

E DIN EN 13757-7:2023-08 (D/E)

Erscheinungsdatum: 2023-07-14

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

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)	26
6.1 Einleitung	26
6.2 Übersicht über die AFL-Struktur	27
6.3 Komponenten der AFL	27
6.3.1 AFL-Längenfeld (AFL.AFL.L)	27
6.3.2 AFL-Fragmentierungskontrollfeld (AFL.FCL)	27
6.3.3 AFL-Nachrichtenkontrollfeld (AFL.MCL)	28
6.3.4 AFL-Schlüsselinformationsfeld (AFL.KI)	29
6.3.5 AFL-Nachrichtenzählerfeld (AFL.MCR)	30
6.3.6 AFL-MAC-Feld (AFL.MAC)	30
6.3.7 AFL-Nachrichtenlängenfeld (AFL.ML)	30
7 Transportschicht (TPL)	31
7.1 Einleitung	31
7.2 Struktur ohne TPL-Header	31
7.3 Struktur mit kurzem TPL-Header	31
7.4 Struktur mit langem TPL-Header	32
7.5 CI-Feld-abhängige Elemente	32
7.5.1 Identifikationsnummer	32
7.5.2 Identifikation des Herstellers	33
7.5.3 Versionsidentifikation	33
7.5.4 Identifikation des Gerätetyps	33
7.5.5 Zugriffsnummer	35
7.5.6 Statusbyte in Zählernachrichten	37
7.5.7 Statusbyte in Partnernachrichten	38
7.5.8 Konfigurationsfeld	39
7.6 Konfigurationsfeldabhängige Struktur	41
7.6.1 Allgemeines	41
7.6.2 Konfigurationsfelderweiterung	42
7.6.3 Optionale TPL-Header-Felder	42

7.6.4	Optionale TPL-Trailer-Felder.....	42
7.6.5	Teilverschlüsselung.....	42
7.7	Sicherheitsmodusspezifische TPL-Felder	43
7.7.1	Gemeinsame Teilfelder des Konfigurationsfelds und der Konfigurationsfelderweiterung.....	43
7.7.2	Konfigurationsfeld des Sicherheitsmodus 0	46
7.7.3	Konfigurationsfeld der Sicherheitsmodi 2 und 3.....	47
7.7.4	Konfigurationsfeld des Sicherheitsmodus 5	48
7.7.5	Konfigurationsfeld des Sicherheitsmodus 7	50
7.7.6	Konfigurationsfeld des Sicherheitsmodus 8	52
7.7.7	Konfigurationsfeld des Sicherheitsmodus 9	55
7.7.8	Konfigurationsfeld des Sicherheitsmodus 10	56
8	Verwaltung der unteren Schichten.....	59
8.1	Allgemeines.....	59
8.2	Setzen der Baudrate für die M-Bus-Verbindungsschicht nach EN 13757-2	59
8.3	Adressstruktur bei Verwendung zusammen mit der drahtlosen Datenverbindungsschicht nach EN 13757-4	59
8.4	Selektion und Sekundäradressierung.....	59
8.5	Generalisiertes Selektionsverfahren.....	60
8.6	Suche nach installierten Slaves.....	61
8.6.1	Primäradressen	61
8.6.2	Sekundäradressen	62
8.6.3	Verfahren der Platzhaltersuche	62
9	Sicherheitsdienste	62
9.1	Allgemeines.....	62
9.2	Nachrichtenzähler	64
9.2.1	Überblick.....	64
9.2.2	Nachrichtenzähler C_M , der vom Zähler übertragen wird	64
9.2.3	Nachrichtenzähler C_{CP} , der vom Kommunikationspartner übertragen wird	65
9.2.4	Nachrichtenzähler C'_{CP} , der vom Zähler erhalten wird	65
9.2.5	Nachrichtenzähler C'_M und C''_M , die vom Kommunikationspartner empfangen werden.....	65
9.3	Authentifizierungsverfahren in der AFL.....	66
9.3.1	Überblick.....	66
9.3.2	Authentifizierungsverfahren AES-CMAC-128	66
9.3.3	Authentifizierungsverfahren AES-GMAC-128	67
9.4	Verschlüsselungs- und Authentifizierungsverfahren in der TPL	68
9.4.1	Überblick über TPL-Schutzmechanismen.....	68
9.4.2	Herstellerspezifischer Schutzmechanismus (Sicherheitsmodus 1)	70
9.4.3	Schutzmechanismus DES-CBC (Sicherheitsmodus 2 und 3)	70
9.4.4	Schutzmechanismus AES-CBC-128 (Sicherheitsmodus 5)	71
9.4.5	Schutzmechanismus AES-CBC-128 (Sicherheitsmodus 7)	72
9.4.6	Schutzmechanismus AES-CTR-128 (Sicherheitsmodus 8).....	73
9.4.7	Schutzmechanismus AES-GCM-128 (Sicherheitsmodus 9)	75
9.4.8	Schutzmechanismus AES-CCM-128 (Sicherheitsmodus 10)	78
9.5	Reaktion auf ein Sicherheitsversagen	81
9.6	Schlüsselableitung	81
9.6.1	Allgemeines.....	81
9.6.2	Schlüsselableitungsfunktion A.....	81
9.7	Schlüsselaustausch	83
	Anhang A (normativ) Übertragungsprotokoll für Sicherheitsinformationen	84
A.1	Einleitung.....	84
A.2	SITP-Dienste	84
A.2.1	Sicherheitsinformationen übertragen	84
A.2.2	Sicherheitsinformationen aktivieren	85
A.2.3	Sicherheitsinformationen deaktivieren	85
A.2.4	Sicherheitsinformationen zerstören	85
A.2.5	kombinierte Aktivierung/Deaktivierung von Sicherheitsinformationen	85

