteme für Zähler — Teil 3: Anwendungsprotokolle*<sup>1</sup>

EN 13757-4:2019, *Kommunikationssysteme für Zähler — Teil 4: Drahtlose M-Bus-Kommunikation*

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-   | Zugriffsbedarf                                                                        | Access Demand                                                                     |
| DMD    |                                                                                       |                                                                                   |
| ACC-NR | Zugriff – Keine Antwort                                                               | Access – No Reply                                                                 |
| ACK    | Quittieren [EN 13757-2/EN 13757-4]                                                    | Acknowledge [EN 13757-2/EN 13757-4]                                               |
| AES    | Advanced Encryption Standard                                                          | Advanced Encryption Standard                                                      |
| AFL    | Authentifizierungs- und Fragmentierungs-<br>Teilschicht                               | Authentication and Fragmentation Sublayer                                         |
| APDU   | Dateneinheit des Anwendungsprotokolls                                                 | Application Protocol Data Unit                                                    |
| APL    | Anwendungsschicht                                                                     | Application Layer                                                                 |
| ASCII  | American Standard Code for Information<br>Interchange                                 | American Standard Code for Information<br>Interchange                             |
| BCD    | Binär kodierte Dezimalzahlen                                                          | Binary Coded Decimal numbers                                                      |
| BCF    | Blockkontrollfeld der SITP-Struktur, Kodierung<br>der Nutzung von Befehl bzw. Antwort | Block control field of SITP structure, coding the<br>usage of command or response |
| BID    | Blockidentifikationsnummer der SITP-Struktur                                          | Block identification number of SITP structure                                     |
| BL     | Blocklänge der SITP-Struktur                                                          | Block length of SITP structure                                                    |
| CBC    | Cipher Block Chaining (AES-Betriebsmodus)                                             | Cipher Block Chaining; (AES mode of operation)                                    |
| CCM    | Verschlüsselungsalgorithmus des Zählermodus<br>mit CBC-MAC (AES-Betriebsmodus)        | Counter mode encryption algorithm with CBC-<br>MAC (AES mode of operation)        |
| CF     | Konfigurationsfeld                                                                    | Configuration Field                                                               |
| CFE    | Konfigurationsfelderweiterung                                                         | Configuration Field Extension                                                     |
| CI     | Steuerinformationsfeld                                                                | Control Information field                                                         |
| CMAC   | Chiffre-basierter MAC [NIST/SP 800-38B]                                               | Cipher-based MAC [NIST/SP 800-38B]                                                |
| CNF-IR | Installationsanforderung bestätigen                                                   | Confirm Installation Request                                                      |
| CTR    | Verschlüsselungsalgorithmus des Zählermodus<br>(AES-Betriebsmodus)                    | Counter Mode encryption algorithm (AES mode<br>of operation)                      |
| DES    | Data Encryption Standard                                                              | Data Encryption Standard                                                          |
| DIF    | Dateninformationsfeld                                                                 | Data Information Field                                                            |
| DLL    | Datenverbindungsschicht                                                               | Data Link Layer                                                                   |
| DLMS   | Device Language Message Specification                                                 | Device Language Message Specification                                             |
| DSI    | Datenstrukturidentifikator, Teil der<br>Blockparameterstruktur innerhalb des SITP     | Data structure identifier, part of block<br>parameter structure inside SITP       |
| DSH    | Header der Datenstruktur, Teil der<br>Blockparameterstruktur innerhalb des SITP       | Data structure header, part of block parameter<br>structure inside SITP           |
| DSH1   | Byte eins des DSH                                                                     | Byte one of DSH                                                                   |

|         |                                                                                                                                                                                                                |                                                                                                             |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| DSH2    | Byte zwei des DSH                                                                                                                                                                                              | Byte two of DSH                                                                                             |
| ELL     | Erweiterte Verbindungsschicht                                                                                                                                                                                  | Extended Link Layer                                                                                         |
| GCM     | Galois-/Zählermodus, ein Algorithmus für die authentifizierte Verschlüsselung mit zugehörigen Daten (AES-Betriebsmodus)                                                                                        | Galois/Counter Mode, an algorithm for authenticated encryption with associated data (AES mode of operation) |
| GMAC    | eine Spezialisierung des GCM zur Erzeugung eines Nachrichtenauthentifizierungscodes (en: Message Authentication Code, MAC) für nicht verschlüsselte Daten                                                      | a specialization of GCM for generating a message authentication code (MAC) on data that is not encrypted    |
| ICV     | Integritätsüberprüfungswert, Teil einer Wrapped-Datenstruktur im SITP                                                                                                                                          | Integrity check value, part of a wrapped data structure in SITP                                             |
| IV      | Initialisierungsvektor                                                                                                                                                                                         | Initialization Vector                                                                                       |
| LSB     | Niedrigstwertiges Byte                                                                                                                                                                                         | Least Significant Byte                                                                                      |
| LSBit   | Niedrigstwertiges Bit                                                                                                                                                                                          | Least Significant Bit                                                                                       |
| MAC     | Nachrichtenauthentifizierungscode<br><br>ANMERKUNG MAC ist in anderen Normen auch das Akronym für Steuerung für Medienzugriff (en: Media Access Control) für die Datenkommunikation an der physischen Schicht. | Message Authentication Code                                                                                 |
| MBAL    | M-Bus-Anpassungsschicht [prEN 13757-8]                                                                                                                                                                         | M-Bus Adaptation layer [prEN 13757-8]                                                                       |
| MK      | Nachrichtenschlüssel (persistent)                                                                                                                                                                              | Message Key (persistent)                                                                                    |
| MLI     | Nachrichtenlängenidentifikator, Teil einer Wrapped-Datenstruktur im SITP                                                                                                                                       | Message Length Indicator, part of a wrapped data structure in SITP                                          |
| MSB     | Höchstwertiges Byte                                                                                                                                                                                            | Most Significant Byte                                                                                       |
| MSBit   | Höchstwertiges Bit                                                                                                                                                                                             | Most Significant Bit                                                                                        |
| NWL     | Netzwerkschicht                                                                                                                                                                                                | Network Layer                                                                                               |
| OBIS    | Object Identification System (EN 62056-61)                                                                                                                                                                     | Object Identification System (EN 62056-61)                                                                  |
| PID     | Protokollidentifikatorfeld, Teil einer Wrapped-Datenstruktur im SITP                                                                                                                                           | Protocol identifier field, part of wrapped data structure in SITP                                           |
| REQ-UD  | Nutzerdaten anfordern (Klasse 1 oder 2) [EN 13757-2/EN 13757-4]                                                                                                                                                | Request User Data (class 1 or 2) [EN 13757-2/EN 13757-4]                                                    |
| RSP-UD  | Mit Nutzerdaten antworten [EN 13757-2/EN 13757-4]                                                                                                                                                              | Respond User Data [EN 13757-2/EN 13757-4]                                                                   |
| RSSI    | Anzeiger für die Signalstärke des empfangenen Signals                                                                                                                                                          | Received Signal Strength Indicator                                                                          |
| SITP    | Übertragungsprotokoll für Sicherheitsinformationen                                                                                                                                                             | Security Information Transfer Protocol                                                                      |
| SND-IR  | Installationsanforderung senden [EN 13757-4]                                                                                                                                                                   | Send Installation Request [EN 13757-4]                                                                      |
| SND-NKE | Verbindungsrücksetzung senden [EN 13757-2/EN 13757-4]                                                                                                                                                          | Send Link Reset [EN 13757-2/EN 13757-4]                                                                     |
| SND-NR  | Senden – Keine Antwort [EN 13757-4]                                                                                                                                                                            | Send – No Reply [EN 13757-4]                                                                                |
| SND-UD  | Nutzerdaten senden [EN 13757-2/EN 13757-4]                                                                                                                                                                     | Send User Data [EN 13757-2/EN 13757-4]                                                                      |
| SND-UD2 | Nutzerdaten senden 2 [EN 13757-2/EN 13757-4]                                                                                                                                                                   | Send User Data 2 [EN 13757-2/EN 13757-4]                                                                    |

|         |                                   |                                    |
|---------|-----------------------------------|------------------------------------|
| SND-UD3 | Nutzerdaten senden 3 [EN 13757-4] | Send User Data 3 [EN 13757-4]      |
| TPDU    | Transportprotokolldateneinheit    | Transport Protocol Data Unit       |
| TPL     | Transportschicht                  | Transport Layer                    |
| VIF     | Wertinformationsfeld              | Value Information Field            |
| VIFE    | Wertinformationsfeld-Erweiterung  | Value Information Field Extensions |

