



# Security Target

## SMGW Version 2.1

## 1 Version History

<b>Ver- sion</b>	<b>Datum</b>	<b>Name</b>	<b>Änderungen</b>
1.10	08.07.2024	C. Miller	Aktualisierung

## 2 Contents

3	<b>Contents .....</b>	<b>3</b>
4	<b>1 Introduction .....</b>	<b>6</b>
5	1.1 ST reference .....	6
6	1.2 TOE reference .....	6
7	1.3 Introduction.....	9
8	1.4 TOE Overview .....	11
9	1.4.1 Introduction .....	11
10	1.4.2 Overview of the Gateway in a Smart Metering System .....	12
11	1.4.3 TOE description.....	15
12	1.4.4 TOE Type definition .....	16
13	1.4.5 TOE logical boundary .....	19
14	1.4.6 The logical interfaces of the TOE .....	27
15	1.4.7 The cryptography of the TOE and its Security Module .....	28
16	TOE life-cycle .....	32
17	<b>2 Conformance Claims .....</b>	<b>33</b>
18	2.1 CC Conformance Claim .....	33
19	2.2 PP Claim / Conformance Statement .....	33
20	2.3 Package Claim .....	33
21	2.4 Conformance Claim Rationale .....	33
22	<b>3 Security Problem Definition.....</b>	<b>34</b>
23	3.1 External entities .....	34
24	3.2 Assets.....	34
25	3.3 Assumptions .....	38
26	3.4 Threats.....	40
27	3.5 Organizational Security Policies.....	43
28	<b>4 Security Objectives .....</b>	<b>45</b>
29	4.1 Security Objectives for the TOE .....	45
30	4.2 Security Objectives for the Operational Environment.....	50
31	4.3 Security Objective Rationale.....	52
32	4.3.1 Overview .....	52
33	4.3.2 Countering the threats.....	53
34	4.3.3 Coverage of organisational security policies .....	56
35	4.3.4 Coverage of assumptions .....	57
36	<b>5 Extended Component definition .....</b>	<b>59</b>
37	5.1 Communication concealing (FPR_CON) .....	59
38	5.2 Family behaviour .....	59
39	5.3 Component levelling.....	59
40	5.4 Management.....	59
41	5.5 Audit .....	59
42	5.6 Communication concealing (FPR_CON.1) .....	59
43	<b>6 Security Requirements.....</b>	<b>61</b>
44	6.1 Overview.....	61

45	<b>6.2 Class FAU: Security Audit.....</b>	<b>65</b>
46	6.2.1 Introduction .....	65
47	6.2.2 Security Requirements for the System Log .....	67
48	6.2.3 Security Requirements for the Consumer Log .....	70
49	6.2.4 Security Requirements for the Calibration Log .....	73
50	6.2.5 Security Requirements that apply to all logs .....	78
51	<b>6.3 Class FCO: Communication.....</b>	<b>80</b>
52	6.3.1 Non-repudiation of origin (FCO_NRO).....	80
53	<b>6.4 Class FCS: Cryptographic Support .....</b>	<b>81</b>
54	6.4.1 Cryptographic support for TLS.....	81
55	6.4.2 Cryptographic support for CMS .....	82
56	6.4.3 Cryptographic support for Meter communication encryption .....	84
57	6.4.4 General Cryptographic support.....	86
58	<b>6.5 Class FDP: User Data Protection.....</b>	<b>89</b>
59	6.5.1 Introduction to the Security Functional Policies .....	89
60	6.5.2 Gateway Access SFP .....	89
61	6.5.3 Firewall SFP .....	91
62	6.5.4 Meter SFP.....	94
63	6.5.5 General Requirements on user data protection.....	98
64	<b>6.6 Class FIA: Identification and Authentication .....</b>	<b>99</b>
65	6.6.1 User Attribute Definition (FIA_ATD).....	99
66	6.6.2 Authentication Failures (FIA_AFL).....	100
67	6.6.3 User Authentication (FIA_UAU).....	100
68	6.6.4 User identification (FIA_UID) .....	102
69	6.6.5 User-subject binding (FIA_USB).....	103
70	<b>6.7 Class FMT: Security Management .....</b>	<b>104</b>
71	6.7.1 Management of the TSF.....	104
72	6.7.2 Security management roles (FMT_SMR) .....	111
73	6.7.3 Management of security attributes for Gateway access SFP.....	112
74	6.7.4 Management of security attributes for Firewall SFP .....	113
75	6.7.5 Management of security attributes for Meter SFP .....	114
76	<b>6.8 Class FPR: Privacy .....</b>	<b>115</b>
77	6.8.1 Communication Concealing (FPR_CON).....	115
78	6.8.2 Pseudonymity (FPR_PSE).....	116
79	<b>6.9 Class FPT: Protection of the TSF .....</b>	<b>117</b>
80	6.9.1 Fail secure (FPT_FLS).....	117
81	6.9.2 Replay Detection (FPT_RPL).....	118
82	6.9.3 Time stamps (FPT_STM) .....	118
83	6.9.4 TSF self test (FPT_TST).....	118
84	6.9.5 TSF physical protection (FPT_PHP).....	119
85	<b>6.10 Class FTP: Trusted path/channels.....</b>	<b>119</b>
86	6.10.1 Inter-TSF trusted channel (FTP_ITC).....	119

87	<b>6.11 Security Assurance Requirements for the TOE.....</b>	<b>121</b>
88	<b>6.12 Security Requirements rationale .....</b>	<b>123</b>
89	6.12.1 Security Functional Requirements rationale.....	123
90	6.12.2 Security Assurance Requirements rationale .....	136
91	<b>7 TOE Summary Specification.....</b>	<b>137</b>
92	7.1 SF.1: Authentication of Communication and Role Assignment for external	
93	entities.....	137
94	7.2 SF.2: Acceptance and Deposition of Meter Data, Encryption of Meter Data for	
95	WAN transmission.....	144
96	7.3 SF.3: Administration, Configuration and SW Update.....	146
97	7.4 SF.4: Displaying Consumption Data.....	148
98	7.5 SF.5: Audit and Logging.....	149
99	7.6 SF.6: TOE Integrity Protection .....	151
100	7.7 TSS Rationale.....	152
101	<b>8 List of Tables.....</b>	<b>156</b>
102	<b>9 List of Figures .....</b>	<b>157</b>
103	<b>10 Appendix .....</b>	<b>158</b>
104	10.1 Mapping from English to German terms .....	158
105	10.2 Glossary .....	160
106	<b>11 Literature .....</b>	<b>165</b>
107		

# 108 1 Introduction

## 109 1.1 ST reference

110	Title:	Security Target, SMGW Version 2.1
111	Editors:	Power Plus Communications AG
112	CC-Version:	3.1 Revision 5
113	Assurance Level:	EAL 4+, augmented by AVA_VAN.5 and ALC_FLR.2
114	General Status:	Final
115	Document Version:	1.10
116	Document Date:	08.07.2024
117	TOE:	SMGW Version 2.1
118	Certification ID:	BSI-DSZ-CC-0831-V7-2023

119 This document contains the security target of the *SMGW Version 2.1*.

120 This security target claims conformance to the *Smart Meter Gateway* protection profile  
121 [PP\_GW].

122

## 123 1.2 TOE reference

124 The TOE described in this security target is the *SMGW Version 2.1*.

125 The following classifications of the product "*Smart Meter Gateway*" contain the TOE:

- 126 • *BPL Smart Meter Gateway* (BPL-SMGW), SMGW-B-2A-111-00
- 127 • *ETH Smart Meter Gateway* (ETH-SMGW), SMGW-E-2A-111-00
- 128 • *LTE Smart Meter Gateway* (LTE-SMGW), SMGW-J-2A-111-10, SMGW-J-2A-  
129 111-30, SMGW-K-2A-111-10 or SMGW-K-2A-111-30
- 130 • *G.hn Smart Meter Gateway* (G.hn-SMGW), SMGW-N-2A-111-00
- 131 • *LTE450 Smart Meter Gateway* (LTE450-SMGW), SMGW-V-2A-111-20

132 The TOE comprises the following parts:

- 133 • hardware device of the hardware generation 2A according to Table 1, including  
134 the TOE's main circuit board, a carrier board, a power-supply unit and a radio

- 135 module for communication with wireless meter (included in the hardware device  
 136 “*Smart Meter Gateway*”)
- 137 • firmware including software application (loaded into the circuit board)
    - 138 ○ “*SMGW Software Version 2.2.0*”, identified by the value 00861-34788  
 139 which comprises of two revision numbers of the underlying version control sys-  
 140 tem for the TOE, where the first part is for the operating system and the second  
 141 part is for the SMGW application
    - 142 • manuals
      - 143 ○ „Handbuch für Verbraucher, Smart Meter Gateway“ [AGD\_Consumer],  
 144 identified by the SHA-256 hash value  
 145 e24e25671d2c16224e058247eb5fdffb1cfd8bd89de2ee318f99f1f9e776beb
      - 146 ○ „Handbuch für Service-Techniker, Smart Meter Gateway“ [AGD\_Techni-  
 147 ker], identified by the SHA-256 hash value  
 148 67d50481c48cba867e65dff66ff434c08c6d62752aabbe85b4e192eec609069
      - 149 ○ „Handbuch für Hersteller von Smart-Meter Gateway-Administrations-  
 150 Software, Smart Meter Gateway“ [AGD\_GWA], identified by the SHA-  
 151 256 hash value  
 152 43f69e9458e582262a7d2505209e8b0233a4729854c906d4d29200eb92d70f3  
 153 0
      - 154 ○ „Logmeldungen, SMGW “ [SMGW\_Logging] identified by the SHA-256  
 155 hash value  
 156 f3a935b6ae1713ccdaa02411b377377a8e4f7dfb092a181efe1a6c9a86f17a64
      - 157 ○ „Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Ausliefe-  
 158 rung“ [AGD\_SEC], identified by the SHA-256 hash value  
 159 5a54d0b95e8473e6c998049f71b6b27ab4fd0daab8363aea39b94d825efe99c9

160 The hardware device “*Smart Meter Gateway*” includes a secure module with the product  
 161 name “*TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE*” which  
 162 is not part of the TOE but has its own certification id “BSI-DSZ-CC-0957-V2-2016”. More-  
 163 over, a hard-wired communication adapter is connected to the TOE via [USB] as shown  
 164 in Figure 3 which is not part of the TOE (but always an inseparable part of the delivered  
 165 entity). This communication adapter can be either a LTE communication adapter, a  
 166 LTE450 communication adapter, a BPL [IEEE 1901] communication adapter, a GPRS  
 167 communication adapter, a CDMA communication adapter, a powerWAN-Ethernet com-  
 168 munication adapter, a G.hn [ITU G.hn] communication adapter or an ethernet



169 communication adapter. There might be not every communication adapter available for  
 170 each Hardware Generation.

171 The following table shows the different “Smart Meter Gateway” product classifications  
 172 applied on the case of the product, while not all of them might be part of the TOE:

#	Characteristic	Value	Description
1	Product family	SMGW	each classification of a type start with this value
2		-	<i>Delimiter</i>
3	Communication Technology	B	Product Type „BPL Smart Meter Gateway“
		C	Product Type „CDMA Smart Meter Gateway“
		E	Product Type „ETH Smart Meter Gateway“
		G	Product Type „GPRS Smart Meter Gateway“
		L	Product Type „LTE Smart Meter Gateway“
		J	Product Type “LTE Smart Meter Gateway”
		K	Product Type „LTE Smart Meter Gateway“
		P	Product Type „powerWAN-ETH Smart Meter Gateway“
		N	Product Type „G.hn Smart Meter Gateway“
	V	Product Type “LTE450 Smart Meter Gateway”	
4		-	<i>Delimiter</i>
5	Hardware generation	1A	Identification of hardware generation; version 1.0 of “SMGW Hardware”
		1B	Identification of hardware generation; version 1.0.1 of “SMGW Hardware” (with new power adapter)



#	Characteristic	Value	Description
		2A	Identification of hardware generation; version 2.0 of "SMGW Hardware"
6		-	<i>Delimiter</i>
7	HAN Interface	1	Ethernet
8	CLS Interface	1	Ethernet
9	LMN Interface	1	Wireless and wired
10		-	<i>Delimiter</i>
11	SIM card type	0	<i>None</i>
		1	SIM card assembled at factory and SIM slot
		2	SIM card assembled at factory only
		3	SIM slot only
12	reserved	0	

173 **Table 1: Smart Meter Gateway product classifications**

174 **1.3 Introduction**

175 The increasing use of *green energy* and upcoming technologies around e-mobility lead  
 176 to an increasing demand for functions of a so called smart grid. A smart grid hereby  
 177 refers to a commodity<sup>1</sup> network that intelligently integrates the behaviour and actions of  
 178 all entities connected to it – suppliers of natural resources and energy, its consumers  
 179 and those that are both – in order to efficiently ensure a more sustainable, economic and  
 180 secure supply of a certain commodity (definition adopted from [CEN]).

---

1 Commodities can be electricity, gas, water or heat which is distributed from its generator to the consumer through a grid (network).

