

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

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

---

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

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

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