A.2.6	Sicherheitsinformationen erzeugen	85
A.2.7	Sicherheitsinformationen erhalten	85
A.2.8	Liste aller Schlüsselinformation erhalten	86
A.2.9	Liste der aktiven Schlüsselinformation erhalten	86
A.2.10	Liste der aktiven Schlüssel- und Schlüsselzählerinformation erhalten	86
A.2.11	Von Ende zu Ende gesicherte Anwendungsdaten übertragen	86
A.3	CI-Felder	86
A.4	SITP-Struktur	86
A.5	Blockkontrollfeld	87
A.6	Blockparameter	88
A.7	Überblick über Datenstrukturen/Mechanismen	89
A.8	Datenstrukturen für Sicherheitsinformationen	91
A.8.1	Allgemeines	91
A.8.2	Datenstruktur 00 _h	91
A.8.3	Datenstruktur 01 _h	91
A.8.4	Datenstruktur 02 _h	92
A.8.5	Datenstruktur 03 _h	93
A.8.6	Datenstruktur 20 _h	94
A.8.7	Datenstruktur 21 _h	95
A.8.8	Datenstruktur 22 _h	95
A.8.9	Datenstruktur 23 _h	96
A.9	Datenstrukturen für gesicherte Anwendungsdaten	97
A.9.1	Allgemeines	97
A.9.2	Datenstruktur 30 _h — AES-Schlüssel-Wrap	99
A.9.3	Datenstruktur 31 _h — HMAC-SHA256	99
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	102
A.9.7	Datenstruktur 36 _h und 37 _h — AES-CCM	103
Anhang B (informativ) Beispiel eines Nachrichtenzählers		105
Literaturhinweise		108

Bilder

Bild 1 — Eingabe und Ausgabe für den GCM-Algorithmus	75
Bild B.1 — Kontrollfluss des Nachrichtenzählers (Teil 1)	106
Bild B.2 — Kontrollfluss des Nachrichtenzählers (Teil 2)	107

Tabellen

Tabelle 1 — Reihenfolge der M-Bus-Schicht	21
Tabelle 2 — Vom Master oder Slave verwendete Codes des CI-Felds	22
Tabelle 3 — Übersicht über alle AFL-Felder	27
Tabelle 4 — AFL-Fragmentierungskontrollfeld — Definitionen der Bitfelder	28
Tabelle 5 — AFL-Nachrichtenkontrollfeld — Definitionen der Bitfelder	28
Tabelle 6 — AT-Teilfeld von AFL.MCL	29

Tabelle 7 — AFL-Schlüsselinformationfeld — Definitionen der Bitfelder	29
Tabelle 8 — AFL-Nachrichtenzählerfeld — Definitionen der Bitfelder	30
Tabelle 9 — AFL-Nachrichtenlängenfeld — Definitionen der Bitfelder.....	30
Tabelle 10 — Allgemeine Struktur der TPL	31
Tabelle 11 — Kurzer TPL-Header	32
Tabelle 12 — Langer TPL-Header.....	32
Tabelle 13 — Identifikation des Gerätetyps	33
Tabelle 14 — Kodierung des Statusfelds.....	37
Tabelle 15 — Mit dem Statusfeld kodierte Anwendungsfehler	37
Tabelle 16 — Bedeutung des Statusbytes für Partnernachrichten	39
Tabelle 17 — Bedeutung der Bits 0 bis 5 im Statusbyte für Partnernachrichten	39
Tabelle 18 — Allgemeine Definition der zwei obligatorischen Konfigurationsfeldbytes.....	40
Tabelle 19 — Definition der Modusbits im Konfigurationsfeld (Sicherheitsmodus)	41
Tabelle 20 — TPL-Struktur einer geschützten Nachricht.....	41
Tabelle 21 — Inhalt der Zählernachricht.....	43
Tabelle 22 — Inhalt der Partnernachricht	44
Tabelle 23 — Verwendung von Inhaltsindexbits	44
Tabelle 24 — Zugänglichkeit eines Geräts	45
Tabelle 25 — Schlüssel-ID.....	45
Tabelle 26 — KDF-Auswahl	46
Tabelle 27 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 0	46
Tabelle 28 — Definition des Konfigurationsfelds für den Sicherheitsmodus 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	48
Tabelle 31 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 5	49
Tabelle 32 — Definition des Konfigurationsfelds für den Sicherheitsmodus 5	49
Tabelle 33 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 7	50
Tabelle 34 — Definition des Konfigurationsfelds für den Sicherheitsmodus 7	50
Tabelle 35 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 7	51