## 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 || 34h ergibt 1 234h.

## 5 Schichtmodell

### 5.1 M-Bus-Schichten

Der M-Bus deckt verschiedene Kommunikationsschichten ab. Die Bitübertragungsschicht und die Daten Verbindungsschicht 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 <sup>b</sup> | OSI-Modell Schicht     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------|---------------------------------------------|-------------------------|------------------------|
| APL (en: Application Layer)                                                                                                                                                                       | Anwendungsschicht                                    | a                       | EN 13757-1/EN 13757-3/<br>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 Transport          |                        |
| 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/<br>EN 13757-5          | Hellblau                |                        |
| PHY (en: Physical Layer)                                                                                                                                                                          | Bitübertragungs- schicht                             | Nein                    | EN 13757-2/EN 13757/<br>EN 13757-5/EN 13757 | Hellgelb                | Physikalisch           |
| <sup>a</sup> Die APL wird nicht von einem zugeordneten CI-Feld eingeführt, sondern vom CI-Feld der TPL angegeben.<br><sup>b</sup> 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 Längengelds 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 <sub>h</sub> bis 1F <sub>h</sub> | Reserviert für DLMS-basierte Anwendungen               | APL     | keine      | DLMS (siehe EN 13757-1)                                                           |
| 20 <sub>h</sub>                     | Spezifische Nutzung <sup>b</sup>                       | APL     | keine      | ANMERKUNG Einführung der Darstellungsschicht aus Literaturhinweis [16]            |
| 21 <sub>h</sub>                     | Spezifische Nutzung <sup>b</sup>                       | APL     | keine      | ANMERKUNG Einführung der Darstellungsschicht aus Literaturhinweis [16]            |
| 22 <sub>h</sub>                     | Spezifische Nutzung <sup>b</sup>                       | APL     | keine      | ANMERKUNG Einführung der Darstellungsschicht aus Literaturhinweis [16]            |
| 23 <sub>h</sub> bis 4F <sub>h</sub> | Reserviert                                             |         |            |                                                                                   |
| 50 <sub>h</sub>                     | Anwendungsrücksetzung oder -auswahl an Gerät           | APL     | keine      | Anwendungsauswahl;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7             |
| 51 <sub>h</sub>                     | Befehl an Gerät<br>(voller M-Bus-Datenrahmen)          | APL     | keine      | M-Bus (nicht für drahtlos);<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7    |
| 52 <sub>h</sub>                     | Auswahl des Geräts                                     |         | keine      | Management, siehe 8.4                                                             |
| 53 <sub>h</sub>                     | Anwendungsrücksetzung oder -auswahl an Gerät           | APL     | Lang       | Anwendungsauswahl;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7             |
| 54 <sub>h</sub>                     | Anfrage der ausgewählten Anwendung an das Gerät        | APL     | keine      | Anwendungsauswahl;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7             |
| 55 <sub>h</sub>                     | Anfrage der ausgewählten Anwendung an das Gerät        | APL     | Lang       | Anwendungsauswahl;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7             |
| 56 <sub>h</sub> bis 59 <sub>h</sub> | Reserviert                                             |         |            |                                                                                   |
| 5A <sub>h</sub>                     | Befehl an Gerät<br>(voller M-Bus-Datenrahmen)          | APL     | Kurz       | M-Bus;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7                         |
| 5B <sub>h</sub>                     | Befehl an Gerät<br>(voller M-Bus-Datenrahmen)          | APL     | Lang       | M-Bus;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 6                         |
| 5C <sub>h</sub>                     | Aktion synchronisieren                                 | APL     | keine      | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 12                                  |
| 5D <sub>h</sub> bis 5E <sub>h</sub> | Reserviert                                             |         |            |                                                                                   |
| 5F <sub>h</sub>                     | Spezifische Nutzung <sup>b</sup>                       | TPL     | Lang       | ANMERKUNG Siehe Literaturhinweis [8].                                             |
| 60 <sub>h</sub>                     | Befehl an Gerät                                        | APL     | Lang       | DLMS/COSEM mit OBIS-Identifikator (nach EN 13757-1 und EN 62056-5-3) <sup>a</sup> |
| 61 <sub>h</sub>                     | Befehl an Gerät                                        | APL     | Kurz       | DLMS/COSEM mit OBIS-Identifikator (nach EN 13757-1 und EN 62056-5-3) <sup>a</sup> |
| 62 <sub>h</sub> bis 63 <sub>h</sub> | Reserviert                                             |         |            |                                                                                   |
| 64 <sub>h</sub>                     | Befehl an Gerät                                        | APL     | Lang       | Reserviert für Beschreiber von Werten des Typs OBIS <sup>a</sup>                  |
| 65 <sub>h</sub>                     | Befehl an Gerät                                        | APL     | Kurz       | Reserviert für Beschreiber von Werten des Typs OBIS <sup>a</sup>                  |
| 66 <sub>h</sub>                     | Antwort bezüglich der ausgewählten Anwendung vom Gerät | APL     | keine      | Anwendungsauswahl;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7             |

**Tabelle 2 (fortgesetzt)**

| CI-Feld                             | Richtung                                               | Schicht | TPL-Header | Protokoll der höheren Schicht                                                     |
|-------------------------------------|--------------------------------------------------------|---------|------------|-----------------------------------------------------------------------------------|
| 67 <sub>h</sub>                     | Antwort bezüglich der ausgewählten Anwendung vom Gerät | APL     | Kurz       | Anwendungsauswahl;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7             |
| 68 <sub>h</sub>                     | Antwort bezüglich der ausgewählten Anwendung vom Gerät | APL     | Lang       | Anwendungsauswahl;<br>nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 7             |
| 69 <sub>h</sub>                     | Antwort vom Gerät (M-Bus-Formatrahmen)                 | APL     | keine      | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , 6, Anhang G                            |
| 6A <sub>h</sub>                     | Antwort vom Gerät (M-Bus-Formatrahmen)                 | APL     | Kurz       | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , Anhang G                               |
| 6B <sub>h</sub>                     | Antwort vom Gerät (M-Bus-Formatrahmen)                 | APL     | Lang       | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , Anhang G                               |
| 6C <sub>h</sub>                     | Zeitsynchronisierung zum Gerät                         | APL     | Lang       | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 8                                   |
| 6D <sub>h</sub>                     | Veraltet (zuvor Zeitsynchronisierung zum Gerät)        | APL     | Lang       | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 8                                   |
| 6E <sub>h</sub>                     | Anwendungsfehler vom Gerät                             | APL     | Kurz       | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 10                                  |
| 6F <sub>h</sub>                     | Anwendungsfehler vom Gerät                             | APL     | Lang       | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 10                                  |
| 70 <sub>h</sub>                     | Anwendungsfehler vom Gerät                             | APL     | keine      | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 10                                  |
| 71 <sub>h</sub>                     | Alarm vom Gerät                                        | APL     | keine      | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 9                                   |
| 72 <sub>h</sub>                     | Antwort vom Gerät<br>(voller M-Bus-Datenrahmen)        | APL     | Lang       | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 6                            |
| 73 <sub>h</sub>                     | Antwort vom Gerät (M-Bus-Kompaktrahmen)                | APL     | Lang       | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 6, Anhang G                  |
| 74 <sub>h</sub>                     | Alarm vom Gerät                                        | APL     | Kurz       | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 9                                   |
| 75 <sub>h</sub>                     | Alarm vom Gerät                                        | APL     | Lang       | nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 9                                   |
| 76 <sub>h</sub> bis 77 <sub>h</sub> | Reserviert                                             |         |            |                                                                                   |
| 78 <sub>h</sub>                     | Antwort vom Gerät<br>(voller M-Bus-Datenrahmen)        | APL     | keine      | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 6                            |
| 79 <sub>h</sub>                     | Antwort vom Gerät (M-Bus-Kompaktrahmen)                | APL     | keine      | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 6, Anhang G                  |
| 7A <sub>h</sub>                     | Antwort vom Gerät<br>(voller M-Bus-Datenrahmen)        | APL     | Kurz       | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 6                            |
| 7B <sub>h</sub>                     | Antwort vom Gerät (M-Bus-Kompaktrahmen)                | APL     | Kurz       | M-Bus; nach EN 13757-3:2023 <sup>1</sup> , Abschnitt 6                            |
| 7C <sub>h</sub>                     | Antwort vom Gerät                                      | APL     | Lang       | DLMS/COSEM mit OBIS-Identifikator (nach EN 13757-1 und EN 62056-5-3) <sup>a</sup> |
| 7D <sub>h</sub>                     | Antwort vom Gerät                                      | APL     | Kurz       | DLMS/COSEM mit OBIS-Identifikator (nach EN 13757-1 und EN 62056-5-3) <sup>a</sup> |
| 7E <sub>h</sub>                     | Antwort vom Gerät                                      | APL     | Lang       | Reserviert für Beschreiber von Werten des Typs OBIS <sup>a</sup>                  |
| 7F <sub>h</sub>                     | Antwort vom Gerät                                      | APL     | Kurz       | Reserviert für Beschreiber von Werten des Typs OBIS <sup>a</sup>                  |
| 80 <sub>h</sub>                     | Transportschicht zum Gerät<br>(ohne APL)               | TPL     | Lang       | nach EN 13757-4                                                                   |