181 In its vision such a smart grid would allow to invoke consumer devices to regulate the  
182 load and availability of resources or energy in the grid, e.g. by using consumer devices  
183 to store energy or by triggering the use of energy based upon the current load of the  
184 grid<sup>2</sup>. Basic features of such a smart use of energy or resources are already reality.  
185 Providers of electricity in Germany, for example, have to offer at least one tariff that has  
186 the purpose to motivate the consumer to save energy.

187 In the past, the production of electricity followed the demand/consumption of the con-  
188 sumers. Considering the strong increase in renewable energy and the production of en-  
189 ergy as a side effect in heat generation today, the consumption/demand has to follow  
190 the – often externally controlled – production of energy. Similar mechanisms can exist  
191 for the gas network to control the feed of biogas or hydrogen based on information sub-  
192 mitted by consumer devices.

193 An essential aspect for all considerations of a smart grid is the so called *Smart Metering*  
194 *System* that meters the consumption or production of certain commodities at the con-  
195 sumers' side and allows sending the information about the consumption or production to  
196 external entities, which is then the basis for e. g. billing the consumption or production.

197 This Security Target defines the security objectives, corresponding requirements and  
198 their fulfilment for a Gateway which is the central communication component of such a  
199 Smart Metering System (please refer to chapter 1.4.2 for a more detailed overview).

200 The Target of Evaluation (TOE) that is described in this document is an electronic unit  
201 comprising hardware and software/firmware<sup>3</sup> used for collection, storage and provision  
202 of Meter Data<sup>4</sup> from one or more Meters of one or multiple commodities.

203 The Gateway connects a Wide Area Network (WAN) with a Network of Devices of one  
204 or more Smart Metering devices (Local Metrological Network, LMN) and the consumer  
205 Home Area Network (HAN), which hosts Controllable Local Systems (CLS) and visuali-  
206 zation devices. The security functionality of the TOE comprises

- 207 • protection of confidentiality, authenticity, integrity of data and
- 208 • information flow control

---

2 Please note that such a functionality requires a consent or a contract between the supplier and the consumer, alterna-  
tively a regulatory requirement.

3 For the rest of this document the term "firmware" will be used if the complete firmware ist meant. For the application in-  
cluding its services the term "software" will be used.

4 Please refer to chapter 3.2 for an exact definition of the term "Meter Data".

209 mainly to protect the privacy of consumers, to ensure a reliable billing process and to  
210 protect the Smart Metering System and a corresponding large scale infrastructure of the  
211 smart grid. The availability of the Gateway is not addressed by this ST.

212

## 213 **1.4 TOE Overview**

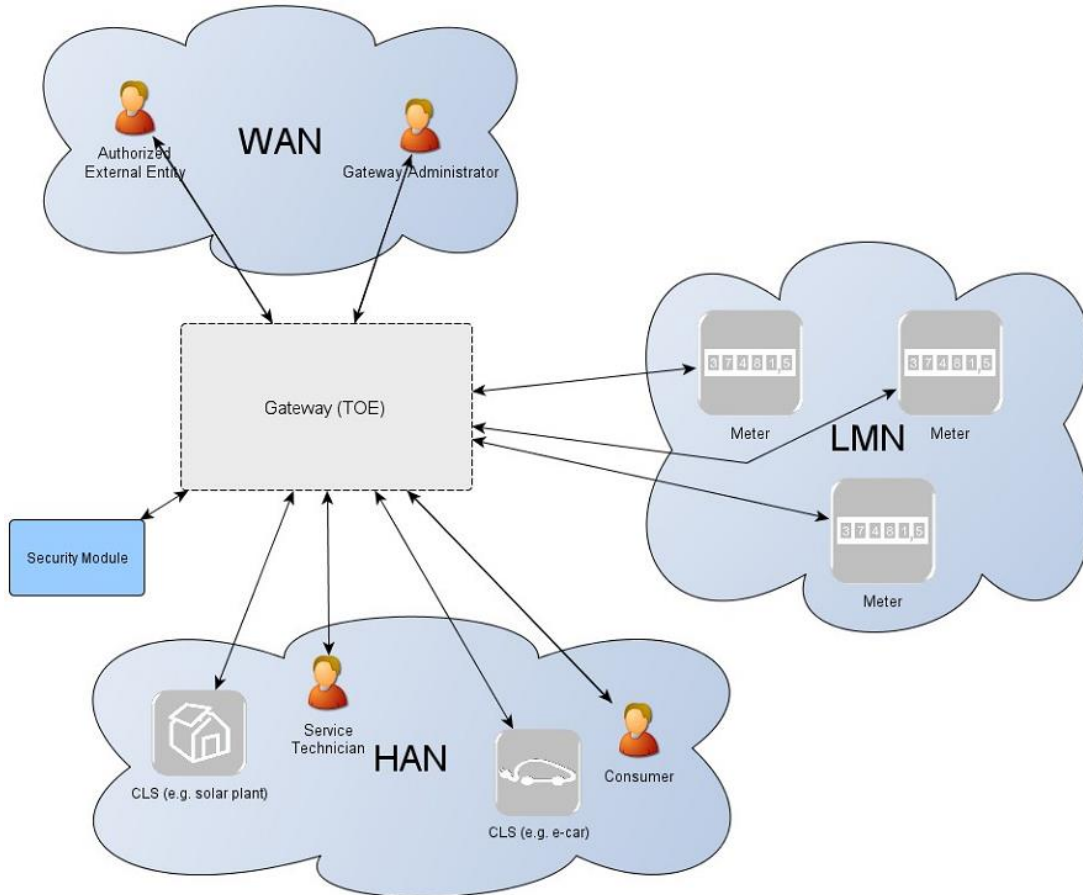
### 214 **1.4.1 Introduction**

215 The TOE as defined in this Security Target is the Gateway in a Smart Metering System.  
216 In the following subsections the overall Smart Metering System will be described first  
217 and afterwards the Gateway itself.

218 There are various different vocabularies existing in the area of Smart Grid, Smart Meter-  
219 ing and Home Automation. Furthermore, the Common Criteria maintain their own vo-  
220 cabulary. The Protection Profile [PP\_GW, chapter 1.3] provides an overview over the  
221 most prominent terms used in this Security Target to avoid any bias which is not fully  
222 repeated here.

223 **1.4.2 Overview of the Gateway in a Smart Metering System**

224 The following figure provides an overview of the TOE as part of a complete Smart Me-  
 225 tering System from a purely functional perspective as used in this ST.<sup>5</sup>



226  
 227 **Figure 1: The TOE and its direct environment**

228  
 229 As can be seen in Figure 1, a system for smart metering comprises different functional  
 230 units in the context of the descriptions in this ST:

- 231
- 232 • The **Gateway** (as defined in this ST) serves as the communication component  
 233 between the components in the local area network (LAN) of the consumer and  
 234 the outside world. It can be seen as a special kind of firewall dedicated to the  
 smart metering functionality. It also collects, processes and stores the records

---

<sup>5</sup> It should be noted that this description purely contains aspects that are relevant to motivate and understand the functionalities of the Gateway as described in this ST. It does not aim to provide a universal description of a Smart Metering System for all application cases.

235 from Meter(s) and ensures that only authorised parties have access to them or  
236 derivatives thereof. Before sending meter data<sup>6</sup> the information will be en-  
237 crypted and signed using the services of a Security Module. The Gateway fea-  
238 tures a mandatory user interface, enabling authorised consumers to access the  
239 data relevant to them.

- 240 • The **Meter** itself records the consumption or production of one or more com-  
241 modities (e.g. electricity, gas, water, heat) and submits those records in defined  
242 intervals to the Gateway. The Meter Data has to be signed and encrypted be-  
243 fore transfer in order to ensure its confidentiality, authenticity, and integrity. The  
244 Meter is comparable to a classical meter<sup>7</sup> and has comparable security require-  
245 ments; it will be sealed as classical meters according to the regulations of the  
246 calibration authority. The Meter further supports the encryption and integrity  
247 protection of its connection to the Gateway<sup>8</sup>.
- 248 • The Gateway utilises the services of a **Security Module** (e.g. a smart card) as  
249 a cryptographic service provider and as a secure storage for confidential assets.  
250 The Security Module will be evaluated separately according to the requirements  
251 in the corresponding Protection Profile (c.f. [SecModPP]).

252 **Controllable Local Systems** (CLS, as shown in Figure 2) may range from local power  
253 generation plants, controllable loads such as air condition and intelligent household ap-  
254 pliances (“white goods”) to applications in home automation. CLS may utilise the ser-  
255 vices of the Gateway for communication services. However, CLS are not part of the  
256 Smart Metering System.

257 The following figure introduces the external interfaces of the TOE and shows the cardi-  
258 nality of the involved entities. Please note that the arrows of the interfaces within the  
259 Smart Metering System as shown in Figure 2 indicate the flow of information. However,  
260 it does not indicate that a communication flow can be initiated bi-directionally. Indeed,

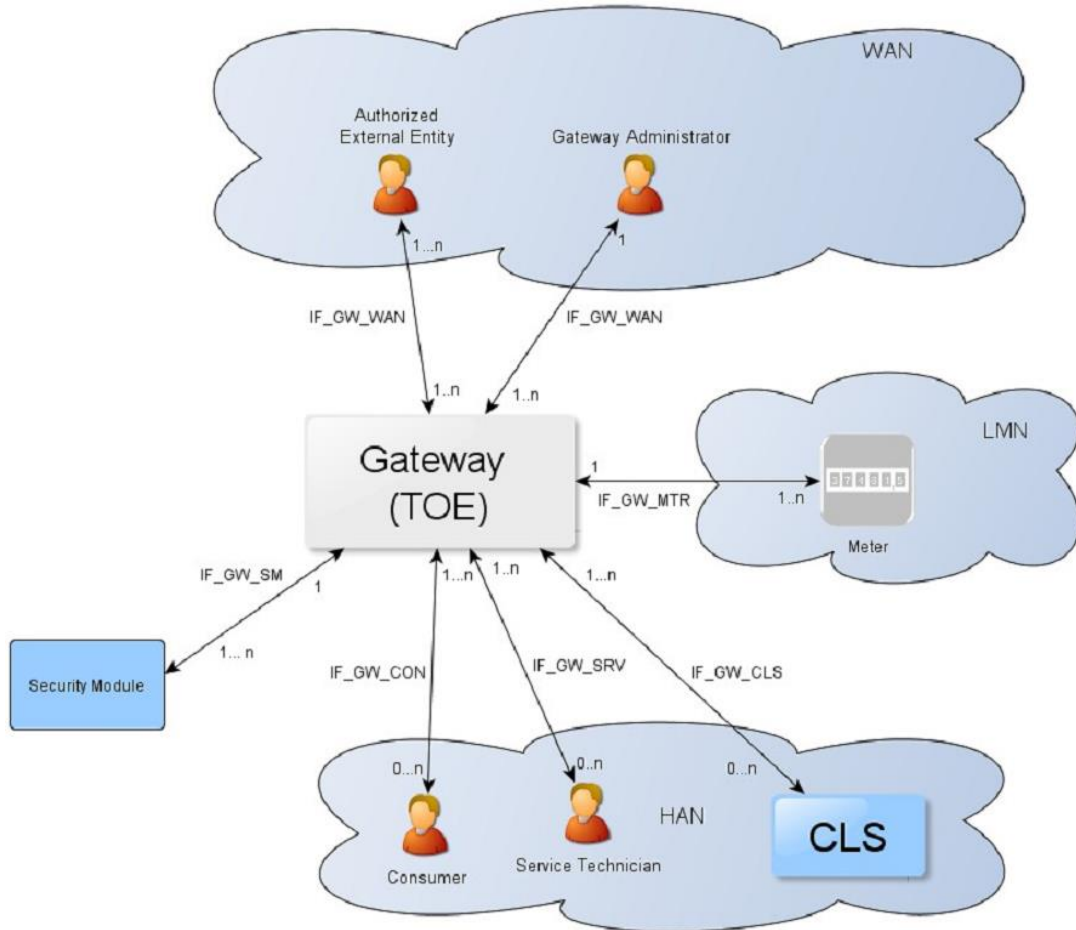
---

6 Please note that readings and data which are not relevant for billing may require an explicit endorsement of the consumer.

7 In this context, a classical meter denotes a meter without a communication channel, i.e. whose values have to be read out locally.

8 It should be noted that this ST does not imply that the connection between the Gateways and external components (specifically meters and CLS) is cable based. It is also possible that the connections as shown in Figure 1 are realised deploying a wireless technology. However, the requirements on how the connections shall be secured apply regardless of the realisation.

261 the following chapters of this ST will place dedicated requirements on the way an infor-  
 262 mation flow can be initiated<sup>9</sup>.



263  
 264 **Figure 2: The logical interfaces of the TOE**

265 The overview of the Smart Metering System as described before is based on a threat  
 266 model that has been developed for the Smart Metering System and has been motivated  
 267 by the following considerations:

- 268 • The Gateway is the central communication unit in the Smart Metering System.  
 269 It is the only unit directly connected to the WAN, to be the first line of defence  
 270 an attacker located in the WAN would have to conquer.
- 271 • The Gateway is the central component that collects, processes and stores Me-  
 272 ter Data. It therewith is the primary point for user interaction in the context of  
 273 the Smart Metering System.

