

DIN EN 13757-7:2025-10 (D)

Kommunikationssysteme für Zähler - Teil 7: Transport- und Sicherheitsdienste; Deutsche Fassung EN 13757-7:2025

Inhalt	Seite
Europäisches Vorwort.....	10
Einleitung	12
1 Anwendungsbereich.....	14
2 Normative Verweisungen	14
3 Begriffe	14
4 Abkürzungen und Symbole	17
4.1 Abkürzungen	17
4.2 Symbole	20
5 Schichtmodell	20
5.1 M-Bus-Schichten	20
5.2 Das CI-Feld-Prinzip	21
6 Authentifizierungs- und Fragmentierungs-Teilschicht (AFL)	27
6.1 Einleitung.....	27
6.2 Übersicht über die AFL-Struktur	28
6.3 Komponenten der AFL.....	28
6.3.1 AFL-Längelfeld (AFL.AFLL).....	28
6.3.2 AFL-Fragmentierungskontrollfeld (AFL.FCL).....	28
6.3.3 AFL-Nachrichtenkontrollfeld (AFL.MCL)	29
6.3.4 AFL-Schlüsselinformationfeld (AFL.KI).....	30
6.3.5 AFL-Nachrichtenzählerfeld (AFL.MCR)	31
6.3.6 AFL-MAC-Feld (AFL.MAC).....	31
6.3.7 AFL-Nachrichtelängelfeld (AFL.ML).....	31
7 Transportschicht (TPL)	32
7.1 Einleitung.....	32
7.2 Struktur ohne TPL-Header.....	32
7.3 Struktur mit kurzem TPL-Header	32
7.4 Struktur mit langem TPL-Header.....	33
7.5 CI-Feld-abhängige Elemente	33
7.5.1 Identifikationsnummer	33
7.5.2 Identifikation des Herstellers	34
7.5.3 Versionsidentifikation.....	34
7.5.4 Identifikation des Gerätetyps.....	34
7.5.5 Zugriffsnummer	37
7.5.6 Statusbyte in Zählernachrichten	38
7.5.7 Statusbyte in Partnernachrichten.....	39
7.5.8 Konfigurationsfeld	41
7.6 Konfigurationsfeldabhängige Struktur	42
7.6.1 Allgemeines	42
7.6.2 Konfigurationsfelderweiterung.....	43
7.6.3 Optionale TPL-Header-Felder	43
7.6.4 Optionale TPL-Trailer-Felder.....	43
7.6.5 Teilverschlüsselung.....	43
7.7 Security Mode spezifische TPL-Felder	44
7.7.1 Gemeinsame Teilfelder des Konfigurationsfelds und der Konfigurationsfelderweiterung.....	44