**Tabelle 2 (fortgesetzt)**

| CI-Feld                             | Richtung                                                  | Schicht | TPL-Header | Protokoll der höheren Schicht                |
|-------------------------------------|-----------------------------------------------------------|---------|------------|----------------------------------------------|
| 81 <sub>h</sub>                     | Netzwerkschichtdaten                                      | NWL     |            | nach EN 13757-5                              |
| 82 <sub>h</sub>                     | Netzwerkmanagementdaten zum Gerät                         | APL     | Lang       | Nach EN 13757-4 und EN 13757-5               |
| 83 <sub>h</sub>                     | Netzwerkmanagementdaten zum Gerät                         | APL     | keine      | Nach EN 13757-4 und EN 13757-5               |
| 84 <sub>h</sub>                     | Transportschicht zum Gerät (M-Bus-Kompaktrahmen erwartet) | TPL     | Lang       | Nach EN 13757-3:2023 <sup>1</sup> , Anhang G |
| 85 <sub>h</sub>                     | Transportschicht zum Gerät (M-Bus-Formatrahmen erwartet)  | TPL     | Lang       | Nach EN 13757-3:2023 <sup>1</sup> , Anhang G |
| 86 <sub>h</sub>                     | Reserviert für erweiterte Verbindungsschicht              | ELL     |            | nach EN 13757-4                              |
| 87 <sub>h</sub>                     | Netzwerkmanagementdaten vom Gerät                         | APL     | Lang       | Nach EN 13757-4, EN 13757-5                  |
| 88 <sub>h</sub>                     | Netzwerkmanagementdaten vom Gerät                         | APL     | Kurz       | Nach EN 13757-4, EN 13757-5                  |
| 89 <sub>h</sub>                     | Netzwerkmanagementdaten vom Gerät                         | APL     | keine      | Nach EN 13757-4, EN 13757-5                  |
| 8A <sub>h</sub>                     | Transportschicht vom Gerät (ohne APL)                     | TPL     | Kurz       | nach EN 13757-4                              |
| 8B <sub>h</sub>                     | Transportschicht vom Gerät (ohne APL)                     | TPL     | Lang       | nach EN 13757-4                              |
| 8C <sub>h</sub> bis 8F <sub>h</sub> | Erweiterte Verbindungsschicht                             | ELL     |            | nach EN 13757-4                              |
| 90 <sub>h</sub>                     | Authentifizierungs- und Fragmentierungs-Teilschicht       | AFL     |            | Nach Abschnitt 6                             |
| 91 <sub>h</sub>                     | Reserviert                                                |         |            |                                              |
| 92 <sub>h</sub> bis 97 <sub>h</sub> | Reserviert                                                |         |            | Nach EN 13757-4, EN 13757-5                  |
| 98 <sub>h</sub> bis 9D <sub>h</sub> | Reserviert                                                |         |            |                                              |
| 9E <sub>h</sub>                     | Spezifische Nutzung <sup>b</sup>                          | TPL     | Kurz       | ANMERKUNG Siehe Literaturhinweis [8].        |
| 9F <sub>h</sub>                     | Spezifische Nutzung <sup>b</sup>                          | TPL     | Lang       | ANMERKUNG Siehe Literaturhinweis [8].        |
| A0 <sub>h</sub> bis B7 <sub>h</sub> | Herstellerspezifisch                                      | APL     |            | Nach EN 13757-3:2023 <sup>1</sup> , 13       |
| B8 <sub>h</sub>                     | Baudrate auf 300 Baud setzen                              | APL     | keine      | Management der unteren Schichten; nach 8.2   |
| B9 <sub>h</sub>                     | Baudrate auf 600 Baud setzen                              | APL     | keine      | Management der unteren Schichten; nach 8.2   |
| BA <sub>h</sub>                     | Baudrate auf 1 200 Baud setzen                            | APL     | keine      | Management der unteren Schichten; nach 8.2   |
| BB <sub>h</sub>                     | Baudrate auf 2 400 Baud setzen                            | APL     | keine      | Management der unteren Schichten; nach 8.2   |
| BC <sub>h</sub>                     | Baudrate auf 4 800 Baud setzen                            | APL     | keine      | Management der unteren Schichten; nach 8.2   |
| BD <sub>h</sub>                     | Baudrate auf 9 600 Baud setzen                            | APL     | keine      | Management der unteren Schichten; nach 8.2   |
| BE <sub>h</sub>                     | Baudrate auf 19 200 Baud setzen                           | APL     | keine      | Management der unteren Schichten; nach 8.2   |

**Tabelle 2 (fortgesetzt)**

| CI-Feld                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Richtung                        | Schicht | TPL-Header | Protokoll der höheren Schicht                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|---------|------------|--------------------------------------------------------------------------------------------------------------------------------------|
| BF <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Baudrate auf 38 400 Baud setzen | APL     | keine      | Management der unteren Schichten; nach 8.2                                                                                           |
| C0 <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Befehl an Gerät                 | APL     | Lang       | Image-Übertragung; nach EN 13757-3:2023 <sup>1</sup> , Anhang I                                                                      |
| C1 <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Antwort vom Gerät               | APL     | Kurz       | Image-Übertragung; nach EN 13757-3:2023 <sup>1</sup> , Anhang I                                                                      |
| C2 <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Antwort vom Gerät               | APL     | Lang       | Image-Übertragung; nach EN 13757-3:2023 <sup>1</sup> Anhang I                                                                        |
| C3 <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Befehl an Gerät                 | APL     | Lang       | Sicherheitsinformationenübertragung; nach Anhang A                                                                                   |
| C4 <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Antwort vom Gerät               | APL     | Kurz       | Sicherheitsinformationenübertragung; nach Anhang A                                                                                   |
| C5 <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Antwort vom Gerät               | APL     | Lang       | Sicherheitsinformationenübertragung; nach Anhang A                                                                                   |
| C6 <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Befehl an Gerät                 | APL     | Kurz       | Sicherheitsinformationsübertragung; nach Anhang A; darf zur Kommunikation mit MBAL verwendet werden (siehe EN 13757-8 <sup>1</sup> ) |
| C7 <sub>h</sub> bis CB <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Reserviert                      |         |            |                                                                                                                                      |
| CC <sub>h</sub> bis CE <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Reserviert                      |         |            | Nach EN 13757-8 <sup>1</sup>                                                                                                         |
| CF <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Kurze M-Bus-Anpassungsschicht   | MBAL    |            | Nach EN 13757-8 <sup>1</sup>                                                                                                         |
| DO <sub>h</sub> bis FF <sub>h</sub>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Reserviert                      |         |            |                                                                                                                                      |
| ANMERKUNG Alle SND-DU-Datagramme werden in der Daten Verbindungsschicht zu quittiert, selbst wenn die Funktion dieser CI-Felder nicht implementiert ist.                                                                                                                                                                                                                                                                                                                                                           |                                 |         |            |                                                                                                                                      |
| <sup>a</sup> Die Anwendungsprotokolle beinhalten ebenfalls OBIS-Kennungen. Im M-Bus-Anwendungsprotokoll sind diese OBIS-Kennungen nicht enthalten, können aber nachträglich hinzugefügt werden. EN 13757-3:2023 <sup>1</sup> , Anhang H, ist zu verwenden, um die OBIS-Kennungen aus den M-Bus-Daten zu generieren.<br><sup>b</sup> 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 Protokolldateneinheiten ein);
- Authentifizierung der Gesamtnachricht durch einen MAC (dies kombiniert den Fragmenttransport mit der Authentifizierung einer Anwendungsprotokolldateneinheit).

