

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

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

Contents		Page
European foreword		4
Introduction		6
1	Scope	8
2	Normative references	8
3	Terms and definitions	8
4	Abbreviations and symbols	11
4.1	Abbreviations	11
4.2	Symbols	13
5	Layer model	13
5.1	M-Bus Layers	13
5.2	The CI-field principle	14
6	Authentication and Fragmentation Sublayer (AFL)	18
6.1	Introduction	18
6.2	Overview of the AFL-Structure	19
6.3	Components of the AFL	20
6.3.1	AFL Length Field (AFL.AFLL)	20
6.3.2	AFL Fragmentation Control Field (AFL.FCL)	20
6.3.3	AFL Message Control Field (AFL.MCL)	20
6.3.4	AFL Key Information-Field (AFL.KI)	21
6.3.5	AFL Message counter field (AFL.MCR)	22
6.3.6	AFL MAC-field (AFL.MAC)	22
6.3.7	AFL Message Length Field (AFL.ML)	22
7	Transport Layer (TPL)	23
7.1	Introduction	23
7.2	Structure of none TPL header	23
7.3	Structure of short TPL header	23
7.4	Structure of long TPL header	24
7.5	CI-field dependent elements	24
7.5.1	Identification number	24
7.5.2	Manufacturer identification	25
7.5.3	Version identification	25
7.5.4	Device type identification	25
7.5.5	Access number	27
7.5.6	Status byte in meter messages	29
7.5.7	Status byte in partner messages	30
7.5.8	Configuration field	31
7.6	Configuration field dependent structure	32
7.6.1	General	32
7.6.2	Configuration field extension	32
7.6.3	Optional TPL-header fields	32
7.6.4	Optional TPL Trailer fields	33
7.6.5	Partial encryption	33
7.7	Security Mode specific TPL-fields	33
7.7.1	Shared subfields of configuration field and configuration field extension	33

7.7.2	Configuration field of Security Mode 0	36
7.7.3	Configuration field of Security Modes 2 and 3	37
7.7.4	Configuration field of Security Mode 5	38
7.7.5	Configuration field of Security Mode 7	39
7.7.6	Configuration field of Security Mode 8	41
7.7.7	Configuration field of Security Mode 9	43
7.7.8	Configuration field of Security Mode 10	45
8	Management of lower layers	47
8.1	General	47
8.2	Switching baud rate for M-Bus Link Layer according to EN 13757-2	47
8.3	Address structure if used together with the wireless Data Link Layer according to EN 13757-4	47
8.4	Selection and secondary addressing	47
8.5	Generalized selection procedure	48
8.6	Searching for installed slaves	49
8.6.1	Primary addresses	49
8.6.2	Secondary addresses	49
8.6.3	Wildcard searching procedure	49
9	Security Services	50
9.1	General	50
9.2	Message counter	51
9.2.1	Overview	51
9.2.2	Message counter CM transmitted by the meter	52
9.2.3	Message counter CCP transmitted by the communication partner	52
9.2.4	Message counter C'CP received by the meter	52
9.2.5	Message counter C'M and C"M received by the communication partner	53
9.3	Authentication methods in the AFL	53
9.3.1	Overview	53
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)	56
9.4.3	Security mechanism DES-CBC (Security Mode 2 and 3)	56
9.4.4	Security mechanism AES-CBC-128 (Security Mode 5)	57
9.4.5	Security mechanism AES-CBC-128 (Security Mode 7)	58
9.4.6	Security mechanism AES-CTR-128 (Security Mode 8)	59
9.4.7	Security mechanism AES-GCM-128 (Security Mode 9)	60
9.4.8	Security mechanism AES-CCM-128 (Security Mode 10)	63
9.5	Reaction to security failure	65
9.6	Key derivation	66
9.6.1	General	66
9.6.2	Key derivation function A	66
9.7	Key Exchange	67
	Annex A (normative) Security Information Transfer Protocol	68
	Annex B (informative) Message counter example	86
	Bibliography	90