---

<sup>9</sup> Please note that the cardinality of the interface to the consumer is 0..n as it cannot be assumed that a consumer is interacting with the TOE at all.

- 274
- To conquer a Meter in the LMN or CLS in the HAN (that uses the TOE for communication) a WAN attacker first would have to attack the Gateway successfully. All data transferred between LAN and WAN flows via the Gateway which makes it an ideal unit for implementing significant parts of the system's overall security functionality.
- 275
- 276
- 277
- 278
- Because a Gateway can be used to connect and protect multiple Meters (while a Meter will always be connected to exactly one Gateway) and CLS with the WAN, there might be more Meters and CLS in a Smart Metering System than there are Gateways.
- 279
- 280
- 281
- 282

283 All these arguments motivated the approach to have a Gateway (using a Security Module for cryptographic support), which is rich in security functionality, strong and evaluated in depth, in contrast to a Meter which will only deploy a minimum of security functions. The Security Module will be evaluated separately.

284

285

286

### 287 **1.4.3 TOE description**

288 The Smart Metering Gateway (in the following short: Gateway or TOE) may serve as the communication unit between devices of private and commercial consumers and service providers of a commodity industry (e.g. electricity, gas, water, etc.). It also collects, processes and stores Meter Data and is responsible for the distribution of this data to external entities.

289

290

291

292

293 Typically, the Gateway will be placed in the household or premises of the consumer<sup>10</sup> of the commodity and enables access to local Meter(s) (i.e. the unit(s) used for measuring the consumption or production of electric power, gas, water, heat etc.) and may enable access to Controllable Local Systems (e.g. power generation plants, controllable loads such as air condition and intelligent household appliances).

294

295

296

297

298 The TOE has a fail-safe design that specifically ensures that any malfunction can not impact the delivery of a commodity, e.g. energy, gas or water<sup>11</sup>.

299

300

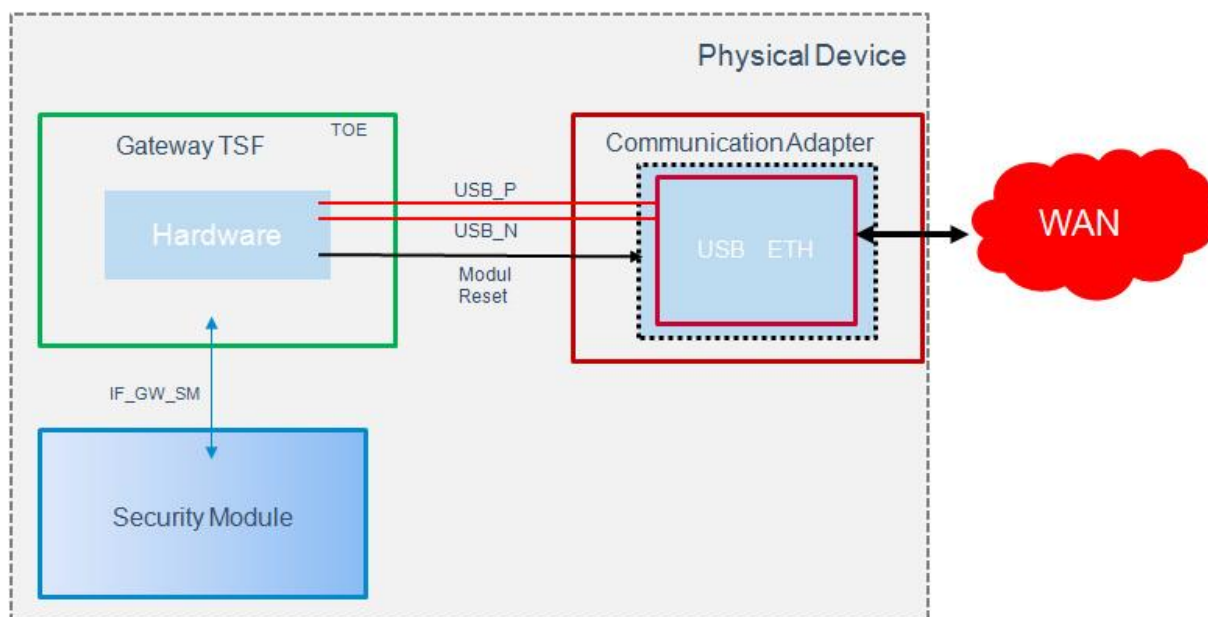
---

<sup>10</sup> Please note that it is possible that the consumer of the commodity is not the owner of the premises where the Gateway will be placed. However, this description acknowledges that there is a certain level of control over the physical access to the Gateway.

<sup>11</sup> Indeed, this Security Target assumes that the Gateway and the Meters have no possibility at all to impact the delivery of a commodity. Even an intentional stop of the delivery of a certain commodity is Not within the scope of this Security Target. It should, however, be noted that such a functionality may be realised by a CLS that utilises the services of the TOE for its communication.



301 The following figure provides an overview of the product with its TOE and non-TOE parts:



302

303 **Figure 3: The product with its TOE and non-TOE parts**

304 The TOE communicates over the interface *IF\_GW\_SM* with a security module and over  
 305 the interfaces *USB\_P*, *USB\_N* and *Module Reset* with one of the possible communica-  
 306 tion adapters according to chapter 1.2. The communication adapters, which are not part  
 307 of the TOE, transmit data from the USB interface to the WAN interface and vice versa.

#### 308 1.4.4 TOE Type definition

309 At first, the TOE is a communication Gateway. It provides different external communica-  
 310 tion interfaces and enables the data communication between these interfaces and con-  
 311 nected IT systems. It further collects, processes and stores Meter Data and is responsi-  
 312 ble for the distribution of this data to external parties.

313 Typically, the Gateway will be placed in the household or premises of the consumer of  
 314 the commodity and enables access to local Meter(s) (i.e. the unit(s) used for measuring  
 315 the consumption or production of electric power, gas, water, heat etc.) and may enable  
 316 access to Controllable Local Systems (e.g. power generation plants, controllable loads  
 317 such as air condition and intelligent household appliances). Roles respectively External  
 318 Entities in the context of the TOE are introduced in chapter 3.1.

319 The TOE described in this ST is a product that has been developed by Power Plus Com-  
 320 munication AG. It is a communication product which complies with the requirements of  
 321 the Protection Profile "Protection Profile for the Gateway of a Smart Metering System"

322 [PP\_GW]. The TOE consists of hardware and software including the operating system.  
323 The communication with more than one meter is possible.

324 The TOE is implemented as a separate physical module which can be integrated into  
325 more complex modular systems. This means that the TOE can be understood as an  
326 OEM module which provides all required physical interfaces and protocols on well de-  
327 fined interfaces. Because of this, the module can be integrated into communication de-  
328 vices and directly into meters.

329 The TOE-design includes the following components:

- 330 • The security relevant components compliant to the Protection Profile.
- 331 • Components with no security relevance (e.g. communication protocols and in-  
332 terfaces).

333 The TOE evaluation does not include the evaluation of the Security Module. In fact, the  
334 TOE relies on the security functionality of the Security Module but it must be security  
335 evaluated in a separate security evaluation<sup>12</sup>.

336 The hardware platform of the TOE mainly consists of a suitable embedded CPU, volatile  
337 and non-volatile memory and supporting circuits like Security Module and RTC.

338 The TOE contains mechanisms for the integrity protection for its firmware.

339 The TOE supports the following communication protocols:

- 340 • OBIS according to [IEC-62056-6-1] and [EN 13757-1],
- 341 • DLMS/COSEM according to [IEC-62056-6-2],
- 342 • SML according to [IEC-62056-5-3-8],
- 343 • unidirectional and bidirectional wireless M-Bus according to [EN 13757-3],  
344 [EN 13757-4], and [IEC-62056-21].

345

---

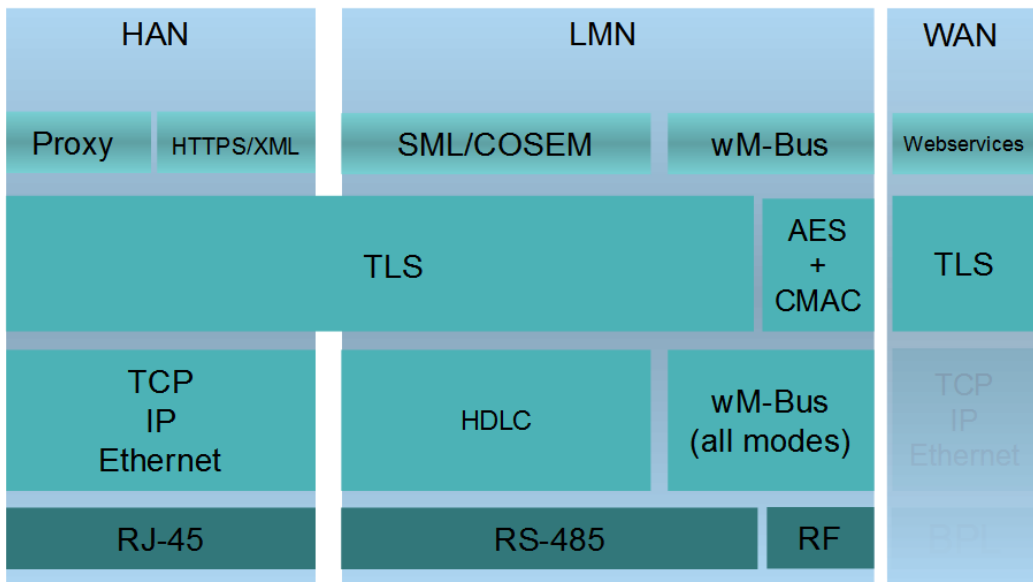
<sup>12</sup> Please note that the Security Module is physically integrated into the Gateway even though it is not part of the TOE.

346 The TOE provides the following physical interfaces for communication

- 347 • Wireless M-Bus (LMN) according to [EN 13757-3],
- 348 • RS-485 (LMN) according to [EIA RS-485],
- 349 • Ethernet (HAN) according to [IEEE 802.3], and
- 350 • USB (WAN) according to [USB].

351 The physical interface for the WAN communication is described in chapter 1.4.3. The  
 352 communication is protected according to [TR-03109].

353 The communication into the HAN is also provided by the Ethernet interface. The proto-  
 354 cols HTTPS and TLS proxy are therefore supported.



355

356 **Figure 4: The TOE's protocol stack**

357 The TOE provides the following functionality:

- 358 • Protected handling of Meter Data compliant to [PP\_GW, chapter 1.4.6.1 and  
 359 1.4.6.2]
- 360 • Integrity and authenticity protection e. g. of Meter Data compliant to [PP\_GW,  
 361 chapter 1.6.4.3]
- 362 • Protection of LAN devices against access from the WAN compliant to [PP\_GW,  
 363 chapter 1.4.6.4]
- 364 • Wake-Up Service compliant to [PP\_GW, chapter 1.4.6.5]
- 365 • Privacy protection compliant to [PP\_GW, chapter 1.4.6.6]
- 366 • Management of Security Functions compliant to [PP\_GW, chapter 1.4.6.7]

- 367           • Cryptography of the TOE and its Security Module compliant to [PP\_GW, chap-  
368           ter 1.4.8]

#### 369           **1.4.5 TOE logical boundary**

370           The logical boundary of the Gateway can be defined by its security features:

- 371           • *Handling of Meter Data*, collection and processing of Meter Data, submission  
372           to authorised external entities (e.g. one of the service providers involved) where  
373           necessary protected by a digital signature
- 374           • *Protection of authenticity, integrity and confidentiality* of data temporarily or per-  
375           sistently stored in the Gateway, transferred locally within the LAN and trans-  
376           ferred in the WAN (between Gateway and authorised external entities)
- 377           • *Firewalling* of information flows to the WAN and information flow control among  
378           Meters, Controllable Local Systems and the WAN
- 379           • *A Wake-Up-Service* that allows to contact the TOE from the WAN side
- 380           • *Privacy preservation*
- 381           • *Management* of Security Functionality
- 382           • *Identification and Authentication* of TOE users

383           The following sections introduce the security functionality of the TOE in more detail.

##### 384           1.4.5.1 Handling of Meter Data<sup>13</sup>

385           The Gateway is responsible for handling Meter Data. It receives the Meter Data from the  
386           Meter(s), processes it, stores it and submits it to external entities.

387           The TOE utilises Processing Profiles to determine which data shall be sent to which  
388           component or external entity. A Processing Profile defines:

- 389           • how Meter Data must be processed,
- 390           • which processed Meter Data must be sent in which intervals,
- 391           • to which component or external entity,
- 392           • signed using which key material,
- 393           • encrypted using which key material,
- 394           • whether processed Meter Data shall be pseudonymised or not, and
- 395           • which pseudonym shall be used to send the data.

---

13           Please refer to chapter 3.2 for an exact definition of the various data types.

396 The Processing Profiles are not only the basis for the security features of the TOE; they  
397 also contain functional aspects as they indicate to the Gateway how the Meter Data shall  
398 be processed. More details on the Processing Profiles can be found in [TR-03109-1].

399 The Gateway restricts access to (processed) Meter Data in the following ways:

- 400 • consumers must be identified and authenticated first before access to any data  
401 may be granted,
- 402 • the Gateway accepts Meter Data from authorised Meters only,
- 403 • the Gateway sends processed Meter Data to correspondingly authorised external  
404 entities only.