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<br>(Bytes)                                                                                                                             | Feldname | Beschreibung                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------|
| 1                                                                                                                                            | CI       | Zeigt an, dass eine Authentifizierungs- und Fragmentierungs-Teilschicht folgt. |
| 1                                                                                                                                            | AFL      | AFL-Länge                                                                      |
| 2                                                                                                                                            | FCL      | Fragmentierungs-Kontrollfeld                                                   |
| 1                                                                                                                                            | MCL      | Nachrichtenkontrollfeld <sup>a</sup>                                           |
| 2                                                                                                                                            | KI       | Schlüsselinformationsfeld <sup>a</sup>                                         |
| 4                                                                                                                                            | MCR      | Nachrichtenzählerfeld <sup>a</sup>                                             |
| N <sup>b</sup>                                                                                                                               | MAC      | Nachrichtenauthentifizierungscode <sup>a</sup>                                 |
| 2                                                                                                                                            | ML       | Nachrichtenlängenfeld <sup>a</sup>                                             |
| <sup>a</sup> Dies ist ein optionales Feld. Ihre Aufnahme wird durch das Fragmentierungskontrollfeld definiert, das in 6.3.2 festgelegt wird. |          |                                                                                |
| <sup>b</sup> 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.AFLL)**

Dieses Feld beschreibt die Anzahl aller Bytes innerhalb der AFL, außer das 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 (Vorgabewert 0 <sub>b</sub> )                                                              |
| 14                                                                | MF       | Mehr Fragmente<br>0 <sub>b</sub> Dies ist das letzte Fragment<br>1 <sub>b</sub> Mehr Fragmente folgen |
| 13                                                                | MCLP     | In diesem Fragment ist eine Nachrichtenkontrolle vorhanden <sup>a</sup>                               |
| 12                                                                | MLP      | In diesem Fragment ist eine Nachrichtenlänge vorhanden <sup>a</sup>                                   |
| 11                                                                | MCRP     | In diesem Fragment ist ein Nachrichtenzähler vorhanden <sup>a</sup>                                   |
| 10                                                                | MACP     | In diesem Fragment ist ein MAC vorhanden <sup>a</sup>                                                 |
| 9                                                                 | KIP      | In diesem Fragment sind Schlüsselinformationen vorhanden <sup>a</sup>                                 |
| 8                                                                 | RES      | Reserviert (Vorgabewert 0 <sub>b</sub> )                                                              |
| 7 bis 0                                                           | FID      | Fragment-ID                                                                                           |
| <sup>a</sup> 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 (Vorgabewert 0 <sub>b</sub> )                               |
| 6   | MLMP     | In dieser Nachricht ist eine Nachrichtenlänge vorhanden <sup>a</sup>   |
| 5   | MCMP     | In dieser Nachricht ist ein Nachrichtenzähler vorhanden <sup>a</sup>   |
| 4   | KIMP     | In dieser Nachricht sind Schlüsselinformationen vorhanden <sup>a</sup> |

**Tabelle 5 (fortgesetzt)**

| Bit                                                               | Feldname | Beschreibung                            |
|-------------------------------------------------------------------|----------|-----------------------------------------|
| 3                                                                 | AT       | Authentifizierungstyp (siehe Tabelle 6) |
| 2                                                                 |          |                                         |
| 1                                                                 |          |                                         |
| 0                                                                 |          |                                         |
| <sup>a</sup> 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 Authentifizierungscode |
|----------|-------------------------|----------------------------------|
| 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 (Vorgabewert 0 <sub>b</sub> )                                                     |

Tabelle 7 (fortgesetzt)

| Bit     | Feldname     | Beschreibung                                                                                            |
|---------|--------------|---------------------------------------------------------------------------------------------------------|
| 5 bis 4 | KDF-Auswahl  | Die KDF-Auswahl identifiziert die angewandte Schlüsselableitungsfunktion, wie in Tabelle 26 festgelegt. |
| 3 bis 0 | Schlüssel-ID | Die Schlüssel-ID identifiziert den angewandten Schlüssel, wie in Tabelle 25 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-Nachrichtenlängelfeld (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<br>Kurzer Header<br>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                 |                             |
|---------------------|--------|-------------------------|-------------------------------------|-----------------------------|
| Zugriffsnr.         | 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. 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:

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

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

Ein FF<sub>h</sub> ist als Platzhalter zu interpretieren. Ein Platzhalter kann jeden Wert von 00<sub>h</sub> bis FE<sub>h</sub> ersetzen. Eine Herstelleridentifikation FFFF<sub>h</sub> 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<sub>h</sub> ist als Platzhalter zu interpretieren. Ein Platzhalter kann jeden Wert von 00<sub>h</sub> bis FE<sub>h</sub> ersetzen. 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<br>Bit 7 ... 0 | Hexadezimal-<br>code |
|--------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------|
| Sonstige                                                                                                                 | 0000 0000                | 00                   |
| Ölzähler                                                                                                                 | 0000 0001                | 01                   |
| Elektrizitätszähler                                                                                                      | 0000 0010                | 02                   |
| Gaszähler                                                                                                                | 0000 0011                | 03                   |
| Veraltet (zuvor Wärmeenergiezähler — Wärme) <sup>h</sup><br>(Volumen, das am Rücklauf temperatúrausgang gemessen wird)   | 0000 0100                | 04                   |
| Dampfzähler                                                                                                              | 0000 0101                | 05                   |
| Warmwasserzähler (30 °C ... 90 °C) <sup>e</sup>                                                                          | 0000 0110                | 06                   |
| Wasserzähler <sup>e</sup>                                                                                                | 0000 0111                | 07                   |
| Heizkostenverteiler                                                                                                      | 0000 1000                | 08                   |
| Druckluft                                                                                                                | 0000 1001                | 09                   |
| Veraltet (zuvor Wärmeenergiezähler — Kühlung) <sup>i</sup><br>(Volumen, das am Rücklauf temperatúrausgang gemessen wird) | 0000 1010                | 0A                   |
| Veraltet (zuvor Wärmeenergiezähler — Kühlung) <sup>i</sup><br>(Volumen gemessen bei Vorlauf temperatur: Vorlauf)         | 0000 1011                | 0B                   |

**Tabelle 13** (*fortgesetzt*)

| Gerätetyp (ehemals Medium)                                                                                    | Binärcode<br>Bit 7 ... 0 | Hexadezimal-<br>code |
|---------------------------------------------------------------------------------------------------------------|--------------------------|----------------------|
| Veraltet (zuvor Wärmeenergiezähler — Wärme) <sup>h</sup><br>(Volumen gemessen bei Vorlauftemperatur: Vorlauf) | 0000 1100                | 0C                   |
| Wärmeenergiezähler — Wärme und Kühlung kombiniert <sup>j</sup>                                                | 0000 1101                | 0D                   |
| Bestandteile des Busses/Systems                                                                               | 0000 1110                | 0E                   |
| Unbekannter Gerätetyp                                                                                         | 0000 1111                | 0F                   |
| Bewässerungswasserzähler <sup>d</sup>                                                                         | 0001 0000                | 10                   |
| Wasserdatenlogger                                                                                             | 0001 0001                | 11                   |
| Gasdatenlogger                                                                                                | 0001 0010                | 12                   |
| Gaskonverter                                                                                                  | 0001 0011                | 13                   |
| Wärmewert                                                                                                     | 0001 0100                | 14                   |
| Heißwasserzähler ( $\geq 90\text{ °C}$ ) <sup>d</sup>                                                         | 0001 0101                | 15                   |
| Kaltwasserzähler <sup>e</sup>                                                                                 | 0001 0110                | 16                   |
| Doppelregister-Wasserzähler (heiß/kalt) <sup>a,e</sup>                                                        | 0001 0111                | 17                   |
| Drucksensor                                                                                                   | 0001 1000                | 18                   |
| A/D-Umwandler                                                                                                 | 0001 1001                | 19                   |
| Rauchwarnmelder <sup>f</sup>                                                                                  | 0001 1010                | 1A                   |
| Raumsensor (z. B. Temperatur oder Feuchte)                                                                    | 0001 1011                | 1B                   |
| Veraltet (zuvor Gasmelder)                                                                                    | 0001 1100                | 1C                   |
| Kohlenstoffmonoxidwarnmelder <sup>f</sup>                                                                     | 0001 1101                | 1D                   |
| Hitzewarnmelder <sup>f</sup>                                                                                  | 0001 1110                | 1E                   |
| Sensorgerät <sup>g</sup>                                                                                      | 0001 1111                | 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 <sup>d</sup>                                                                                   | 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) <sup>b</sup>                                                                      | 0011 0110                | 36                   |

**Tabelle 13 (fortgesetzt)**

| Gerätetyp (ehemals Medium)               | Binärcode<br>Bit 7 ... 0 | Hexadezimal-<br>code |
|------------------------------------------|--------------------------|----------------------|
| Funkumsetzer (zählerseitig) <sup>c</sup> | 0011 0111                | 37                   |
| Busumsetzer (zählerseitig) <sup>c</sup>  | 0011 1000                | 38                   |
| Reserviert für Systemgeräte              | .....                    | 39 bis 3F            |
| Wärmeenergiezähler — Wärme               | 0100 0000                | 40                   |
| Wärmeenergiezähler — Kühlung             | 0100 0001                | 41                   |
| Reserviert                               | .....                    | 42 bis FE            |
| Platzhalter                              | 1111 1111                | FF                   |

<sup>a</sup> Ein derartiger Zähler erfasst den Wasserdurchfluss oberhalb einer Grenztemperatur in einem separaten Register mit einer entsprechenden Tarif-ID.