7.7.2	Konfigurationsfeld des Security Mode 0.....	47
7.7.3	Konfigurationsfeld der Sicherheitsmodi 2 und 3.....	48
7.7.4	Konfigurationsfeld des Security Mode 5.....	49
7.7.5	Konfigurationsfeld des Security Mode 7.....	51
7.7.6	Konfigurationsfeld des Security Mode 8.....	53
7.7.7	Konfigurationsfeld des Security Mode 9.....	56
7.7.8	Konfigurationsfeld des Security Mode 10.....	57
8	Verwaltung der unteren Schichten.....	60
8.1	Allgemeines.....	60
8.2	Setzen der Baudrate für die M-Bus-Verbindungsschicht nach EN 13757-2.....	60
8.3	Adressstruktur bei Verwendung zusammen mit der drahtlosen Sicherungsschicht nach EN 13757-4.....	60
8.4	Selektion und Sekundäradressierung.....	60
8.5	Generalisiertes Selektionsverfahren.....	61
8.6	Suche nach installierten Slaves.....	62
8.6.1	Primäradressen.....	62
8.6.2	Sekundäradressen.....	63
8.6.3	Verfahren der Platzhaltersuche.....	63
9	Sicherheitsdienste.....	63
9.1	Allgemeines.....	63
9.2	Nachrichtenzähler.....	65
9.2.1	Überblick.....	65
9.2.2	Nachrichtenzähler C_M , der vom Zähler übertragen wird.....	65
9.2.3	Nachrichtenzähler C_{CP} , der vom Kommunikationspartner übertragen wird.....	66
9.2.4	Nachrichtenzähler C'_{CP} , der vom Zähler erhalten wird.....	66
9.2.5	Nachrichtenzähler C'_M und C''_M , die vom Kommunikationspartner empfangen werden.....	66
9.3	Authentifizierungsverfahren in der AFL.....	67
9.3.1	Überblick.....	67
9.3.2	Authentifizierungsverfahren AES-CMAC-128.....	67
9.3.3	Authentifizierungsverfahren AES-GMAC-128.....	68
9.4	Verschlüsselungs- und Authentifizierungsverfahren in der TPL.....	69
9.4.1	Überblick über TPL-Schutzmechanismen.....	69
9.4.2	Herstellerspezifischer Schutzmechanismus (Security Mode 1).....	71
9.4.3	Schutzmechanismus DES-CBC (Security Mode 2 und 3).....	71
9.4.4	Schutzmechanismus AES-CBC-128 (Security Mode 5).....	72
9.4.5	Schutzmechanismus AES-CBC-128 (Security Mode 7).....	73
9.4.6	Schutzmechanismus AES-CTR-128 (Security Mode 8).....	74
9.4.7	Schutzmechanismus AES-GCM-128 (Security Mode 9).....	76
9.4.8	Schutzmechanismus AES-CCM-128 (Security Mode 10).....	80
9.5	Reaktion auf ein Sicherheitsversagen.....	82
9.6	Schlüsselableitung.....	83
9.6.1	Allgemeines.....	83
9.6.2	Schlüsselableitungsfunktion A.....	83
9.7	Schlüsselaustausch.....	84
	Anhang A (normativ) Übertragungsprotokoll für Sicherheitsinformationen.....	85
A.1	Einleitung.....	85
A.2	SITP-Dienste.....	85
A.2.1	Sicherheitsinformationen übertragen.....	85
A.2.2	Sicherheitsinformationen aktivieren.....	86
A.2.3	Sicherheitsinformationen deaktivieren.....	86
A.2.4	Sicherheitsinformationen zerstören.....	86
A.2.5	Kombinierte Aktivierung/Deaktivierung von Sicherheitsinformationen.....	86
A.2.6	Sicherheitsinformationen erzeugen.....	86
A.2.7	Sicherheitsinformationen erhalten.....	86
A.2.8	Liste aller Schlüsselinformation erhalten.....	87
A.2.9	Liste der aktiven Schlüsselinformation erhalten.....	87

A.2.10	Liste der aktiven Schlüssel- und Schlüsselzählerinformation erhalten	87
A.2.11	Von Ende zu Ende gesicherte Anwendungsdaten übertragen	87
A.3	CI-Felder	87
A.4	SITP-Struktur	87
A.5	Blockkontrollfeld	88
A.6	Blockparameter	89
A.7	Überblick über Datenstrukturen/Mechanismen	90
A.8	Datenstrukturen für Sicherheitsinformationen.....	92
A.8.1	Allgemeines.....	92
A.8.2	Datenstruktur 00 _h	92
A.8.3	Datenstruktur 01 _h	92
A.8.4	Datenstruktur 02 _h	93
A.8.5	Datenstruktur 03 _h	94
A.8.6	Datenstruktur 20 _h	95
A.8.7	Datenstruktur 21 _h	96
A.8.8	Datenstruktur 22 _h	96
A.8.9	Datenstruktur 23 _h	97
A.9	Datenstrukturen für gesicherte Anwendungsdaten	98
A.9.1	Allgemeines	98
A.9.2	Datenstruktur 30 _h — AES-Schlüssel-Wrap.....	100
A.9.3	Datenstruktur 31 _h — HMAC-SHA256.....	100
A.9.4	Datenstruktur 32 _h und 33 _h — CMAC	100
A.9.5	Datenstruktur 34 _h — AES-GCM	101
A.9.6	Datenstruktur 35 _h — AES-GMAC	103
A.9.7	Datenstruktur 36 _h und 37 _h — AES-CCM	104
Anhang B (informativ) Beispiel für einen Nachrichtenzähler.....		106
Literaturhinweise		110