405 The Gateway accepts data (e.g. configuration data, firmware updates) from correspond-  
406 ingly authorised Gateway Administrators or correspondingly authorised external entities  
407 only. This restriction is a prerequisite for a secure operation and therewith for a secure  
408 handling of Meter Data. Further, the Gateway maintains a calibration log with all relevant  
409 events that could affect the calibration of the Gateway.

410 These functionalities:

- 411 • prevent that the Gateway accepts data from or sends data to unauthorised en-  
412 tities,
- 413 • ensure that only the minimum amount of data leaves the scope of control of the  
414 consumer,
- 415 • preserve the integrity of billing processes and as such serve in the interests of  
416 the consumer as well as in the interests of the supplier. Both parties are inter-  
417 ested in an billing process that ensures that the value of the consumed amount  
418 of a certain commodity (and only the used amount) is transmitted,
- 419 • preserve the integrity of the system components and their configurations.

420 The TOE offers a local interface to the consumer (see also IF\_GW\_CON in Figure 2)  
421 and allows the consumer to obtain information via this interface. This information com-  
422 prises the billing-relevant data (to allow the consumer to verify an invoice) and infor-  
423 mation about which Meter Data has been and will be sent to which external entity. The  
424 TOE ensures that the communication to the consumer is protected by using TLS and  
425 ensures that consumers only get access to their own data. Therefore, the TOE contains  
426 a web server that delivers the content to the web browser after successful authentication  
427 of the user.

428 1.4.5.2 Confidentiality protection

429 The TOE protects data from unauthorised disclosure

- 430
- 431 • while received from a Meter via the LMN,
  - 432 • while received from the administrator via the WAN,
  - 433 • while temporarily stored in the volatile memory of the Gateway,
  - 434 • while transmitted to the corresponding external entity via the WAN or HAN.

435 Furthermore, all data, which no longer have to be stored in the Gateway, are securely  
436 erased to prevent any form of access to residual data via external interfaces of the TOE.  
437 These functionalities protect the privacy of the consumer and prevent that an unauthor-  
438 ised party is able to disclose any of the data transferred in and from the Smart Metering  
439 System (e.g. Meter Data, configuration settings).

440 The TOE utilises the services of its Security Module for aspects of this functionality.

441 1.4.5.3 Integrity and Authenticity protection

442 The Gateway provides the following authenticity and integrity protection:

- 443 • Verification of authenticity and integrity when receiving Meter Data from a Meter  
444 via the LMN, to verify that the Meter Data have been sent from an authentic  
445 Meter and have not been altered during transmission. The TOE utilises the ser-  
446 vices of its Security Module for aspects of this functionality.
- 447 • Application of authenticity and integrity protection measures when sending pro-  
448 cessed Meter Data to an external entity, to enable the external entity to verify  
449 that the processed Meter Data have been sent from an authentic Gateway and  
450 have not been changed during transmission. The TOE utilises the services of  
451 its Security Module for aspects of this functionality.
- 452 • Verification of authenticity and integrity when receiving data from an external  
453 entity (e.g. configuration settings or firmware updates) to verify that the data  
454 have been sent from an authentic and authorised external entity and have not  
455 been changed during transmission. The TOE utilises the services of its Security  
456 Module for aspects of this functionality.

457 These functionalities

- 458 • prevent within the Smart Metering System that data may be sent by a non-  
459 authentic component without the possibility that the data recipient can detect  
460 this,

- 460
- facilitate the integrity of billing processes and serve for the interests of the consumer as well as for the interest of the supplier. Both parties are interested in the transmission of correct processed Meter Data to be used for billing,

461

462

463

    - protect the Smart Metering System and a corresponding large scale Smart Grid infrastructure by preventing that data (e.g. Meter Data, configuration settings, or firmware updates) from forged components (with the aim to cause damage to the Smart Grid) will be accepted in the system.

464

465

466

#### 467 1.4.5.4 Information flow control and firewall

468 The Gateway separates devices in the LAN of the consumer from the WAN and enforces  
469 the following information flow control to control the communication between the networks  
470 that the Gateway is attached to:

- only the Gateway may establish a connection to an external entity in the WAN<sup>14</sup>; specifically connection establishment by an external entity in the WAN or a Meter in the LMN to the WAN is not possible,
  - the Gateway can establish connections to devices in the LMN or in the HAN,
  - Meters in the LMN are only allowed to establish a connection to the Gateway,
  - the Gateway shall offer a wake-up service that allows external entities in the WAN to trigger a connection establishment by the Gateway,
  - connections are allowed to pre-configured addresses only,
  - only cryptographically-protected (i.e. encrypted, integrity protected and mutually authenticated) connections are possible.<sup>15</sup>
- 471
- 472
- 473
- 474
- 475
- 476
- 477
- 478
- 479
- 480

481 These functionalities

- prevent that the Gateway itself or the components behind the Gateway (i.e. Meters or Controllable Local Systems) can be conquered by a WAN attacker (as defined in section 3.4), that processed data are transmitted to the wrong external entity, and that processed data are transmitted without being confidentiality/authenticity/integrity-protected,
  - protect the Smart Metering System and a corresponding large scale infrastructure in two ways: by preventing that conquered components will send forged
- 482
- 483
- 484
- 485
- 486
- 487
- 488

---

<sup>14</sup> Please note that this does not affect the functionality for a CLS to establish a secure channel to a party in the WAN. Technically however, this channel is established by the TOE who acts as a proxy between the CLS and the WAN.

<sup>15</sup> To establish an encrypted channel the TOE may use the required protocols such as DHCP or PPP. Beside the establishment of an encrypted channel no unprotected communication between the TOE and external entities located in the WAN or LAN is allowed.



489 Meter Data (with the aim to cause damage to the Smart Grid), and by preventing  
 490 that widely distributed Smart Metering Systems can be abused as a platform  
 491 for malicious software/firmware to attack other systems in the WAN (e.g. a WAN  
 492 attacker who would be able to install a botnet on components of the Smart Me-  
 493 tering System).

494 The communication flows that are enforced by the Gateway between parties in the HAN,  
 495 LMN and WAN are summarized in the following table<sup>16</sup>:

Source(1 <sup>st</sup> column) Destination (1 <sup>st</sup> row)	WAN	LMN	HAN
WAN	- (see following list)	No connection establishment allowed	No connection establishment allowed
LMN	No connection establishment allowed	- (see following list)	No connection establishment allowed
HAN	Connection establishment is allowed to trustworthy, pre-configured endpoints and via an encrypted channel only <sup>17</sup>	No connection establishment allowed	- (see following list)

496 **Table 2: Communication flows between devices in different networks**

497 For communications within the different networks the following assumptions are defined:

- 498 1. Communications within the **WAN** are not restricted. However, the Gateway is  
 499 not involved in this communication,
- 500 2. No communications between devices in the **LMN** are assumed. Devices in the  
 501 LMN may only communicate to the Gateway and shall not be connected to any  
 502 other network,
- 503 3. Devices in the **HAN** may communicate with each other. However, the Gateway  
 504 is not involved in this communication. If devices in the HAN have a separate

---

16 Please note that this table only addresses the communication flow between devices in the various networks attached to the Gateway. It does not aim to provide an overview over the services that the Gateway itself offers to those devices nor an overview over the communication between devices in the same network. This information can be found in the paragraphs following the table.

17 The channel to the external entity in the WAN is established by the Gateway.

505 connection to parties in the WAN (beside the Gateway) this connection is as-  
506 sumed to be appropriately protected. It should be noted that for the case that a  
507 TOE connects to more than one HAN communications between devices within  
508 different HAN via the TOE are only allowed if explicitly configured by a Gateway  
509 Administrator.

510 Finally, the Gateway itself offers the following services within the various networks:

- 511 • the Gateway accepts the submission of Meter Data from the LMN,
- 512 • the Gateway offers a wake-up service at the WAN side as described in chapter  
513 1.4.6.5 of [PP\_GW],
- 514 • the Gateway offers a user interface to the HAN that allows CLS or consumers  
515 to connect to the Gateway in order to read relevant information.

#### 516 1.4.5.5 Wake-Up-Service

517 In order to protect the Gateway and the devices in the LAN against threats from the WAN  
518 side the Gateway implements a strict firewall policy and enforces that connections with  
519 external entities in the WAN shall only be established by the Gateway itself (e.g. when  
520 the Gateway delivers Meter Data or contacts the Gateway Administrator to check for  
521 updates)<sup>18</sup>.

522 While this policy is the optimal policy from a security perspective, the Gateway  
523 Administrator may want to facilitate applications in which an instant communication to  
524 the Gateway is required.

525 In order to allow this kind of re-activeness of the Gateway, this ST allows the Gateway  
526 to keep existing connections to external entities open (please refer to [TR-03109-3] for  
527 more details) and to offer a so called wake-up service.

528 The Gateway is able to receive a wake-up message that is signed by the Gateway  
529 Administrator. The following steps are taken:

- 530 1. The Gateway verifies the wake-up packet. This comprises
  - 531 i. a check if the header identification is correct,
  - 532 ii. the recipient is the Gateway,
  - 533 iii. the wake-up packet has been sent/received within an acceptable period  
534 of time in order to prevent replayed messages,

---

<sup>18</sup> Please note that this does not affect the functionality for a CLS to establish a secure channel to a party in the WAN. Technically however, this channel is established by the TOE who acts as a proxy between the CLS and the WAN.

- 535                   iv. the wake-up message has not been received before,  
536                   2. If the wake-up message could not be verified as described in step #1, the  
537                   message will be dropped/ignored. No further operations will be initiated and no  
538                   feedback is provided.  
539                   3. If the message could be verified as described in step #1, the signature of the  
540                   wake-up message will be verified. The Gateway uses the services of its Security  
541                   Module for signature verification.  
542                   4. If the signature of the wake-up message cannot be verified as described in step  
543                   #3 the message will be dropped/ignored. No feedback is given to the sending  
544                   external entity and the wake-up sequence terminates.  
545                   5. If the signature of the wake-up message could be verified successfully , the  
546                   Gateway initiates a connection to a pre-configured external entity; however no  
547                   feedback is given to the sending external entity.

548                   More details on the exact implementation of this mechanism can be found in [TR-03109-  
549                   1, „Wake-Up Service“].

#### 550                   1.4.5.6 Privacy Preservation

551                   The preservation of the privacy of the consumer is an essential aspect that is imple-  
552                   mented by the functionality of the TOE as required by this ST.

553                   This contains two aspects:

554                   The Processing Profiles that the TOE obeys facilitate an approach in which only a mini-  
555                   mum amount of data have to be submitted to external entities and therewith leave the  
556                   scope of control of the consumer. The mechanisms “encryption” and “pseudonymisation”  
557                   ensure that the data can only be read by the intended recipient and only contains an  
558                   association with the identity of the Meter if this is necessary.

559                   On the other hand, the TOE provides the consumer with transparent information about  
560                   the information flows that happen with their data. In order to achieve this, the TOE im-  
561                   plements a consumer log that specifically contains the information about the information  
562                   flows which has been and will be authorised based on the previous and current Pro-  
563                   cessing Profiles. The access to this consumer log is only possible via a local interface  
564                   from the HAN and after authentication of the consumer. The TOE does only allow a  
565                   consumer access to the data in the consumer log that is related to their own consumption  
566                   or production. The following paragraphs provide more details on the information that is  
567                   included in this log:

## 568 **Monitoring of Data Transfers**

569 The TOE keeps track of each data transmission in the consumer log and allows the  
570 consumer to see details on which information have been and will be sent (based on the  
571 previous and current settings) to which external entity.

## 572 **Configuration Reporting**

573 The TOE provides detailed and complete reporting in the consumer log of each security  
574 and privacy-relevant configuration setting. Additional to device specific configuration set-  
575 tings, the consumer log contains the parameters of each Processing Profile. The con-  
576 sumer log contains the configured addresses for internal and external entities including  
577 the CLS.

## 578 **Audit Log and Monitoring**

579 The TOE provides all audit data from the consumer log at the user interface  
580 IF\_GW\_CON. Access to the consumer log is only possible after successful authentica-  
581 tion and only to information that the consumer has permission to (i.e. that has been  
582 recorded based on events belonging to the consumer).

### 583 1.4.5.7 Management of Security Functions

584 The Gateway provides authorised Gateway Administrators with functionality to manage  
585 the behaviour of the security functions and to update the TOE.

586 Further, it is defined that only authorised Gateway Administrators may be able to use  
587 the management functionality of the Gateway (while the Security Module is used for the  
588 authentication of the Gateway Administrator) and that the management of the Gateway  
589 shall only be possible from the WAN side interface.

## 590 **System Status**

591 The TOE provides information on the current status of the TOE in the system log. Spe-  
592 cifically it shall indicate whether the TOE operates normally or any errors have been  
593 detected that are of relevance for the administrator.