<sup>b</sup> Ein systemseitiger Funkumsetzer arbeitet als Funk-Master und Bus-Slave.

<sup>c</sup> Ein zählerseitiger Funkumsetzer arbeitet als Slave wie ein Zähler.

<sup>d</sup> Dieser Gerätetyp muss für nicht trinkbares Wasser/Industriewasser verwendet werden.

<sup>e</sup> Dieser Gerätetyp muss für Trinkwasser verwendet werden.

<sup>f</sup> Die übertragenen Daten werden zur Instandhaltung des Geräts verwendet, nicht für den Alarm selbst.

<sup>g</sup> Siehe EN 13757-3:2023<sup>1</sup>, 6.5.

<sup>h</sup> Wärmeenergiezähler – Wärme – müssen den Gerätetyp 40<sub>h</sub> verwenden.

<sup>i</sup> Wärmeenergiezähler – Kühlung – müssen den Gerätetyp 41<sub>h</sub> verwenden.

<sup>j</sup> Ein Wärmeenergiezähler, der sowohl Wärmeenergie als auch Kühlenergie messen kann, muss den Gerätetyp 0D<sub>h</sub> verwenden.  
Ein solcher Gerätetyp muss die orthogonale VIFE = E011 1100 (siehe EN13757-3:2023<sup>1</sup>, Tabelle 15) für Kühlenergie anwenden.

Ein FF<sub>h</sub> ist als Platzhalter zu interpretieren. Ein Platzhalter kann jeden Wert von 00<sub>h</sub> bis FE<sub>h</sub> ersetzen. 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.

Ein M-Bus-Gerät darf den Gerätetyp nicht ändern, da sich das die eindeutige M-Bus-Adresse des Geräts und möglicherweise auch auf die Verteilung der Sicherheitsschlüssel auswirkt.

## 7.5.5 Zugriffsnummer

### 7.5.5.1 Überblick

Die Zugriffsnummer ist Teil des TPL-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  $VIF = FD_{h,08h}$  (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, muss die Zugriffsnummer 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 Nachrichteninhalt 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 Zugriffsnummer 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. Zur Verwendung des FCB siehe CEN/TR 17167:2023<sup>1</sup>, A.7.

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. Bei einer wiederholten Anfrage (REQ-UD1 oder REQ-UD2 mit einem ungetoggelten FCB) wiederholt der Zähler die letzte Antwort mit der gleichen Zugriffsnummer. 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    | Permanenter Fehler          | Kein dauerhafter Fehler           |
| 2    | Energiereserve niedrig      | Energieversorgung in Ordnung      |
| 1, 0 | Siehe Tabelle 15            | Siehe Tabelle 15                  |

**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.<br><br>Der Zähler kann mithilfe des Anwendungsfehlerprotokolls in der nächsten Zählerantwort Einzelheiten über den aufgetretenen Anwendungsfehler zur Verfügung stellen (siehe EN 13757-3:2023 <sup>1</sup> , Abschnitt 10). |
| Ungewöhnlicher Zustand      | 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 EN 13757-3:2023<sup>1</sup>, 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.

ANMERKUNG Für weitere Angaben siehe CEN/TR 17167:2023<sup>1</sup>, Anhang D.

Im Fall von Umgebungsgeräuschen ist der RSSI jedoch 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 Mindestrauschabstand 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 darauffolgenden Bits festgelegt 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 bis 0 | 0 bis 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 bis 62:          | Der Empfangspegel wird als $-130 + (2 \times \text{RSSI-Wert})$ dBm berechnet.<br>Der Pegel liegt im Bereich –126 dBm bis –6 dBm. |
|      | 63:                | Der Empfangspegel liegt bei –4 dBm oder höher.                                                                                    |
|      |                    |                                                                                                                                   |

**Tabelle 17 (fortgesetzt)**

| Typ                         | Wert und Bedeutung |                                                                                                                            |
|-----------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------|
| Ver-<br>bindungs-<br>grenze | 0:                 | Keine Informationen zur Verbindungsgrenze vorhanden oder drahtgebundene Kommunikation.                                     |
|                             | 1:                 | Die Verbindungsgrenze liegt bei -10 dB oder weniger.                                                                       |
|                             | 2 bis 62:          | Die Verbindungsgrenze wird als (-11 + Verbindungsgrenzwert) dB berechnet.<br>Der Pegel liegt im Bereich -9 dBm bis +51 dB. |
|                             | 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);
- Anzahl, 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<br>15               | Bit<br>14                  | Bit<br>13                  | Bit<br>12             | Bit<br>11             | Bit<br>10             | Bit<br>9              | Bit<br>8              | Bit<br>7                   | Bit<br>6                   | Bit<br>5                   | Bit<br>4                   | Bit<br>3                   | Bit<br>2                   | Bit<br>1                   | LS Bit<br>0                |
|----------------------------|----------------------------|----------------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|
| Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch | Sicherheitsmodusbit 4 | Sicherheitsmodusbit 3 | Sicherheitsmodusbit 2 | Sicherheitsmodusbit 1 | Sicherheitsmodusbit 0 | Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch | Sicherheitsmodusspezifisch |
| 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 | Sicherheitsmodus Eigenschaften    | Verweisung                            |
|------------------|-----------------------------------|---------------------------------------|
| 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 <sup>a</sup>  | 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 <sup>a</sup>  | ANMERKUNG Siehe Literaturhinweis [8]. |
| 14               | Reserviert für zukünftige Nutzung | —                                     |
| 15               | Spezifische Nutzung <sup>a</sup>  | ANMERKUNG Siehe Literaturhinweis [7]. |
| 16–31            | Reserviert für zukünftige Nutzung | —                                     |

<sup>a</sup> Siehe Referenz in den Literaturhinweisen zur Verwendung dieses Modus zum Zeitpunkt der Veröffentlichung dieser Norm.

## 7.6 Konfigurationsfeldabhängige Struktur

### 7.6.1 Allgemeines

**Tabelle 20 — TPL-Struktur einer geschützten Nachricht**

|         | TPL-Header                              |                               |                             | APL                            |                                      | TPL-Trailer                 |
|---------|-----------------------------------------|-------------------------------|-----------------------------|--------------------------------|--------------------------------------|-----------------------------|
| CI-Feld | CI-abhängige Felder (siehe 7.3 und 7.4) | Konfigurationsfelderweiterung | Optionale TPL-Header-Felder | Verschlüsselte Anwendungsdaten | Nicht verschlüsselte Anwendungsdaten | Optionale TPL-Trailerfelder |

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 verschlüsselten 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 Längenangaben 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<sub>b</sub>), wird festgelegt, 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<sub>b</sub> gesetzt sind, folgen keine verschlüsselten Daten. Dies ist hilfreich, wenn die Nachricht unverschlüsselt, aber dennoch authentifiziert übertragen werden sollte.

Der Empfänger der Nachricht muss die Header-Struktur des angewandten Sicherheitsmodus für die korrekte Erkennung des unverschlüsselten Teils einer teilverschlüsselten Nachricht interpretieren.

**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 Sicherheitsmodusspezifische 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 (nach 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. Sicherheitsmodi, die diese Teilfelder nicht unterstützen, können diesen Dienst mithilfe einer ELL (siehe EN 13757-4) nutzen.