Bilder

Bild 1	— Eingabe und Ausgabe für den GCM-Algorithmus	77
Bild B.1	— Kontrollfluss des Nachrichtenzählers (Teil 1)	107
Bild B.2	— Kontrollfluss des Nachrichtenzählers (Teil 2)	109

Tabellen

Tabelle 1	— Reihenfolge der M-Bus-Schicht	21
Tabelle 2	— Codes des CI-Felds	22
Tabelle 3	— Übersicht über alle AFL-Felder	28
Tabelle 4	— AFL-Fragmentierungskontrollfeld — Definitionen der Bitfelder	29
Tabelle 5	— AFL-Nachrichtenkontrollfeld — Definitionen der Bitfelder	29
Tabelle 6	— AT-Teilfeld von AFL.MCL	30
Tabelle 7	— AFL-Schlüsselinformationfeld — Definitionen der Bitfelder	30
Tabelle 8	— AFL-Nachrichtenzählerfeld — Definitionen der Bitfelder.....	31

Tabelle 9 — AFL-Nachrichtenlängelfeld — Definitionen der Bitfelder.....	31
Tabelle 10 — Allgemeine Struktur der TPL	32
Tabelle 11 — Kurzer TPL-Header	33
Tabelle 12 — Langer TPL-Header.....	33
Tabelle 13 — Identifikation des Gerätetyps	34
Tabelle 14 — Kodierung des Statusfelds.....	38
Tabelle 15 — Mit dem Statusfeld kodierte Anwendungsfehler	38
Tabelle 16 — Bedeutung des Statusbytes für Partnernachrichten	40
Tabelle 17 — Bedeutung der Bits 0 bis 5 im Statusbyte für Partnernachrichten	40
Tabelle 18 — Allgemeine Definition der zwei obligatorischen Konfigurationsfeldbytes.....	41
Tabelle 19 — Definition der Modusbits im Konfigurationsfeld (Sicherheitsmodus)	41
Tabelle 20 — TPL-Struktur einer geschützten Nachricht.....	42
Tabelle 21 — Inhalt der Zählernachricht.....	44
Tabelle 22 — Inhalt der Partnernachricht	44
Tabelle 23 — Verwendung von Inhaltsindexbits	45
Tabelle 24 — Zugänglichkeit eines Geräts	45
Tabelle 25 — Schlüssel-ID.....	46
Tabelle 26 — KDF-Auswahl	47
Tabelle 27 — Konfigurationsfeld und nachfolgende Felder mit dem Security Mode 0	47
Tabelle 28 — Definition des Konfigurationsfelds für den Security Mode 0.....	47
Tabelle 29 — Konfigurationsfeld und nachfolgende Felder mit den Sicherheitsmodi 2 und 3	48
Tabelle 30 — Definition des Konfigurationsfeldes für die Sicherheitsmodi 2 und 3	49
Tabelle 31 — Konfigurationsfeld und nachfolgende Felder mit dem Security Mode 5	49
Tabelle 32 — Definition des Konfigurationsfelds für den Security Mode 5.....	50
Tabelle 33 — Konfigurationsfeld und nachfolgende Felder mit dem Security Mode 7	51
Tabelle 34 — Definition des Konfigurationsfelds für den Security Mode 7.....	51
Tabelle 35 — Definition der Konfigurationsfelderweiterung für den Security Mode 7	52
Tabelle 36 — Konfigurationsfeld und nachfolgende Felder mit dem Security Mode 8	53
Tabelle 37 — Definition des Konfigurationsfelds für Modus 8.....	53