Tabelle 36 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 8	52
Tabelle 37 — Definition des Konfigurationsfelds für Modus 8	52
Tabelle 38 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 8	54
Tabelle 39 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 9	55
Tabelle 40 — Definition des Konfigurationsfelds für den Sicherheitsmodus 9	55
Tabelle 41 — Konfigurationsfeld und nachfolgende Felder mit dem Sicherheitsmodus 10.....	56
Tabelle 42 — Definition des Konfigurationsfelds für den Sicherheitsmodus 10.....	57
Tabelle 43 — Definition der Konfigurationsfelderweiterung für den Sicherheitsmodus 10.....	58
Tabelle 44 — Adressstruktur der Verbindungsschicht für Funk.....	59
Tabelle 45 — Struktur eines Datagramms für die Selektion eines Slaves.....	60
Tabelle 46 — Anwendungsschichtstruktur eines Datagramms für die erweiterte Selektion	61
Tabelle 47 — Sicherheitsdienste und Sicherheitsziele.....	63
Tabelle 48 — Schutzmechanismen für die Ablesung des Zählers	69
Tabelle 49 — Initialisierungsvektor des Sicherheitsmodus 5	71
Tabelle 50 — Struktur des Initialisierungsvektors in Sicherheitsmodus 8.....	74
Tabelle 51 — Eingabe- und Ausgabeinformationen für die GCM-Funktionen	76
Tabelle 52 — Struktur des Initialisierungsvektors in Sicherheitsmodus 9.....	78
Tabelle 53 — Struktur der Nonce N	80
Tabelle 54 — Konstante DC für die Schlüsselableitung.....	82
Tabelle A.1 — CI-Felder des Übertragungsprotokolls für Sicherheitsinformationen	86
Tabelle A.2 — Interne Blockstruktur des SITP.....	87
Tabelle A.3 — Blockkontrollfeld	88
Tabelle A.4 — Blockparameterstruktur	88
Tabelle A.5 — Liste der SITP-Datenstrukturen/Mechanismen	89
Tabelle A.6 — DSH-Inhalt von DSI 00_h.....	91
Tabelle A.7 — Wrapped-Datenstruktur 01_h	92
Tabelle A.8 — Wrapped-Datenstruktur 02_h.....	92
Tabelle A.9 — Wrapped-Datenstruktur 03_h.....	93
Tabelle A.10 — Optionen für Wrapped-Datenstruktur 03_h	94

Tabelle A.11 — Datenstruktur 20_h für alle von einem Wrapper umhüllten Schlüssel	94
Tabelle A.12 — Datenstruktur 21_h für aktiven Schlüssel	95
Tabelle A.13 — Statusantwortstruktur	95
Tabelle A.14 — Definition des Statusantwortbytes.....	96
Tabelle A.15 — Datenstruktur 23_h für aktiven Schlüsselzähler.....	97
Tabelle A.16 — Liste der unterstützten PIDs.....	98
Tabelle A.17 — Datenstruktur 31_h.....	99
Tabelle A.18 — Auswahl von Datenstruktur 32_h und 33_h.....	100
Tabelle A.19 — Datenstruktur 32_h und 33_h.....	100
Tabelle A.20 — Datenstruktur 34_h.....	101
Tabelle A.21 — Struktur von IV bei AES-GCM	102
Tabelle A.22 — Datenstruktur 35_h.....	102
Tabelle A.23 — Struktur von IV bei AES-GMAC	103
Tabelle A.24 — Auswahl von Datenstruktur 36_h und 37_h.....	103
Tabelle A.25 — Wrapped-Datenstruktur 36_h und 37_h.....	104
Tabelle A.26 — Struktur der CCM-Nonce bei AES-GMAC.....	104