#### *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 $C_L$ | Inhalt der Nachricht                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------|
| 0                                                                                                                                                                                 | 0         | Normdatennachricht                                                                                                       |
| 0                                                                                                                                                                                 | 1         | Reserviert                                                                                                               |
| 1                                                                                                                                                                                 | 0         | Statische Nachricht (bestehend aus Parameter, OBIS-Definitionen und sonstigen Daten, die nicht häufig verändert werden). |
| 1                                                                                                                                                                                 | 1         | Reserviert für zukünftige Erweiterungen                                                                                  |
| ANMERKUNG Das Teilfeld CC darf nur für die Nachrichtentypen SND-NR und SND-IR (siehe EN 13757-4) angewandt werden. Alle anderen Zählernachrichtentypen müssen $CC = 00_b$ nutzen. |           |                                                                                                                          |

**Tabelle 22 — Inhalt der Partnernachricht**

| Bit $C_H$                                                                                                                                                                                    | Bit $C_L$ | Inhalt der Nachricht                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------------------------------|
| 0                                                                                                                                                                                            | 0         | Normbefehlsnachricht                    |
| 0                                                                                                                                                                                            | 1         | Reserviert                              |
| 1                                                                                                                                                                                            | 0         | Reserviert                              |
| 1                                                                                                                                                                                            | 1         | Reserviert für zukünftige Erweiterungen |
| ANMERKUNG Das Teilfeld CC darf nur für die Nachrichtentypen SND-UD, SND-UD2 und SND-UD3 (siehe EN 13757-4) angewandt werden. Alle anderen Partnernachrichtentypen müssen $CC = 00_b$ nutzen. |           |                                         |

#### *Teilfeld IIII: Inhaltsindex*

Dieses Feld wird verwendet, um zwischen Zählernachrichten mit unterschiedlichem Inhalt, aber mit demselben Inhaltsfeldwert „CC“ zu unterscheiden. Mit diesem Feld kann ein Empfänger Nachrichten 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 legt nicht den tatsächlichen Inhalt fest, das beste Vorgehen wäre jedoch die Nutzung des niedrigsten Wertes für die am häufigsten übertragenen Nachrichten. Tabelle 23 zeigt die Verwendung der Inhaltsindexbits.

**Tabelle 23 — Verwendung von Inhaltsindexbits**

| Inhaltsindex [III] (binär)                      | Inhalte der Nachricht                             |
|-------------------------------------------------|---------------------------------------------------|
| 0000                                            | Altzähler, keine weitere Nutzung des Inhaltsindex |
| 0001                                            | Daten für mobile Ablesung                         |
| 0010                                            | Daten für Ablesung im festen Netzwerk             |
| 0011                                            | Verbraucherinformationen                          |
| 0100 ... 0111                                   | Herstellerspezifischer Inhalt                     |
| 1000 ... 1111                                   | Reserviert <sup>a</sup>                           |
| <sup>a</sup> Gilt nicht für Sicherheitsmodus 7. |                                                   |

#### **Teilfelder B, A und S: Verbindungszugriffskontrolle**

Bit S wird zur Deklaration einer synchronen Übertragung verwendet. Wenn die Übertragungstaktung (vorher-sagbare 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.

Die Konfigurationsfeldbits A und B (Zugänglichkeit (en: Accessibility) und Bidirektionale Kommunikation) werden entsprechend Tabelle 24 zur Zugriffskontrolle für das Gerät, z. B. Zähler, Akteur oder Kommunikations-partner, verwendet.

**Tabelle 24 — Zugänglichkeit eines Geräts**

| Bit B | Bit A | Zugänglichkeit eines drahtlosen Geräts                                                                                    |
|-------|-------|---------------------------------------------------------------------------------------------------------------------------|
| 0     | 0     | Gerät stellt kein Zugriffsfenster bereit (unidirektionales Gerät)                                                         |
| 0     | 1     | Gerät unterstützt allgemein den bidirektionalen Zugriff, nach dieser Übertragung gibt es jedoch kein Zugriffsfenster mehr |
| 1     | 0     | Gerät stellt nur unmittelbar nach dieser Übertragung ein kurzes Zugriffsfenster bereit                                    |
| 1     | 1     | Gerät stellt unbegrenzten Zugriff bereit (mindestens bis zur nächsten Übertragung)                                        |

Der Kommunikationspartner signalisiert unbegrenzten Zugriff (letzte Zeile von Tabelle 24).

Sicherheitsmodi, die diese Teilfelder nicht unterstützen, können diesen Dienst mithilfe einer ELL (siehe EN 13757-4) nutzen.

Diese Bits sind für die drahtlose M-Bus-Kommunikation reserviert. Für die Kommunikation auf dem drahtge-bundenen 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 25 zeigt die Struktur der Schlüssel-ID-Liste.

**Tabelle 25 — 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 Schlüsselversionsfeld)**

Das Versionsbit (V) aktiviert das Schlüsselversionsfeld. Das Schlüsselversionsfeld ist nur dann im TPL-Header vorhanden (siehe 7.7.5 bis 7.7.8), wenn das Versionsbit gesetzt wurde. Das AFL.KI-Feld unterstützt auch ein Schlüsselversionsfeld (siehe 6.3.4). Wenn das Schlüsselversionsfeld vorhanden ist, identifiziert es die angewandte Version des Schlüssels mit der entsprechenden Schlüssel-ID.

Das Schlüsselversionsfeld wird verwendet, um Schlüssel mit derselben Schlüssel-ID (und demselben Zweck) zu unterscheiden. Ein neuer Schlüssel sollte eine höhere Versionsnummer als ein älterer Schlüssel besitzen. Eine gültige Schlüsselversion liegt im Bereich von 0 bis 254. Der Wert 0 wird vom Hersteller als Standardwert genutzt. Der Wert 255 signalisiert, dass das Schlüsselversionsfeld nicht verwendet wird.

Im Fall von abgeleiteten flüchtigen Schlüsseln muss die Schlüsselversion 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 26 zeigt die möglichen Werte dieses Teilfelds an.

**Tabelle 26 — KDF-Auswahl**

| KDF | D | D | Angewandte Schlüsselableitungsfunktion      |
|-----|---|---|---------------------------------------------|
| —   | 0 | 0 | persistenter Schlüssel <sup>a</sup>         |
| A   | 0 | 1 | Schlüsselableitungsfunktion A (siehe 9.6.1) |
| B   | 1 | 0 | Reserviert                                  |
| C   | 1 | 1 | Reserviert                                  |

<sup>a</sup> Keine Schlüsselableitung – gespeicherter Schlüssel wird direkt für die Verschlüsselung oder Authentifizierung verwendet.

### 7.7.2 Konfigurationsfeld des Sicherheitsmodus 0

Tabelle 27 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 0.

**Tabelle 27 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 0**

| Feldname | Konfig.feld (siehe Tabelle 28) | Nicht verschlüsselte Anwendungsdaten |
|----------|--------------------------------|--------------------------------------|
| Länge    | 2                              | ...                                  |

**Tabelle 28 — Definition des Konfigurationsfelds für den Sicherheitsmodus 0**

| MS Bit<br>15                 | Bit<br>14      | Bit<br>13      | Bit<br>12        | Bit<br>11        | Bit<br>10        | Bit<br>9         | Bit<br>8         | Bit<br>7   | Bit<br>6   | Bit<br>5   | Bit<br>4   | Bit<br>3             | Bit<br>2             | Bit<br>1         | LS Bit<br>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           |

0: Hop-Zähler „H“

— Dieses Bit ist festgelegt in 7.7.1.

Bit 1: Repeater-Zugriff „R“

— Dieses Bit ist festgelegt 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<sub>b</sub>

Bit 8 bis Bit 12: Sicherheitsmodus „MMMMM“

- Für die Spezifikation der Modi (siehe Tabelle 19)
- Modus 0 wird angegeben durch MMMMM = 00000<sub>b</sub>

Bit 13: Synchronisierungsbit „S“

- Dieses Bit ist festgelegt in 7.7.1.

Bit 14: Zugänglichkeits-Bit „A“

- Dieses Bit ist festgelegt in 7.7.1.

Bit 15: Bidirektionales Bit „B“

- Dieses Bit ist festgelegt in 7.7.1.

### 7.7.3 Konfigurationsfeld der Sicherheitsmodi 2 und 3

Tabelle 29 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle der Sicherheitsmodi 2 und 3.

