DIN EN 13757-7:2018-06 (D)

Kommunikationssysteme für Zähler - Teil 7: Transport- und Sicherheitsdienste; Deutsche Fassung EN 13757-7:2018

Inhalt

Seite

Europäisches Vorwort 5

Einleitung 7

1 Anwendungsbereich 9

2 Normative Verweisungen 9

3 Begriffe 10

4 Abkürzungen und Symbole 12
4.1 Abkürzungen 12
4.2 Symbole 14

5 Schichtmodell 14
5.1 M-Bus-Schichten 14
5.2 Das CI-Feld-Prinzip 15

6 Authentifizierungs- und Fragmentierungs-Teilschicht (AFL) 20
6.1 Einleitung 20
6.2 Übersicht über die AFL-Struktur 21
6.3 Komponenten der AFL 21
6.3.1 AFL-Längenfeld (AFL.AFLL) 21
6.3.2 AFL-Fragmentierungskontrollfeld (AFL.FCL) 21
6.3.3 AFL-Nachrichtenkontrollfeld (AFL.MCL) 22
6.3.4 AFL-Schlüsselinformationsfeld (AFL.KI) 23
6.3.5 AFL-Nachrichtenzählerfeld (AFL.MCR) 23
6.3.6 AFL-MAC-Feld (AFL.MAC) 24
6.3.7 AFL-Nachrichtenlängenfeld (AFL.ML) 24

7 Transportschicht (TPL) 24
7.1 Einleitung 24
7.2 Struktur ohne TPL-Header 25
7.3 Struktur mit kurzem TPL-Header 25
7.4 Struktur mit langem TPL-Header 25
7.5 CI-Feld-abhängige Elemente 26
7.5.1 Identifikationsnummer 26
7.5.2 Identifikation des Herstellers 26
7.5.3 Versionsidentifikation 27
7.5.4 Identifikation des Gerätetyps 27
7.5.5 Zugriffsnummer 29
7.5.6 Statusbyte in Zählernachrichten 30
7.5.7 Statusbyte in Partnernachrichten 31
7.5.8 Konfigurationsfeld 32
7.6 Konfigurationsfeldabhängige Struktur 34
7.6.1 Allgemeines 34
7.6.2 Konfigurationsfelderweiterung 34
7.6.3 Optionale TPL-Header-Felder 34
7.6.4 Optionale TPL-Trailer-Felder 34
7.6.5 Teilverschlüsselung 35
7.7 Sicherheitsmodusspezifische TPL-Felder 35
7.7.1 Gemeinsame Teilfelder des Konfigurationsfelds und der Konfigurationsfelderweiterung 35

7.7.2 Konfigurationsfeld des Sicherheitsmodus 0 38
7.7.3 Konfigurationsfeld der Sicherheitsmodi 2 und 3 39
7.7.4 Konfigurationsfeld des Sicherheitsmodus 5 40
7.7.5 Konfigurationsfeld des Sicherheitsmodus 7 42
7.7.6 Konfigurationsfeld des Sicherheitsmodus 8 43
7.7.7 Konfigurationsfeld des Sicherheitsmodus 9 46
7.7.8 Konfigurationsfeld des Sicherheitsmodus 10 48

8 Verwaltung der unteren Schichten 50
8.1 Allgemeines 50
8.2 Setzen der Baudrate für die M-Bus-Verbindungsschicht nach EN 13757-2 50
8.3 Adressstruktur bei Verwendung zusammen mit der drahtlosen Datenverbindungsschicht nach EN 13757-4 50
8.4 Selektion und Sekundäradressierung 50
8.5 Generalisiertes Selektionsverfahren 52
8.6 Suche nach installierten Slaves 52
8.6.1 Primäradressen 52
8.6.2 Sekundäradressen 53
8.6.3 Verfahren der Platzhaltersuche 53

9 Sicherheitsdienste 53
9.1 Allgemeines 53
9.2 Nachrichtenzähler 55
9.2.1 Überblick 55
9.2.2 Nachrichtenzähler C_M, der vom Zähler übertragen wird 55
9.2.3 Nachrichtenzähler C_{CP}, der vom Kommunikationspartner übertragen wird 56
9.2.4 Nachrichtenzähler C'_{CP}, der vom Zähler erhalten wird 56
9.2.5 Nachrichtenzähler C'_M und C''_M, die vom Kommunikationspartner empfangen werden 57
9.3 Authentifizierungsverfahren in der AFL 57
9.3.1 Überblick 57
9.3.2 Authentifizierungsverfahren AES-CMAC-128 58
9.3.3 Authentifizierungsverfahren AES-GMAC-128 58
9.4 Verschlüsselungs- und Authentifizierungsverfahren in der TPL 59
9.4.1 Überblick über TPL-Schutzmechanismen 59
9.4.2 Herstellerspezifischer Schutzmechanismus (Sicherheitsmodus 1) 61
9.4.3 Schutzmechanismus DES-CBC (Sicherheitsmodus 2 und 3) 61
9.4.4 Schutzmechanismus AES-CBC-128 (Sicherheitsmodus 5) 62
9.4.5 Schutzmechanismus AES-CBC-128 (Sicherheitsmodus 7) 63
9.4.6 Schutzmechanismus AES-CTR-128 (Sicherheitsmodus 8) 64
9.4.7 Schutzmechanismus AES-GCM-128 (Sicherheitsmodus 9) 66
9.4.8 Schutzmechanismus AES-CCM-128 (Sicherheitsmodus 10) 69
9.5 Reaktion auf ein Sicherheitsversagen 71
9.6 Schlüsselableitung 72
9.6.1 Allgemeines 72
9.6.2 Schlüsselableitungsfunktion A 72
9.7 Schlüsselaustausch 73

Anhang A (normativ) Übertragungsprotokoll für Sicherheitsinformationen 74
A.1 Einleitung 74
A.2 SITP-Dienste 74
A.2.1 Sicherheitsinformationen übertragen 74
A.2.2 Sicherheitsinformationen aktivieren 75
A.2.3 Sicherheitsinformationen deaktivieren 75
A.2.4 Sicherheitsinformationen zerstören 75
A.2.5 Kombinierte Aktivierung/Deaktivierung von Sicherheitsinformationen 75
A.2.6 Sicherheitsinformationen erzeugen 75
A.2.7 Sicherheitsinformationen erhalten 75
A.2.8 Liste aller Schlüsselinformation erhalten 75

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

Anhang B (informativ) Beispiel eines Nachrichtenzählers 93

Literaturhinweise 97