### 594 1.4.5.8 Identification and Authentication

595 To protect the TSF as well as User Data and TSF data from unauthorized modification  
596 the TOE provides a mechanism that requires each user to be successfully identified and  
597 authenticated before allowing any other actions on behalf of that user. This functionality  
598 includes the identification and authentication of users who receive data from the

599 Gateway as well as the identification and authentication of CLS located in HAN and  
 600 Meters located in LMN.

601 The Gateway provides different kinds of identification and authentication mechanisms  
 602 that depend on the user role and the used interfaces. Most of the mechanisms require  
 603 the usage of certificates. Only consumers are able to decide whether they use certifi-  
 604 cates or username and password for identification and authentication.

605 **1.4.6 The logical interfaces of the TOE**

606 The TOE offers its functionality as outlined before via a set of external interfaces. Figure  
 607 2 also indicates the cardinality of the interfaces. The following table provides an overview  
 608 of the mandatory external interfaces of the TOE and provides additional information:

Interface Name	Description
IF_GW_CON	Via this interface the Gateway provides the consumer <sup>19</sup> with the possibility to review information that is relevant for billing or the privacy of the consumer.  Specifically the access to the consumer log is only allowed via this interface.
IF_GW_MTR	Interface between the Meter and the Gateway. The Gateway receives Meter Data via this interface. <sup>20</sup>
IF_GW_SM	The Gateway invokes the services of its Security Module via this interface.
IF_GW_CLS	CLS may use the communication services of the Gateway via this interface. The implementation of at least one interface for CLS is mandatory.
IF_GW_WAN	The Gateway submits information to authorised external entities via this interface.
IF_GW_SRV	Local interface via which the service technician has the possibility to review information that are relevant to maintain the Gateway. Specifically he has

19 Please note that this interface allows consumer (or consumer's CLS) to connect to the gateway in order to read consumer specific information.

20 Please note that an implementation of this external interface is also required in the case that Meter and Gateway are implemented within one physical device in order to allow the extension of the system by another Meter.

	read access to the system log only via this interface. He has also the possibility to view non-TSF data via this interface.
--	---

609 **Table 3: Mandatory TOE external interfaces**

610 **1.4.7 The cryptography of the TOE and its Security Module**

611 Parts of the cryptographic functionality used in the upper mentioned functions is provided  
 612 by a Security Module. The Security Module provides strong cryptographic functionality,  
 613 random number generation, secure storage of secrets and supports the authentication  
 614 of the Gateway Administrator. The Security Module is a different IT product and not part  
 615 of the TOE as described in this ST. Nevertheless, it is physically embedded into the  
 616 Gateway and protected by the same level of physical protection. The requirements  
 617 applicable to the Security Module are specified in a separate PP (see [SecModPP]).

618 The following table provides a more detailed overview on how the cryptographic  
 619 functions are distributed between the TOE and its Security Module.

Aspect	TOE	Security Module
Communication with external entities	<ul style="list-style-type: none"> <li>• encryption</li> <li>• decryption</li> <li>• hashing</li> <li>• key derivation</li> <li>• MAC generation</li> <li>• MAC verification</li> <li>• secure storage of the TLS certificates</li> </ul>	Key negotiation: <ul style="list-style-type: none"> <li>• support of the authentication of the external entity</li> <li>• secure storage of the private key</li> <li>• random number generation</li> <li>• digital signature verification and generation</li> </ul>
Communication with the consumer	<ul style="list-style-type: none"> <li>• encryption</li> <li>• decryption</li> <li>• hashing</li> <li>• key derivation</li> <li>• MAC generation</li> <li>• MAC verification</li> <li>• secure storage of the TLS certificates</li> </ul>	Key negotiation: <ul style="list-style-type: none"> <li>• support of the authentication of the consumer</li> <li>• secure storage of the private key</li> <li>• digital signature verification and generation</li> <li>• random number generation</li> </ul>

Communication with the Meter	<ul style="list-style-type: none"> <li>• encryption</li> <li>• decryption</li> <li>• hashing</li> <li>• key derivation</li> <li>• MAC generation</li> <li>• MAC verification</li> <li>• secure storage of the TLS certificates</li> </ul>	Key negotiation (in case of TLS connection): <ul style="list-style-type: none"> <li>• support of the authentication of the meter</li> <li>• secure storage of the private key</li> <li>• digital signature verification and generation</li> <li>• random number generation</li> </ul>
Signing data before submission to an external entity	<ul style="list-style-type: none"> <li>• hashing</li> </ul>	Signature creation <ul style="list-style-type: none"> <li>• secure storage of the private key</li> </ul>
Content data encryption and integrity protection	<ul style="list-style-type: none"> <li>• encryption</li> <li>• decryption</li> <li>• MAC generation</li> <li>• key derivation</li> <li>• secure storage of the public Key</li> </ul>	Key negotiation: <ul style="list-style-type: none"> <li>• secure storage of the private key</li> <li>• random number generation</li> </ul>

**Table 4: Cryptographic support of the TOE and its Security Module**

620

621

622 1.4.7.1 Content data encryption vs. an encrypted channel

623 The TOE utilises concepts of the encryption of data on the content level as well as the

624 establishment of a trusted channel to external entities.

625 As a general rule, all processed Meter Data that is prepared to be submitted to ex-

626 ternal entities is encrypted and integrity protected on a content level using CMS (ac-

627 cording to [TR-03109-1-I]).

628 Further, all communication with external entities is enforced to happen via encrypted,

629 integrity protected and mutually authenticated channels.

630 This concept of encryption on two layers facilitates use cases in which the external

631 party that the TOE communicates with is not the final recipient of the Meter Data. In



632 this way, it is for example possible that the Gateway Administrator receives Meter  
633 Data that they forward to other parties. In such a case, the Gateway Administrator is  
634 the endpoint of the trusted channel but cannot read the Meter Data.

635 Administration data that is transmitted between the Gateway Administrator and the TOE  
636 is also encrypted and integrity protected using CMS.

637 The following figure introduces the communication process between the Meter, the TOE  
638 and external entities (focussing on billing-relevant Meter Data).

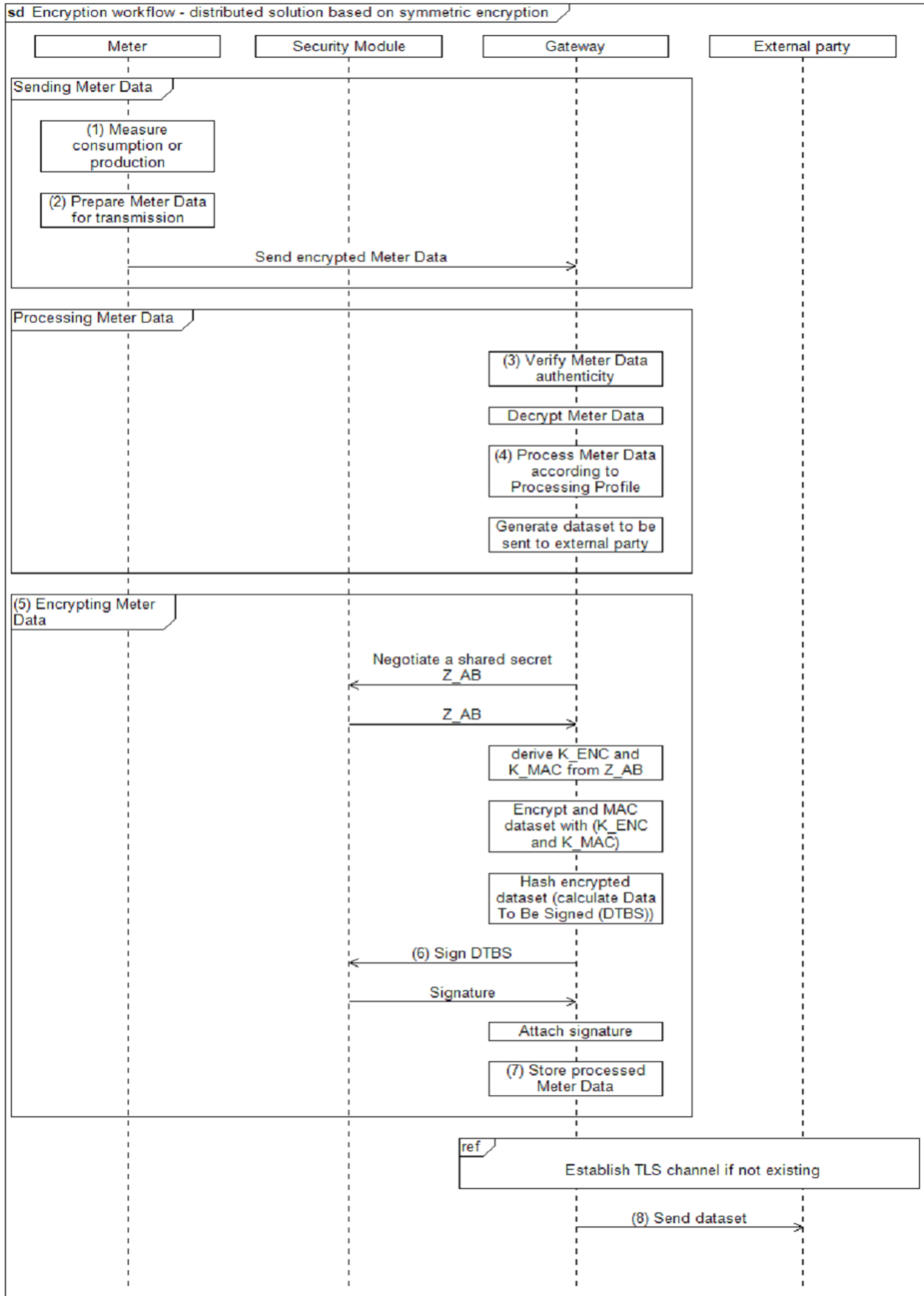
639 The basic information flow for Meter Data is as follows and shown in Figure 5:

- 640 1. The Meter measures the consumption or production of a certain commodity.
- 641 2. The Meter Data is prepared for transmission:
  - 642 a. The Meter Data is typically signed (typically using the services of an  
643 integrated Security Module).
  - 644 b. If the communication between the Meter and the Gateway is performed  
645 bidirectional, the Meter Data is transmitted via an encrypted and mutually  
646 authenticated channel to the Gateway. Please note that the submission of  
647 this information may be triggered by the Meter or the Gateway.
- 648 or
- 649 c. If a unidirectional communication is performed between the Meter and the  
650 Gateway, the Meter Data is encrypted using a symmetric algorithm  
651 (according to [TR-03109-3]) and facilitating a defined data structure to ensure  
652 the authenticity and confidentiality.
- 653 3. The authenticity and integrity of the Meter Data is verified by the Gateway.
- 654 4. If (and only if) authenticity and integrity have been verified successfully, the  
655 Meter Data is further processed by the Gateway according to the rules in the  
656 Processing Profile else the cryptographic information flow will be cancelled.
- 657 5. The processed Meter Data is encrypted and integrity protected using CMS  
658 (according to [TR-03109-1-I]) for the final recipient of the data<sup>21</sup>.
- 659 6. The processed Meter Data is signed using the services of the Security Module.
- 660 7. The processed and signed Meter Data may be stored for a certain amount of  
661 time.

---

21 Optionally the Meter Data can additionally be signed before any encryption is done.

- 662 8. The processed Meter Data is finally submitted to an authorised external entity  
 663 in the WAN via an encrypted and mutually authenticated channel.



664  
 665 **Figure 5: Cryptographic information flow for distributed Meters and Gateway**  
 666

667 **TOE life-cycle**

668 The life-cycle of the TOE can be separated into the following phases:

- 669 1. Development
- 670 2. Production
- 671 3. Pre-personalization at the developer's premises (without Security Module)
- 672 4. Pre-personalization and integration of Security Module
- 673 5. Installation and start of operation
- 674 6. Personalization
- 675 7. Normal operation

676 A detailed description of the phases #1 to #4 and #6 to #7 is provided in [TR-03109-1-  
677 VI], while phase #5 is described in the TOE manuals.

678 The TOE will be delivered after phase “Pre-personalization and integration of Security  
679 Module”. The phase “Personalization” will be performed when the TOE is started for the  
680 first time after phase “Installation and start of operation”. The TOE delivery process is  
681 specified in [AGD\_SEC].

## 682 2 Conformance Claims

### 683 2.1 CC Conformance Claim

- 684 • This ST has been developed using Version 3.1 Revision 5 of Common Criteria  
685 [CC].
- 686 • This ST is [CC] part 2 extended due to the use of FPR\_CON.1.
- 687 • This ST claims conformance to [CC] part 3; no extended assurance compo-  
688 nents have been defined.

689

### 690 2.2 PP Claim / Conformance Statement

691 This Security Target claims strict conformance to Protection Profile [PP\_GW].

692

### 693 2.3 Package Claim

694 This Security Target claims an assurance package EAL4 augmented by AVA\_VAN.5  
695 and ALC\_FLR.2 as defined in [CC] Part 3 for product certification.

696

### 697 2.4 Conformance Claim Rationale

698 This Security Target claims strict conformance to only one PP [PP\_GW].

699 This Security Target is consistent to the TOE type according to [PP\_GW] because the  
700 TOE is a communication Gateway that provides different external communication inter-  
701 faces and enables the data communication between these interfaces and connected IT  
702 systems. It further collects processes, and stores Meter Data.