**Tabelle 29 — Konfigurationsfeld und nachfolgende Felder mit den Sicherheitsmodi 2 und 3**

| Feldname | Konfig.feld (siehe Tabelle 30) | Verschlüsselte Anwendungsdaten | Nicht verschlüsselte Anwendungsdaten (optional) |
|----------|--------------------------------|--------------------------------|-------------------------------------------------|
| Länge    | 2                              | NNNNNNNN                       | ...                                             |

**Tabelle 30 — Definition des Konfigurationsfeldes für die Sicherheitsmodi 2 und 3**

| MS Bit<br>15 | Bit<br>14  | Bit<br>13  | Bit<br>12        | Bit<br>11        | Bit<br>10        | Bit<br>9         | Bit<br>8         | Bit<br>7                 | Bit<br>6                 | Bit<br>5                 | Bit<br>4                 | Bit<br>3                 | Bit<br>2                 | Bit<br>1                 | LS Bit<br>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 (z. B. NNNNNNNN = 00010000<sub>b</sub> 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 MMMM = 00010<sub>b</sub>
- Modus 3 wird angegeben durch MMMM = 00011<sub>b</sub>

Bit 13 bis Bit 15: Reserviert mit Wert gleich 0<sub>b</sub>

Siehe 9.4.3 für Einzelheiten über diese Sicherheitsmodi.

#### **7.7.4 Konfigurationsfeld des Sicherheitsmodus 5**

Tabelle 31 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 5.

**Tabelle 31 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 5**

| Feldname | Konfig.feld (siehe Tabelle 32) | Entschlüsselungs-verifizierung (verschlüsselt) | Verschlüsselte Anwendungsdaten | Nicht verschlüsselte Anwendungsdaten (optional) |
|----------|--------------------------------|------------------------------------------------|--------------------------------|-------------------------------------------------|
| Länge    | 2                              | 2                                              | 16*NNNN – 2                    | ...                                             |

**Tabelle 32 — Definition des Konfigurationsfelds für den Sicherheitsmodus 5**

| MS Bit                       | Bit            | Bit            | Bit              | Bit              | Bit              | Bit              | Bit              | Bit                        | Bit                        | Bit                        | Bit                        | Bit                  | Bit                  | Bit              | LS Bit     |
|------------------------------|----------------|----------------|------------------|------------------|------------------|------------------|------------------|----------------------------|----------------------------|----------------------------|----------------------------|----------------------|----------------------|------------------|------------|
| 15                           | 14             | 13             | 12               | 11               | 10               | 9                | 8                | 7                          | 6                          | 5                          | 4                          | 3                    | 2                    | 1                | 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 festgelegt in 7.7.1.

Bit 1: Repeater-Zugriff „R“

- Dieses Bit ist festgelegt in 7.7.1.

Bit 2 bis Bit 3: Inhalt der Nachricht „CC“

- Diese Bits sind festgelegt 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 (z. B. NNNN = 0010<sub>b</sub> 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 MMMM = 00101<sub>b</sub>

Bit 13: Synchronisierungsbit „S“

- Dieses Bit ist festgelegt in 7.7.1.

Bit 14: Zugänglichkeits-Bit „A“

- Dieses Bit ist festgelegt in 7.7.1.

Bit 15: Bidirektionales Bit „B“

- Dieses Bit ist festgelegt in 7.7.1.

Siehe 9.4.4 für Einzelheiten über diese Sicherheitsmodi.

### 7.7.5 Konfigurationsfeld des Sicherheitsmodus 7

Tabelle 33 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 7.

**Tabelle 33 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 7**

| <b>Feld-name</b> | Konfig.feld<br>(siehe<br>Tabelle 34) | Konfig.feld-<br>erweite-<br>rung<br>(siehe<br>Tabelle 35) | Schlüs-<br>selver-<br>sion<br>(optio-<br>nal) | Nach-<br>richten-<br>zähler<br>(optio-<br>nal) | Entschlüs-<br>sungsverifizie-<br>rung<br>(verschlüs-<br>selt) | Ver-<br>schlüsselte<br>Anwen-<br>dungsdaten | TPL-<br>Füllung<br>(optio-<br>nal) | Nicht ver-<br>schlüsselte<br>Anwen-<br>dungsdaten<br>(optional) |
|------------------|--------------------------------------|-----------------------------------------------------------|-----------------------------------------------|------------------------------------------------|---------------------------------------------------------------|---------------------------------------------|------------------------------------|-----------------------------------------------------------------|
| <b>Länge</b>     | 2                                    | 1                                                         | (1)                                           | (4)                                            | 2                                                             | 16*NNNN – 2                                 | (1 bis 16)                         | ...                                                             |

**Tabelle 34 — Definition des Konfigurationsfelds für den Sicherheitsmodus 7**

| <b>MS<br/>Bit<br/>15</b> | <b>Bit<br/>14</b>    | <b>Bit<br/>13</b> | <b>Bit<br/>12</b> | <b>Bit<br/>11</b> | <b>Bit<br/>10</b> | <b>Bit<br/>9</b> | <b>Bit<br/>8</b> | <b>Bit<br/>7</b>           | <b>Bit<br/>6</b>           | <b>Bit<br/>5</b>           | <b>Bit<br/>4</b>           | <b>Bit<br/>3</b> | <b>Bit<br/>2</b> | <b>Bit<br/>1</b> | <b>LS<br/>Bit<br/>0</b> |
|--------------------------|----------------------|-------------------|-------------------|-------------------|-------------------|------------------|------------------|----------------------------|----------------------------|----------------------------|----------------------------|------------------|------------------|------------------|-------------------------|
| 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 | Füllmaterial     | Inhaltsindex     | Inhaltsindex     | Inhaltsindex            |
| C                        | C                    | Z                 | M                 | M                 | M                 | M                | M                | N                          | N                          | N                          | N                          | P                | I                | I                | I                       |

Bit 0 bis Bit 2: Inhaltsindex „III“

- Inhaltsindex wie in 7.7.1 festgelegt, mit einer Begrenzung des maximalen Inhaltsindexwerts = 7.

Bit 3: Füllung „P“

- Dieses Bit definiert das Vorhandensein des Felds TPL-Füllung.
- Füllungsbit entspricht  $0_b$ : Das Feld TPL-Füllung ist nicht vorhanden (0 Byte)
- Füllungsbit entspricht  $1_b$ : Das Feld TPL-Füllung ist vorhanden (1 bis 16 Bytes nach 9.4.5.4).

ANMERKUNG Die Größe des Felds TPL-Füllung wird vom Feld selbst definiert.

Bit 4 bis Bit 7: Länge „NNNN“

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

Bit 8 bis Bit 12: Sicherheitsmodus „MMMM“

- 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 Bytes (vorhanden).

Bit 14 bis Bit 15: Inhalt der Nachricht „CC“

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

**Tabelle 35 — 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 25 festgelegt (siehe 7.7.1).

Bit 4 bis Bit 5: KDF-Auswahl „DD“

- Selektor für die Schlüsselabweichungsfunktion, wie in Tabelle 26 festgelegt (siehe 7.7.1).

Bit 6: Version „V“

- Versionsbit entspricht  $0_b$ : Das Feld Schlüsselversion ist nicht vorhanden (0 Byte).
- Versionsbit entspricht  $1_b$ : Das Feld Schlüsselversion ist vorhanden (1 Byte) (siehe 7.7.1).

Bit 7: Reserviert mit Wert gleich 0<sub>b</sub>

Siehe 9.4.5 für Einzelheiten über diesen Sicherheitsmodus.

### 7.7.6 Konfigurationsfeld des Sicherheitsmodus 8

Tabelle 36 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 8.