Tabelle 38 — Definition der Konfigurationsfelderweiterung für den Security Mode 8	55
Tabelle 39 — Konfigurationsfeld und nachfolgende Felder mit dem Security Mode 9.....	56
Tabelle 40 — Definition des Konfigurationsfelds für den Security Mode 9.....	56
Tabelle 41 — Konfigurationsfeld und nachfolgende Felder mit dem Security Mode 10	58
Tabelle 42 — Definition des Konfigurationsfelds für den Security Mode 10	58
Tabelle 43 — Definition der Konfigurationsfelderweiterung für den Security Mode 10.....	59
Tabelle 44 — Adressstruktur der Verbindungsschicht für Funk.....	60
Tabelle 45 — Struktur eines Datagramms für die Selektion eines Slaves.....	61
Tabelle 46 — Anwendungsschichtstruktur eines Datagramms für die erweiterte Selektion	62
Tabelle 47 — Sicherheitsdienste und Sicherheitsziele.....	64
Tabelle 48 — Schutzmechanismen für die Ablesung des Zählers	70
Tabelle 49 — Initialisierungsvektor des Security Mode 5.....	72
Tabelle 50 — Struktur des Initialisierungsvektors in Security Mode 8	76
Tabelle 51 — Eingabe- und Ausgabeinformationen für die GCM-Funktionen	77
Tabelle 52 — Struktur des Initialisierungsvektors in Security Mode 9	79
Tabelle 53 — Struktur der Nonce N	81
Tabelle 54 — Konstante DC für die Schlüsselableitung.....	83
Tabelle A.1 — CI-Felder des Übertragungsprotokolls für Sicherheitsinformationen	87
Tabelle A.2 — Interne Blockstruktur des SITP.....	88
Tabelle A.3 — Blockkontrollfeld.....	88
Tabelle A.4 — Blockparameterstruktur	89
Tabelle A.5 — Liste der SITP-Datenstrukturen/Mechanismen	90
Tabelle A.6 — DSH-Inhalt von DSI 00 _h	92
Tabelle A.7 — Wrapped-Datenstruktur 01 _h	93
Tabelle A.8 — Wrapped-Datenstruktur 02 _h	93
Tabelle A.9 — Wrapped-Datenstruktur 03 _h	94
Tabelle A.10 — Optionen für Wrapped-Datenstruktur 03 _h	95
Tabelle A.11 — Wrapped-Datenstruktur 20 _h für alle Schlüssel	95
Tabelle A.12 — Datenstruktur 21 _h für aktiven Schlüssel.....	96

Tabelle A.13 — Statusantwortstruktur	96
Tabelle A.14 — Definition des Statusantwortbytes.....	96
Tabelle A.15 — Datenstruktur 23_h für aktiven Schlüsselzähler.....	98
Tabelle A.16 — Liste der unterstützten PIDs.....	99
Tabelle A.17 — Datenstruktur 31_h.....	100
Tabelle A.18 — Auswahl von Datenstruktur 32_h und 33_h.....	101
Tabelle A.19 — Datenstruktur 32_h und 33_h.....	101
Tabelle A.20 — Datenstruktur 34_h.....	102
Tabelle A.21 — Struktur von IV bei AES-GCM.....	102
Tabelle A.22 — Datenstruktur 35_h.....	103
Tabelle A.23 — Struktur von IV bei AES-GMAC.....	104
Tabelle A.24 — Auswahl von Datenstruktur 36_h und 37_h.....	104
Tabelle A.25 — Wrapped-Datenstruktur 36_h und 37_h.....	104
Tabelle A.26 — Struktur der CCM-Nonce bei AES-GMAC.....	105