703 This Security Target is consistent to the security problem defined in [PP\_GW].

704 This Security Target is consistent to the security objectives stated in [PP\_GW], no secu-  
705 rity objective of the PP is removed, nor added to this Security Target.

706 This Security Target is consistent to the security requirements stated in [PP\_GW], no  
707 security requirement of the PP is removed, nor added to this Security Target.

708

## 709 3 Security Problem Definition

### 710 3.1 External entities

711 The following external entities interact with the system consisting of Meter and Gateway.  
 712 Those roles have been defined for the use in this Security Target. It is possible that a  
 713 party implements more than one role in practice.

Role	Description
Consumer	The authorised individual or organization that “owns” the Meter Data. In most cases, this will be tenants or house owners consuming electricity, water, gas or further commodities. However, it is also possible that the consumer produces or stores energy (e.g. with their own solar plant).
Gateway Administrator	Authority that installs, configures, monitors, and controls the Smart Meter Gateway.
Service Technician	The authorised individual that is responsible for diagnostic purposes.
Authorised External Entity / User	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary. In the context of this ST, the term <i>user</i> or <i>external entity</i> serve as a hypernym for all entities mentioned before.

714 **Table 5: Roles used in the Security Target**

715

### 716 3.2 Assets

717 The following tables introduces the relevant assets for this Security Target. The tables  
 718 focus on the assets that are relevant for the Gateway and does not claim to provide an  
 719 overview over all assets in the Smart Metering System or for other devices in the LMN.

720 The following Table 6 lists all assets typified as “user data”:

721

Asset	Description	Need for Protection
Meter Data	<p>Meter readings that allow calculation of the quantity of a commodity, e.g. electricity, gas, water or heat consumed over a period.</p> <p>Meter Data comprise Consumption or Production Data (billing-relevant) and grid status data (not billing-relevant).</p> <p>While billing-relevant data needs to have a relation to the Consumer, grid status data do not have to be directly related to a Consumer.</p>	<ul style="list-style-type: none"> <li>• According to their specific need (see below)</li> </ul>
System log data	<p>Log data from the</p> <ul style="list-style-type: none"> <li>• system log.</li> </ul>	<ul style="list-style-type: none"> <li>• Integrity</li> <li>• Confidentiality (only authorised SMGW administrators and Service technicians may read the log data)</li> </ul>
Consumer log data	<p>Log data from the</p> <ul style="list-style-type: none"> <li>• consumer log.</li> </ul>	<ul style="list-style-type: none"> <li>• Integrity</li> <li>• Confidentiality (only authorised Consumers may read the log data)</li> </ul>
Calibration log data	<p>Log data from the</p> <ul style="list-style-type: none"> <li>• calibration log.</li> </ul>	<ul style="list-style-type: none"> <li>• Integrity</li> <li>• Confidentiality (only authorised SMGW administrators may read the log data)</li> </ul>
Consumption Data	<p>Billing-relevant part of Meter Data. Please note that the term <i>Consumption Data</i> implicitly includes Production Data.</p>	<ul style="list-style-type: none"> <li>• Integrity and authenticity (comparable to the classical meter and its security requirements)</li> <li>• Confidentiality (due to privacy concerns)</li> </ul>

Status Data	Grid status data, subset of Meter Data that is not billing-relevant <sup>22</sup> .	<ul style="list-style-type: none"> <li>• Integrity and authenticity (comparable to the classical meter and its security requirements)</li> <li>• Confidentiality (due to privacy concerns)</li> </ul>
Supplementary Data	The Gateway may be used for communication purposes by devices in the LMN or HAN. It may be that the functionality of the Gateway that is used by such a device is limited to pure (but secure) communication services. Data that is transmitted via the Gateway but that does not belong to one of the aforementioned data types is named <i>Supplementary Data</i> .	<ul style="list-style-type: none"> <li>• According to their specific need</li> </ul>
Data	The term <i>Data</i> is used as hypernym for <i>Meter Data and Supplementary Data</i> .	<ul style="list-style-type: none"> <li>• According to their specific need</li> </ul>
Gateway time	Date and time of the real-time clock of the Gateway. Gateway Time is used in Meter Data records sent to external entities.	<ul style="list-style-type: none"> <li>• Integrity</li> <li>• Authenticity (when time is adjusted to an external reference time)</li> </ul>
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.	<ul style="list-style-type: none"> <li>• Confidentiality</li> </ul>

722 **Table 6: Assets (User data)**

723 Table 7 lists all assets typified as “TSF data”:

---

<sup>22</sup> Please note that these readings and data of the Meter which are not relevant for billing may require an explicit endorsement of the consumer(s).



Asset	Description	Need for Protection
Meter config (secondary asset)	Configuration data of the Meter to control its behaviour including the Meter identity. Configuration data is transmitted to the Meter via the Gateway.	<ul style="list-style-type: none"> <li>• Integrity and authenticity</li> <li>• Confidentiality</li> </ul>
Gateway config (secondary asset)	Configuration data of the Gateway to control its behaviour including the Gateway identity, the Processing Profiles and certificate/key material for authentication.	<ul style="list-style-type: none"> <li>• Integrity and authenticity</li> <li>• Confidentiality</li> </ul>
CLS config (secondary asset)	Configuration data of a CLS to control its behaviour. Configuration data is transmitted to the CLS via the Gateway.	<ul style="list-style-type: none"> <li>• Integrity and authenticity</li> <li>• Confidentiality</li> </ul>
Firmware update (secondary asset)	Firmware update that is downloaded by the TOE to update the firmware of the TOE.	<ul style="list-style-type: none"> <li>• Integrity and authenticity</li> </ul>
Ephemeral keys (secondary asset)	Ephemeral cryptographic material used by the TOE for cryptographic operations.	<ul style="list-style-type: none"> <li>• Integrity and authenticity</li> <li>• Confidentiality</li> </ul>

724

**Table 7: Assets (TSF data)**

725

## 726 3.3 Assumptions

727 In this threat model the following assumptions about the environment of the components  
728 need to be taken into account in order to ensure a secure operation.

729 **A.ExternalPrivacy** It is assumed that authorised and authenticated external  
730 entities receiving any kind of privacy-relevant data or bill-  
731 ing-relevant data and the applications that they operate are  
732 trustworthy (in the context of the data that they receive) and  
733 do not perform unauthorised analyses of this data with re-  
734 spect to the corresponding Consumer(s).

735 **A.TrustedAdmins** It is assumed that the Gateway Administrator and the Ser-  
736 vice Technician are trustworthy and well-trained.

737 **A.PhysicalProtection** It is assumed that the TOE is installed in a non-public en-  
738 vironment within the premises of the Consumer which pro-  
739 vides a basic level of physical protection. This protection  
740 covers the TOE, the Meter(s) that the TOE communicates  
741 with and the communication channel between the TOE and  
742 its Security Module.

743 **A.ProcessProfile** The Processing Profiles that are used when handling data  
744 are assumed to be trustworthy and correct.

745 **A.Update** It is assumed that firmware updates for the Gateway that  
746 can be provided by an authorised external entity have un-  
747 dergone a certification process according to this Security  
748 Target before they are issued and can therefore be as-  
749 sumed to be correctly implemented. It is further assumed  
750 that the external entity that is authorised to provide the up-  
751 date is trustworthy and will not introduce any malware into  
752 a firmware update.

753 **A.Network** It is assumed that

- 754 • a WAN network connection with a sufficient reliabil-  
755 ity and bandwidth for the individual situation is  
756 available,
- 757 • one or more trustworthy sources for an update of  
758 the system time are available in the WAN,

- 759
- 760
- 761
- 762
- 763
- the Gateway is the only communication gateway for Meters in the LMN<sup>23</sup>,
  - if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

764 **A.Keygen**

It is assumed that the ECC key pair for a Meter (TLS) is generated securely according to [TR-03109-3] and brought into the Gateway in a secure way by the Gateway Administrator.

768 **Application Note 1:**

This ST acknowledges that the Gateway cannot be completely protected against unauthorised physical access by its environment. However, it is important for the overall security of the TOE that it is not installed within a public environment.

773 The level of physical protection that is expected to be provided by the environment is the same level of protection that is expected for classical meters that operate according to the regulations of the national calibration authority [TR-03109-1].

778 **Application Note 2:**

779 The Processing Profiles that are used for information flow control as referred to by A.ProcessProfile are an essential factor for the preservation of the privacy of the Consumer.

780 The Processing Profiles are used to determine which data shall be sent to which entity at which frequency and how

781 data are processed, e.g. whether the data needs to be related to the Consumer (because it is used for billing purposes) or whether the data shall be pseudonymised.

782 The Processing Profiles shall be visible for the Consumer

783 to allow a transparent communication.

784

785

786

787

---

23 Please note that this assumption holds on a logical level rather than on a physical one. It may be possible that the Meters in the LMN have a physical connection to other devices that would in theory also allow a communication. This is specifically true for wireless communication technologies. It is further possible that signals of Meters are amplified by other devices or other Meters on the physical level without violating this assumption. However, it is assumed that the Meters do only communicate with the TOE and that only the TOE is able to decrypt the data sent by the Meter.

788 It is essential that Processing Profiles correctly define the  
789 amount of information that must be sent to an external en-  
790 tity. Exact regulations regarding the Processing Profiles  
791 and the Gateway Administrator are beyond the scope of  
792 this Security Target.

793

### 794 **3.4 Threats**

795 The following sections identify the threats that are posed against the assets handled by  
796 the Smart Meter System. Those threats are the result of a threat model that has been  
797 developed for the whole Smart Metering System first and then has been focussed on  
798 the threats against the Gateway. It should be noted that the threats in the following par-  
799 agraphs consider two different kinds of attackers:

- 800 • Attackers having physical access to Meter, Gateway, a connection between  
801 these components or local logical access to any of the interfaces (local at-  
802 tacker), trying to disclose or alter assets while stored in the Gateway or while  
803 transmitted between Meters in the LMN and the Gateway. Please note that the  
804 following threat model assumes that the local attacker has less motivation than  
805 the WAN attacker as a successful attack of a local attacker will always only  
806 impact one Gateway. Please further note that the local attacker includes au-  
807 thorised individuals like consumers.
- 808 • An attacker located in the WAN (WAN attacker) trying to compromise the con-  
809 fidentiality and/or integrity of the processed Meter Data and or configuration  
810 data transmitted via the WAN, or attacker trying to conquer a component of the  
811 infrastructure (i.e. Meter, Gateway or Controllable Local System) via the WAN  
812 to cause damage to a component itself or to the corresponding grid (e.g. by  
813 sending forged Meter Data to an external entity).

814 The specific rationale for this situation is given by the expected benefit of a successful  
815 attack. An attacker who has to have physical access to the TOE that they are attacking,  
816 will only be able to compromise one TOE at a time. So the effect of a successful attack  
817 will always be limited to the attacked TOE. A logical attack from the WAN side on the  
818 other hand may have the potential to compromise a large amount of TOEs.

819

820	<b>T.DataModificationLocal</b>	A local attacker may try to modify (i.e. alter, delete, insert,
821		replay or redirect) Meter Data when transmitted between
822		Meter and Gateway, Gateway and Consumer, or Gateway
823		and external entities. The objective of the attacker may be
824		to alter billing-relevant information or grid status infor-
825		mation. The attacker may perform the attack via any inter-
826		face (LMN, HAN, or WAN).
827		In order to achieve the modification, the attacker may also
828		try to modify secondary assets like the firmware or config-
829		uration parameters of the Gateway.
830	<b>T.DataModificationWAN</b>	A WAN attacker may try to modify (i.e. alter, delete, insert,
831		replay or redirect) Meter Data, Gateway config data, Meter
832		config data, CLS config data or a firmware update when
833		transmitted between the Gateway and an external entity in
834		the WAN.
835		When trying to modify Meter Data, it is the objective of the
836		WAN attacker to modify billing-relevant information or grid
837		status data.
838		When trying to modify config data or a firmware update, the
839		WAN attacker tries to circumvent security mechanisms of
840		the TOE or tries to get control over the TOE or a device in
841		the LAN that is protected by the TOE.
842	<b>T.TimeModification</b>	A local attacker or WAN attacker may try to alter the Gate-
843		way time. The motivation of the attacker could be e.g. to
844		change the relation between date/time and measured con-
845		sumption or production values in the Meter Data records
846		(e.g. to influence the balance of the next invoice).
847	<b>T.DisclosureWAN</b>	A WAN attacker may try to violate the privacy of the Con-
848		sumer by disclosing Meter Data or configuration data (Me-
849		ter config, Gateway config or CLS config) or parts of it
850		when transmitted between Gateway and external entities
851		in the WAN.

