

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

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

Contents		Page
European foreword		5
Introduction		7
1	Scope	9
2	Normative references	9
3	Terms and definitions	10
4	Abbreviations and symbols	12
4.1	Abbreviations	12
4.2	Symbols	14
5	Layer model	14
5.1	M-Bus Layers	14
5.2	The CI-field principle	15
6	Authentication and Fragmentation Sublayer (AFL)	19
6.1	Introduction	19
6.2	Overview of the AFL-Structure	20
6.3	Components of the AFL	21
6.3.1	AFL Length Field (AFL.AFLL)	21
6.3.2	AFL Fragmentation Control Field (AFL.FCL)	21
6.3.3	AFL Message Control Field (AFL.MCL)	22
6.3.4	AFL Key Information-Field (AFL.KI)	23
6.3.5	AFL Message counter field (AFL.MCR)	23
6.3.6	AFL MAC-field (AFL.MAC)	24
6.3.7	AFL Message Length Field (AFL.ML)	24
7	Transport Layer (TPL)	24
7.1	Introduction	24
7.2	Structure of none TPL header	25
7.3	Structure of short TPL header	25
7.4	Structure of long TPL header	25
7.5	CI-field dependent elements	25
7.5.1	Identification number	25
7.5.2	Manufacturer identification	26
7.5.3	Version identification	26
7.5.4	Device type identification	26
7.5.5	Access number	28
7.5.6	Status byte in meter messages	30
7.5.7	Status byte in partner messages	31
7.5.8	Configuration field	32
7.6	Configuration field dependent structure	33
7.6.1	General	33
7.6.2	Configuration field extension	34
7.6.3	Optional TPL-header fields	34
7.6.4	Optional TPL Trailer fields	34
7.6.5	Partial encryption	34
7.7	Security mode specific TPL-fields	34

7.7.1	Shared subfields of configuration field and configuration field extension	34
7.7.2	Configuration field of Security mode 0	37
7.7.3	Configuration field of Security modes 2 and 3	38
7.7.4	Configuration field of Security mode 5	39
7.7.5	Configuration field of Security mode 7	40
7.7.6	Configuration field of Security mode 8	41
7.7.7	Configuration field of Security mode 9	44
7.7.8	Configuration field of Security mode 10	46
8	Management of lower layers	48
8.1	General	48
8.2	Switching baud rate for M-Bus Link Layer according to EN 13757-2	48
8.3	Address structure if used together with the wireless Data Link Layer according to EN 13757-4	48
8.4	Selection and secondary addressing	48
8.5	Generalized selection procedure	49
8.6	Searching for installed slaves	50
8.6.1	Primary addresses	50
8.6.2	Secondary addresses	50
8.6.3	Wildcard searching procedure	50
9	Security Services	51
9.1	General	51
9.2	Message counter	52
9.2.1	Overview	52
9.2.2	Message counter CM transmitted by the meter	52
9.2.3	Message counter CCP transmitted by the communication partner	53
9.2.4	Message counter C'CP received by the meter	53
9.2.5	Message counter C'M and C"M received by the communication partner	53
9.3	Authentication methods in the AFL	54
9.3.1	Overview	54
9.3.2	Authentication method AES-CMAC-128	54
9.3.3	Authentication method AES-GMAC-128	54
9.4	Encryption and Authentication methods in the TPL	55
9.4.1	Overview about TPL-Security mechanisms	55
9.4.2	Manufacturer specific Security mechanism (Security mode 1)	57
9.4.3	Security mechanism DES-CBC (Security mode 2 and 3)	57
9.4.4	Security mechanism AES-CBC-128 (Security mode 5)	58
9.4.5	Security mechanism AES-CBC-128 (Security mode 7)	59
9.4.6	Security mechanism AES-CTR-128 (Security mode 8)	59
9.4.7	Security mechanism AES-GCM-128 (Security mode 9)	61
9.4.8	Security mechanism AES-CCM-128 (Security mode 10)	64
9.5	Reaction to security failure	66
9.6	Key derivation	67
9.6.1	General	67
9.6.2	Key derivation function A	67
9.7	Key Exchange	68
Annex A (normative)	Security Information Transfer Protocol	69
A.1	Introduction	69
A.2	SITP Services	69
A.2.1	Transfer security information	69
A.2.2	Activate security information	70
A.2.3	Deactivate security information	70
A.2.4	Destroy security information	70
A.2.5	Combined activation/deactivation of security information	70
A.2.6	Generate security information	70
A.2.7	Get security information	70
A.2.8	Get list of all key information	70
A.2.9	Get list of active key information	70

A.2.10	Transfer end to end secured application data	70
A.3	CI-Fields	71
A.4	SITP structure	71
A.5	Block Control Field	71
A.6	Block parameters	72
A.7	Overview about Data Structures / Mechanisms	73
A.8	Data structures for Security Information	74
A.8.1	General	74
A.8.2	Data Structure 00h	75
A.8.3	Data Structure 01h	75
A.8.4	Data Structure 02h	75
A.8.5	Data Structure 03h	76
A.8.6	Data Structure 20h	77
A.8.7	Data Structure 21h	77
A.8.8	Data Structure 22h	78
A.9	Data structures for secured application data	79
A.9.1	General	79
A.9.2	Data Structure 30h -- AES Key-Wrap	80
A.9.3	Data Structure 31h -- HMAC-SHA256	81
A.9.4	Data Structure 32h and 33h -- CMAC	82
A.9.5	Data Structure 34h -- AES-GCM	82
A.9.6	Data Structure 35h -- AES-GMAC	84
A.9.7	Data Structure 36h and 37h -- AES-CCM	85
Annex B (informative)	Message counter example	87
Bibliography		91