**Tabelle 36 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 8**

| Feldname | Konfig.feld<br>(siehe Tabelle 37) | Konfig.felderweiterung<br>(optional)<br>(siehe Tabelle 38) | Schlüsselversion<br>(optional) | Länge [E]<br>(optional) | Nachrichtenzähler | Verschlüsselte Anwendungsdaten | Nicht verschlüsselte Anwendungsdaten (optional) | Authentifizierungs-Tag 1 | Übertragungszeitstempel<br>(optional) | Authentifizierungs-Tag 2<br>(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 37 — Definition des Konfigurationsfelds für Modus 8**

| MS<br>Bit<br>15 | Bit<br>14   | Bit<br>13   | Bit<br>12        | Bit<br>11        | Bit<br>10        | Bit<br>9         | Bit<br>8         | Bit<br>7  | Bit<br>6                                             | Bit<br>5    | Bit<br>4    | Bit<br>3     | Bit<br>2     | Bit<br>1     | LS<br>Bit<br>0 |
|-----------------|-------------|-------------|------------------|------------------|------------------|------------------|------------------|-----------|------------------------------------------------------|-------------|-------------|--------------|--------------|--------------|----------------|
| CPE             | KDF-Auswahl | KDF-Auswahl | Sicherheitsmodus | Sicherheitsmodus | Sicherheitsmodus | Sicherheitsmodus | Sicherheitsmodus | Len E Bit | Authentifizierungs-Tag 2 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 25 festgelegt (siehe 7.7.1)

Bit 4 bis Bit 5: Zählergröße „ZZ“

- Zählergrößenbits entsprechen 00<sub>b</sub>: reserviert
- Zählergrößenbits entsprechen 01<sub>b</sub>: Das nachfolgende Zählerfeld ist 2 Bytes groß
- Zählergrößenbits entsprechen 10<sub>b</sub>: Das nachfolgende Zählerfeld ist 3 Bytes groß
- Zählergrößenbits entsprechen 11<sub>b</sub>: Das nachfolgende Zählerfeld ist 4 Bytes groß

Bit 6: Authentifizierungs-Tag 2 und Übertragungszeitstempel „O“

- Bit Authentifizierungs-Tag 2 und Übertragungszeitstempel entsprechen 0<sub>b</sub>: Das Authentifizierungs-Tag 2 und der Übertragungszeitstempel sind nicht vorhanden (0 Byte).
- Bit Authentifizierungs-Tag 2 und Übertragungszeitstempel entsprechen 1<sub>b</sub>: 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<sub>b</sub>: Das Feld Länge [E] ist nicht vorhanden (0 Byte). (Es sind keine unverschlüsselten Anwendungsdaten nach den verschlüsselten Anwendungsdaten vorhanden.)
- Len E Bit entspricht 1<sub>b</sub>: 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<sub>b</sub>

Bit 13 bis Bit 14: KDF-Auswahl „DD“

- Selektor für die Schlüsselabweichungsfunktion, wie in Tabelle 26 festgelegt (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 36.

**Tabelle 38 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 8**

| MSBit 7      | Bit 6        | Bit 5        | Bit 4        | Bit 3          | Bit 2   | Bit 1                | LSBit 0              |
|--------------|--------------|--------------|--------------|----------------|---------|----------------------|----------------------|
| Inhaltsindex | Inhaltsindex | Inhaltsindex | Inhaltsindex | Reserviert     | Version | Inhalt der Nachricht | Inhalt der Nachricht |
| I            | I            | I            | I            | 0 <sub>b</sub> | V       | C                    | C                    |

Bit 0 bis Bit 1: Inhalt der Nachricht „CC“

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

Bit 2: Version „V“

- Versionsbit entspricht 0<sub>b</sub>: Das Feld Schlüsselversion ist nicht vorhanden (0 Byte).
- Versionsbit entspricht 1<sub>b</sub>: Das Feld Schlüsselversion ist vorhanden (1 Byte) (siehe 7.7.1).

Bit 3: Reserviert mit Wert gleich 0

Bit 4 bis Bit 7: Inhaltsindex „IIII“

- Inhaltsindex wie festgelegt in 7.7.1.

Nachrichtenzählerfeld:

- Siehe 9.2.

Authentifizierungs-Tag 1:

- Für die Spezifikation des Authentifizierungs-Tags 1, siehe 9.4.6.3.

Übertragungszeitstempel:

- Der optionale Übertragungszeitstempel zeigt das Übertragungsdatum/die Übertragungsuhrzeit der Nachricht durch den Zähler oder den Kommunikationspartner an. Dieser Übertragungszeitstempel stellt nicht den Zeitpunkt der Datenerfassung dar. Er muss aktualisiert werden, wenn dieselbe Kapazität mehrmals übertragen wird. Dies bietet Schutz vor einem Replay-Angriff. Format: Datum in Sekunden (wie UNIX EPOCH) seit 1. Januar 2013 um 00:00, kodiert mit 3 Bytes. Der Höchstwert ist FFFFFFF<sub>h</sub>.

BEISPIEL    Kodierung am 1. Februar 2015 um 02:00

- Anzahl an Sekunden seit 1. Januar 2013 um 00:00 = 65 757 600 s
- Umwandlung in Hexadezimalzahlen: 3EB61A0<sub>h</sub>
- Wert des Übertragungszeitstempel: EB61A0<sub>h</sub>, d. h. 15 425 952 s

Authentifizierungs-Tag 2:

- Für die Spezifikation des Authentifizierungs-Tags 2, siehe 9.4.6.3.

### 7.7.7 Konfigurationsfeld des Sicherheitsmodus 9

Tabelle 39 zeigt die Nachrichtenstruktur hinter (und einschließlich) dem Konfigurationsfeld im Falle des Sicherheitsmodus 9.

**Tabelle 39 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 9**

| Feldname | Konfig.feld (siehe Tabelle 30) | Schlüsselversion (optional) | Länge (E) | Länge (U) | Nachrichtenzähler | Verschlüsselte Anwendungsdaten | Nicht verschlüsselte Anwendungsdaten (optional) | Authentifizierungs-Tag (optional) |
|----------|--------------------------------|-----------------------------|-----------|-----------|-------------------|--------------------------------|-------------------------------------------------|-----------------------------------|
| Länge    | 2                              | (1)                         | 1 oder 2  | 1 oder 2  | 4                 | Länge (E)                      | Länge (U)                                       | 12                                |

ANMERKUNG    Das Authentifizierungs-Tag befindet sich am Ende der Nachricht.

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

**Tabelle 40 — Definition des Konfigurationsfelds für den Sicherheitsmodus 9**

| MS<br>Bit<br>15                  | Bit<br>14 | Bit<br>13                         | Bit<br>12        | Bit<br>11        | Bit<br>10        | Bit 9            | Bit 8            | Bit 7     | Bit 6     | Bit 5       | Bit 4       | Bit 3        | Bit 2        | Bit 1        | LS<br>Bit 0  |
|----------------------------------|-----------|-----------------------------------|------------------|------------------|------------------|------------------|------------------|-----------|-----------|-------------|-------------|--------------|--------------|--------------|--------------|
| Reserviert für Felderweiterungen | Version   | Größe des Authentifizierungs-Tags | Sicherheitsmodus | Sicherheitsmodus | Sicherheitsmodus | Sicherheitsmodus | Sicherheitsmodus | Len U Bit | Len E Bit | KDF-Auswahl | KDF-Auswahl | Schlüssel-ID | Schlüssel-ID | Schlüssel-ID | Schlüssel-ID |
| 0 <sub>b</sub>                   | V         | O                                 | M                | M                | M                | M                | M                | U         | E         | D           | D           | K            | K            | K            | K            |

Bit 0 bis Bit 3: Schlüssel-ID „KKKK“

- Schlüssel-ID, wie in Tabelle 25 festgelegt (siehe 7.7.1)

Bit 4 bis Bit 5: KDF-Auswahl „DD“

- Selektor für die Schlüsselauswahlfunktion, wie in Tabelle 26 festgelegt (siehe 7.7.1)

Bit 6: Len E Bit „E“

- Len E Bit entspricht 0<sub>b</sub>: Das Feld Länge (E) ist ein Byte mit vorzeichenlosem Integer (Dies ermöglicht eine maximale Länge von 255 Bytes an verschlüsselten Anwendungsdaten)
- Len E Bit entspricht 1<sub>b</sub>: Das Feld Länge (E) ist zwei Bytes mit vorzeichenlosem Integer (Dies ermöglicht eine maximale Länge von 65 535 Bytes an unverschlüsselten Anwendungsdaten)

Bit 7: Len U Bit „U“

- Len U Bit entspricht 0<sub>b</sub>: Das Feld Länge (U) ist ein Byte mit vorzeichenlosem Integer (Dies ermöglicht eine maximale Länge von 255 Bytes an unverschlüsselten Anwendungsdaten)
- Len U Bit entspricht 1<sub>b</sub>: Das Feld Länge (U) ist zwei Bytes mit vorzeichenlosem Integer (Dies ermöglicht eine maximale Länge von 65 535 Bytes an unverschlüsselten Anwendungsdaten)

Bit 8 bis Bit 12: Sicherheitsmodus „MMMM“

- Für die Spezifikation der Sicherheitsmodi (siehe Tabelle 19)
- Modus 9 wird angegeben durch MMMMM = 01001<sub>b</sub>

Bit 13: Größe des Authentifizierungs-Tags „O“

- Größenbit des Authentifizierungs-Tags entspricht 0<sub>b</sub>: Authentifizierungs-Tag ist 0 Byte (nicht vorhanden)
- Größenbit des Authentifizierungs-Tags entspricht 1<sub>b</sub>: Authentifizierungs-Tag ist 12 Bytes (vorhanden)