852	<b>T.DisclosureLocal</b>	A local attacker may try to violate the privacy of the Consumer by disclosing Meter Data transmitted between the TOE and the Meter. This threat is of specific importance if Meters of more than one Consumer are served by one Gateway.
853		
854		
855		
856		
857	<b>T.Infrastructure</b>	A WAN attacker may try to obtain control over Gateways, Meters or CLS via the TOE, which enables the WAN attacker to cause damage to Consumers or external entities or the grids used for commodity distribution (e.g. by sending wrong data to an external entity).
858		
859		
860		
861		
862		A WAN attacker may also try to conquer a CLS in the HAN first in order to logically attack the TOE from the HAN side.
863		
864	<b>T.ResidualData</b>	By physical and/or logical means a local attacker or a WAN attacker may try to read out data from the Gateway, which travelled through the Gateway before and which are no longer needed by the Gateway (i.e. Meter Data, Meter config, or CLS config).
865		
866		
867		
868		
869	<b>T.ResidentData</b>	A WAN or local attacker may try to access (i.e. read, alter, delete) information to which they don't have permission to while the information is stored in the TOE.
870		
871		
872		While the WAN attacker only uses the logical interface of the TOE that is provided into the WAN, the local attacker may also physically access the TOE.
873		
874		
875	<b>T.Privacy</b>	A WAN attacker may try to obtain more detailed information from the Gateway than actually required to fulfil the tasks defined by its role or the contract with the Consumer. This includes scenarios in which an external entity that is primarily authorised to obtain information from the TOE tries to obtain more information than the information that has been authorised as well as scenarios in which an attacker who is not authorised at all tries to obtain information.
876		
877		
878		
879		
880		
881		
882		
883		
884		

### 885 3.5 Organizational Security Policies

886 This section lists the organizational security policies (OSP) that the Gateway shall com-  
887 ply with:

888 **OSP.SM** The TOE shall use the services of a certified Security Mod-  
889 ule for

- 890 • verification of digital signatures,
- 891 • generation of digital signatures,
- 892 • key agreement,
- 893 • key transport,
- 894 • key storage,
- 895 • Random Number Generation,

896 The Security Module shall be certified according to  
897 [SecModPP] and shall be used in accordance with its rele-  
898 vant guidance documentation.

899 **OSP.Log** The TOE shall maintain a set of log files as defined in [TR-  
900 03109-1] as follows:

- 901 1. A system log of relevant events in order to allow an  
902 authorised Gateway Administrator to analyse the  
903 status of the TOE. The TOE shall also analyse the  
904 system log automatically for a cumulation of secu-  
905 rity relevant events.
- 906 2. A consumer log that contains information about the  
907 information flows that have been initiated to the  
908 WAN and information about the Processing Profiles  
909 causing this information flow as well as the billing-  
910 relevant information.
- 911 3. A calibration log (as defined in chapter 6.2.1) that  
912 provides the Gateway Administrator with a possibil-  
913 ity to review calibration relevant events.

914 The TOE shall further limit access to the information in the  
915 different log files as follows:

- 916 1. Access to the information in the system log shall  
917 only be allowed for an authorised Gateway

918 Administrator via the IF\_GW\_WAN interface of the  
919 TOE and an authorised Service Technician via the  
920 IF\_GW\_SRV interface of the TOE.

921 2. Access to the information in the calibration log shall  
922 only be allowed for an authorised Gateway Admin-  
923 istrator via the IF\_GW\_WAN interface of the TOE.

924 3. Access to the information in the consumer log shall  
925 only be allowed for an authorised Consumer via the  
926 IF\_GW\_CON interface of the TOE. The Consumer  
927 shall only have access to their own information.

928 The system log may overwrite the oldest events in case  
929 that the audit trail gets full.

930 For the consumer log the TOE shall ensure that a sufficient  
931 amount of events is available (in order to allow a Consumer  
932 to verify an invoice) but may overwrite older events in case  
933 that the audit trail gets full.

934 For the calibration log, however, the TOE shall ensure the  
935 availability of all events over the lifetime of the TOE.



## 936 4 Security Objectives

### 937 4.1 Security Objectives for the TOE

#### 938 O.Firewall

939 The TOE shall serve as the connection point for the con-  
940 nected devices within the LAN to external entities within  
941 the WAN and shall provide firewall functionality in order to  
942 protect the devices of the LMN and HAN (as long as they  
943 use the Gateway) and itself against threats from the WAN  
944 side.

944 The firewall:

- 945 • shall allow only connections established from HAN  
946 or the TOE itself to the WAN (i.e. from devices in  
947 the HAN to external entities in the WAN or from the  
948 TOE itself to external entities in the WAN),
- 949 • shall provide a wake-up service on the WAN side  
950 interface,
- 951 • shall not allow connections from the LMN to the  
952 WAN,
- 953 • shall not allow any other services being offered on  
954 the WAN side interface,
- 955 • shall not allow connections from the WAN to the  
956 LAN or to the TOE itself,
- 957 • shall enforce communication flows by allowing traf-  
958 fic from CLS in the HAN to the WAN only if confi-  
959 dentiality-protected and integrity-protected and if  
960 endpoints are authenticated.

#### 961 O.SeparateIF

962 The TOE shall have physically separated ports for the  
963 LMN, the HAN and the WAN and shall automatically detect  
964 during its self test whether connections (wired or wireless),  
if any, are wrongly connected.

965 **Application Note 3:** O.SeparateIF refers to physical inter-  
966 faces and must not be fulfilled by a pure logical separation  
967 of one physical interface only.

968	<b>O.Conceal</b>	To protect the privacy of its Consumers, the TOE shall conceal the communication with external entities in the WAN in order to ensure that no privacy-relevant information may be obtained by analysing the frequency, load, size or the absence of external communication. <sup>24</sup>
969		
970		
971		
972		
973	<b>O.Meter</b>	The TOE receives or polls information about the consumption or production of different commodities from one or multiple Meters and is responsible for handling this Meter Data.
974		
975		
976		
977		This includes that:
978		<ul style="list-style-type: none"><li>• The TOE shall ensure that the communication to the Meter(s) is established in an Gateway Administrator-definable interval or an interval as defined by the Meter,</li></ul>
979		<ul style="list-style-type: none"><li>• the TOE shall enforce encryption and integrity protection for the communication with the Meter<sup>25</sup>,</li></ul>
980		<ul style="list-style-type: none"><li>• the TOE shall verify the integrity and authenticity of the data received from a Meter before handling it further,</li></ul>
981		<ul style="list-style-type: none"><li>• the TOE shall process the data according to the definition in the corresponding Processing Profile,</li></ul>
982		<ul style="list-style-type: none"><li>• the TOE shall encrypt the processed Meter Data for the final recipient, sign the data and</li></ul>
983		<ul style="list-style-type: none"><li>• deliver the encrypted data to authorised external entities as defined in the corresponding Processing Profiles facilitating an encrypted channel,</li></ul>
984		<ul style="list-style-type: none"><li>• the TOE shall store processed Meter Data if an external entity cannot be reached and re-try to send</li></ul>
985		
986		
987		
988		
989		
990		
991		
992		
993		
994		
995		

---

<sup>24</sup> It should be noted that this requirement only applies to communication flows in the WAN.

<sup>25</sup> It is acknowledged that the implementation of a secure channel between the Meter and the Gateway is a security function of both units. The TOE as defined in this Security Target only has a limited possibility to secure this communication as both sides have to sign responsible for the quality of a cryptographic connection. However, it should be noted that the encryption of this channel only needs to protect against the Local Attacker possessing a basic attack potential and that the Meter utilises the services of its Security Module to negotiate the channel.

996 the data until a configurable number of unsuccessful  
 997 retrials has been reached,  
 998 • the TOE shall pseudonymize the data for parties  
 999 that do not need the relation between the pro-  
 1000 cessed Meter Data and the identity of the Con-  
 1001 sumer.

## 1002 **O.Crypt**

1003 The TOE shall provide cryptographic functionality as fol-  
 1004 lows:

- 1004 • authentication, integrity protection and encryption  
 1005 of the communication and data to external entities  
 1006 in the WAN,
- 1007 • authentication, integrity protection and encryption  
 1008 of the communication to the Meter,
- 1009 • authentication, integrity protection and encryption  
 1010 of the communication to the Consumer,
- 1011 • replay detection for all communications with exter-  
 1012 nal entities,
- 1013 • encryption of the persistently stored TSF and user  
 1014 data of the TOE<sup>26</sup>.

1015 In addition, the TOE shall generate the required keys uti-  
 1016 lising the services of its Security Module<sup>27</sup>, ensure that the  
 1017 keys are only used for an acceptable amount of time and  
 1018 destroy ephemeral<sup>28</sup> keys if no longer needed.<sup>29</sup>

## 1019 **O.Time**

1020 The TOE shall provide reliable time stamps and update  
 1021 its internal clock in regular intervals by retrieving reliable  
 1022 time information from a dedicated reliable source in the  
 WAN.

---

26 The encryption of the persistent memory shall support the protection of the TOE against local attacks.

27 Please refer to chapter 1.4.7 for an overview on how the cryptographic functions are distributed between the TOE and its Security Module.

28 This objective addresses the destruction of ephemeral keys only because all keys that need to be stored persistently are stored in the Security Module.

29 Please refer to chapter F.9 of part 2 of [CC] for more detailed information about what kind of information this objective applies to.

1023	<b>O.Protect</b>	The TOE shall implement functionality to protect its security functions against malfunctions and tampering.
1024		
1025		Specifically, the TOE shall
1026		<ul style="list-style-type: none"> <li>• encrypt its TSF and user data as long as it is not in use,</li> </ul>
1027		
1028		<ul style="list-style-type: none"> <li>• overwrite any information that is no longer needed to ensure that it is no longer available via the external interfaces of the TOE<sup>30</sup>,</li> </ul>
1029		
1030		
1031		<ul style="list-style-type: none"> <li>• monitor user data and the TOE firmware for integrity errors,</li> </ul>
1032		
1033		<ul style="list-style-type: none"> <li>• contain a test that detects whether the interfaces for WAN and LAN are separate,</li> </ul>
1034		
1035		<ul style="list-style-type: none"> <li>• have a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g. energy, gas, heat or water)<sup>31</sup>,</li> </ul>
1036		
1037		
1038		<ul style="list-style-type: none"> <li>• make any physical manipulation within the scope of the intended environment detectable for the Consumer and Gateway Administrator.</li> </ul>
1039		
1040		
1041	<b>O.Management</b>	The TOE shall only provide authorised Gateway Administrators with functions for the management of the security features.
1042		
1043		
1044		The TOE shall ensure that any change in the behaviour of the security functions can only be achieved from the WAN side interface. Any management activity from a local interface may only be read only.
1045		
1046		
1047		
1048		Further, the TOE shall implement a secure mechanism to update the firmware of the TOE that ensures that only authorised entities are able to provide updates for the TOE
1049		
1050		

---

<sup>30</sup> Please refer to chapter F.9 of part 2 of [CC] for more detailed information about what kind of information this objective applies to.

<sup>31</sup> Indeed this Security Target acknowledges that the Gateway and the Meters have no possibility at all to impact the delivery of a commodity. Even an intentional stop of the delivery of a certain commodity is not within the scope of this Security Target. It should however be noted that such a functionality may be realised by a CLS that utilises the services of the TOE for its communication.

1051 and that only authentic and integrity protected updates are  
1052 applied.

1053 **O.Log**

1054 The TOE shall maintain a set of log files as defined in [TR-  
1055 03109-1] as follows:

- 1056 1. A system log of relevant events in order to allow an  
1057 authorised Gateway Administrator or an authorised  
1058 Service Technician to analyse the status of the  
1059 TOE. The TOE shall also analyse the system log  
1060 automatically for a cumulation of security relevant  
1061 events.
- 1062 2. A consumer log that contains information about the  
1063 information flows that have been initiated to the  
1064 WAN and information about the Processing Profiles  
1065 causing this information flow as well as the billing-  
1066 relevant information and information about the sys-  
1067 tem status (including relevant error messages).
- 1068 3. A calibration log that provides the Gateway Admin-  
1069 istrator with a possibility to review calibration rele-  
1070 vant events.

1070 The TOE shall further limit access to the information in the  
1071 different log files as follows:

- 1072 1. Access to the information in the system log shall  
1073 only be allowed for an authorised Gateway Admin-  
1074 istrator via IF\_GW\_WAN or for an authorised Ser-  
1075 vice Technician via IF\_GW\_SRV.
- 1076 2. Access to the information in the consumer log shall  
1077 only be allowed for an authorised Consumer via the  
1078 IF\_GW\_CON interface of the TOE and via a se-  
1079 cured (i.e. confidentiality and integrity protected)  
1080 connection. The Consumer shall only have access  
1081 to their own information.
- 1082 3. Read-only access to the information in the calibra-  
1083 tion log shall only be allowed for an authorised

1084 Gateway Administrator via the WAN interface of the  
1085 TOE.

1086 The system log may overwrite the oldest events in case  
1087 that the audit trail gets full.

1088 For the consumer log, the TOE shall ensure that a suffi-  
1089 cient amount of events is available (in order to allow a Con-  
1090 sumer to verify an invoice) but may overwrite older events  
1091 in case that the audit trail gets full.

1092 For the calibration log however, the TOE shall ensure the  
1093 availability of all events over the lifetime of the TOE.

1094 **O.Access** The TOE shall control the access of external entities in  
1095 WAN, HAN or LMN to any information that is sent to, from  
1096 or via the TOE via its external interfaces<sup>32</sup>. Access control  
1097 shall depend on the destination interface that is used to  
1098 send that information.

1099

## 1100 4.2 Security Objectives for the Operational Environment

1101 **OE.ExternalPrivacy** Authorised and authenticated external entities receiving  
1102 any kind of private or billing-relevant data shall be trustwor-  
1103 thy and shall not perform unauthorised analyses of these  
1104 data with respect to the corresponding consumer(s).

1105 **OE.TrustedAdmins** The Gateway Administrator and the Service Technician  
1106 shall be trustworthy and well-trained.

1107 **OE.PhysicalProtection** The TOE shall be installed in a non-public environment  
1108 within the premises of the Consumer that provides a basic  
1109 level of physical protection. This protection shall cover the  
1110 TOE, the Meters that the TOE communicates with and the  
1111 communication channel between the TOE and its Security

---

<sup>32</sup> While in classical access control mechanisms the Gateway Administrator gets complete access, the TOE also maintains a set of information (specifically the consumer log) to which Gateway Administrators have restricted access.

1112		Module. Only authorised individuals may physically access
1113		the TOE.
1114	<b>OE.Profile</b>	The Processing Profiles that are used when handling data
1115		shall be obtained from a trustworthy and reliable source
1116		only.
1117	<b>OE.SM</b>	The environment shall provide the services of a certified
1118		Security Module for
1119		<ul style="list-style-type: none"><li>• verification of digital signatures,</li></ul>
1120		<ul style="list-style-type: none"><li>• generation of digital signatures,</li></ul>
1121		<ul style="list-style-type: none"><li>• key agreement,</li></ul>
1122		<ul style="list-style-type: none"><li>• key transport,</li></ul>
1123		<ul style="list-style-type: none"><li>• key storage,</li></ul>
1124		<ul style="list-style-type: none"><li>• Random Number Generation.</li></ul>
1125		The Security Module used shall be certified according to
1126		[SecModPP] and shall be used in accordance with its rele-
1127		vant guidance documentation.
1128	<b>OE.Update</b>	The firmware updates for the Gateway that can be pro-
1129		vided by an authorised external entity shall undergo a cer-
1130		tification process according to this Security Target before
1131		they are issued to show that the update is implemented
1132		correctly. The external entity that is authorised to provide
1133		the update shall be trustworthy and ensure that no mal-
1134		ware is introduced via a firmware update.
1135	<b>OE.Network</b>	It shall be ensured that
1136		<ul style="list-style-type: none"><li>• a WAN network connection with a sufficient reliabil-</li></ul>
1137		ity and bandwidth for the individual situation is
1138		available,
1139		<ul style="list-style-type: none"><li>• one or more trustworthy sources for an update of</li></ul>
1140		the system time are available in the WAN,
1141		<ul style="list-style-type: none"><li>• the Gateway is the only communication gateway for</li></ul>
1142		Meters in the LMN,

- 1143 if devices in the HAN have a separate connection
- 1144 to parties in the WAN (beside the Gateway) this
- 1145 connection is appropriately protected.

1146 **OE.Keygen** It shall be ensured that the ECC key pair for a Meter (TLS)

1147 is generated securely according to the [TR-03109-3]. It

1148 shall also be ensured that the keys are brought into the

1149 Gateway in a secure way by the Gateway Administrator.

1150

### 1151 4.3 Security Objective Rationale

#### 1152 4.3.1 Overview

1153 The following table gives an overview how the assumptions, threats, and organisational

1154 security policies are addressed by the security objectives. The text of the following sec-

1155 tions justifies this more in detail.

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	OE.SM	OE.ExternalPrivacy	OE.TrustedAdmins	OE.Physical Protec-	OE.Profile	OE.Update	OE.Network	OE.Keygen
T.DataModification-Local				X	X		X	X					X	X				
T.DataModification-WAN	X				X		X	X					X					
T.TimeModification					X	X	X	X					X	X				
T.DisclosureWAN	X		X		X		X	X					X					
T.DisclosureLocal				X	X		X	X					X	X				
T.Infrastructure	X	X		X	X		X	X					X					
T.ResidualData							X	X					X					



T.ResidentData	X				X		X	X		X			X	X				
T.Privacy	X		X	X	X		X	X					X		X			
OSP.SM					X		X	X		X			X					
OSP.Log							X	X	X	X			X					
A.ExternalPrivacy													X					
A.TrustedAdmins													X					
A.PhysicalProtection														X				
A.ProcessProfile															X			
A.Update																X		
A.Network																	X	
A.Keygen																		X

1156 **Table 8: Rationale for Security Objectives**

1157

1158 **4.3.2 Countering the threats**

1159 The following sections provide more detailed information on how the threats are coun-  
 1160 tered by the security objectives for the TOE and its operational environment.

1161

1162 4.3.2.1 General objectives

1163 The security objectives **O.Protect**, **O.Management** and **OE.TrustedAdmins** contribute  
 1164 to counter each threat and contribute to each OSP.

1165 **O.Management** is indispensable as it defines the requirements around the management  
 1166 of the Security Functions. Without a secure management no TOE can be secure. Also  
 1167 **OE.TrustedAdmins** contributes to this aspect as it provides the requirements on the  
 1168 availability of a trustworthy Gateway Administrator and Service Technician. **O.Protect** is  
 1169 present to ensure that all security functions are working as specified.

1170 Those general objectives will not be addressed in detail in the following paragraphs.

1171 4.3.2.2 T.DataModificationLocal

1172 The threat **T.DataModificationLocal** is countered by a combination of the security ob-  
1173 jectives **O.Meter**, **O.Crypt**, **O.Log** and **OE.PhysicalProtection**.

1174 **O.Meter** defines that the TOE will enforce the encryption of communication when receiv-  
1175 ing Meter Data from the Meter. **O.Crypt** defines the required cryptographic functionality.  
1176 The objectives together ensure that the communication between the Meter and the TOE  
1177 cannot be modified or released.

1178 **OE.PhysicalProtection** is of relevance as it ensures that access to the TOE is limited.

1179 4.3.2.3 T.DataModificationWAN

1180 The threat **T.DataModificationWAN** is countered by a combination of the security ob-  
1181 jectives **O.Firewall** and **O.Crypt**.

1182 **O.Firewall** defines the connections for the devices within the LAN to external entities  
1183 within the WAN and shall provide firewall functionality in order to protect the devices of  
1184 the LMN and HAN (as long as they use the Gateway) and itself against threats from the  
1185 WAN side. **O.Crypt** defines the required cryptographic functionality. Both objectives to-  
1186 gether ensure that the data transmitted between the TOE and the WAN cannot be mod-  
1187 ified by a WAN attacker.

1188 4.3.2.4 T.TimeModification

1189 The threat **T.TimeModification** is countered by a combination of the security objectives  
1190 **O.Time**, **O.Crypt** and **OE.PhysicalProtection**.

1191 **O.Time** defines that the TOE needs a reliable time stamp mechanism that is also up-  
1192 dated from reliable sources regularly in the WAN. **O.Crypt** defines the required crypto-  
1193 graphic functionality for the communication to external entities in the WAN. Therewith,  
1194 O.Time and O.Crypt are the core objective to counter the threat T.TimeModification.

1195 **OE.PhysicalProtection** is of relevance as it ensures that access to the TOE is limited.

1196 4.3.2.5 T.DisclosureWAN

1197 The threat **T.DisclosureWAN** is countered by a combination of the security objectives  
1198 **O.Firewall**, **O.Conceal** and **O.Crypt**.

1199 **O.Firewall** defines the connections for the devices within the LAN to external entities  
1200 within the WAN and shall provide firewall functionality in order to protect the devices of  
1201 the LMN and HAN (as long as they use the Gateway) and itself against threats from the  
1202 WAN side. **O.Crypt** defines the required cryptographic functionality. Both objectives

1203 together ensure that the communication between the Meter and the TOE cannot be dis-  
1204 closed.

1205 **O.Conceal** ensures that no information can be disclosed based on additional character-  
1206 istics of the communication like frequency, load or the absence of a communication.

1207 4.3.2.6 T.DisclosureLocal

1208 The threat **T.DisclosureLocal** is countered by a combination of the security objectives  
1209 **O.Meter**, **O.Crypt** and **OE.PhysicalProtection**.

1210 **O.Meter** defines that the TOE will enforce the encryption and integrity protection of com-  
1211 munication when polling or receiving Meter Data from the Meter. **O.Crypt** defines the  
1212 required cryptographic functionality. Both objectives together ensure that the communi-  
1213 cation between the Meter and the TOE cannot be disclosed.

1214 **OE.PhysicalProtection** is of relevance as it ensures that access to the TOE is limited.

1215 4.3.2.7 T.Infrastructure

1216 The threat **T.Infrastructure** is countered by a combination of the security objectives  
1217 **O.Firewall**, **O.SeparateIF**, **O.Meter** and **O.Crypt**.

1218 **O.Firewall** is the core objective that counters this threat. It ensures that all communica-  
1219 tion flows to the WAN are initiated by the TOE. The fact that the TOE does not offer any  
1220 services to the WAN side and will not react to any requests (except the wake-up call)  
1221 from the WAN is a significant aspect in countering this threat. Further the TOE will only  
1222 communicate using encrypted channels to authenticated and trustworthy parties which  
1223 mitigates the possibility that an attacker could try to hijack a communication.

1224 **O.Meter** defines that the TOE will enforce the encryption and integrity protection for the  
1225 communication with the Meter.

1226 **O.SeparateIF** facilitates the disjunction of the WAN from the LMN.

1227 **O.Crypt** supports the mitigation of this threat by providing the required cryptographic  
1228 primitives.

1229 4.3.2.8 T.ResidualData

1230 The threat **T.ResidualData** is mitigated by the security objective **O.Protect** as this se-  
1231 curity objective defines that the TOE shall delete information as soon as it is no longer  
1232 used. Assuming that a TOE follows this requirement, an attacker cannot read out any  
1233 residual information as it does simply not exist.

1234 4.3.2.9 T.ResidentData

1235 The threat **T.ResidentData** is countered by a combination of the security objectives  
1236 **O.Access**, **O.Firewall**, **O.Protect** and **O.Crypt**. Further, the environment (**OE.Physi-**  
1237 **calProtection** and **OE.TrustedAdmins**) contributes to this.

1238 **O.Access** defines that the TOE shall control the access of users to information via the  
1239 external interfaces.

1240 The aspect of a local attacker with physical access to the TOE is covered by a combi-  
1241 nation of **O.Protect** (defining the detection of physical manipulation) and **O.Crypt** (re-  
1242 quiring the encryption of persistently stored TSF and user data of the TOE). In addition,  
1243 the physical protection provided by the environment (**OE.PhysicalProtection**) and the  
1244 Gateway Administrator (**OE.TrustedAdmins**) who could realise a physical manipulation  
1245 contribute to counter this threat.

1246 The aspect of a WAN attacker is covered by **O.Firewall** as this objective ensures that  
1247 an adequate level of protection is realised against attacks from the WAN side.

1248 4.3.2.10 T.Privacy

1249 The threat **T.Privacy** is primarily addressed by the security objectives **O.Meter**, **O.Crypt**  
1250 and **O.Firewall** as these objective ensures that the TOE will only distribute Meter Data  
1251 to external parties in the WAN as defined in the corresponding Processing Profiles and  
1252 that the data will be protected for the transfer. **OE.Profile** is present to ensure that the  
1253 Processing Profiles are obtained from a trustworthy and reliable source only.

1254 Finally, **O.Conceal** ensures that an attacker cannot obtain the relevant information for  
1255 this threat by observing external characteristics of the information flow.

1256 **4.3.3 Coverage of organisational security policies**

1257 The following sections provide more detailed information about how the security objec-  
1258 tives for the environment and the TOE cover the organizational security policies.

1259 4.3.3.1 OSP.SM

1260 The Organizational Security Policy **OSP.SM** that mandates that the TOE utilises the ser-  
1261 vices of a certified Security Module is directly addressed by the security objectives  
1262 **OE.SM** and **O.Crypt**. The objective **OE.SM** addresses the functions that the Security  
1263 Module shall be utilised for as defined in **OSP.SM** and also requires a certified Security  
1264 Module. **O.Crypt** defines the cryptographic functionalities for the TOE itself. In this

1265 context, it has to be ensured that the Security Module is operated in accordance with its  
1266 guidance documentation.

#### 1267 4.3.3.2 OSP.Log

1268 The Organizational Security Policy **OSP.Log** that mandates that the TOE maintains an  
1269 audit log is directly addressed by the security objective for the TOE **O.Log**.

1270 **O.Access** contributes to the implementation of the OSP as it defines that also Gateway  
1271 Administrators are not allowed to read/modify all data. This is of specific importance to  
1272 ensure the confidentiality and integrity of the log data as is required by the **OSP.Log**.

#### 1273 4.3.4 Coverage of assumptions

1274 The following sections provide more detailed information about how the security objec-  
1275 tives for the environment cover the assumptions.

##### 1276 4.3.4.1 A.ExternalPrivacy

1277 The assumption **A.ExternalPrivacy** is directly and completely covered by the security  
1278 objective **OE.ExternalPrivacy**. The assumption and the objective for the environment  
1279 are drafted in a way that the correspondence is obvious.

##### 1280 4.3.4.2 A.TrustedAdmins

1281 The assumption **A.TrustedAdmins** is directly and completely covered by the security  
1282 objective **OE.TrustedAdmins**. The assumption and the objective for the environment  
1283 are drafted in a way that the correspondence is obvious.

##### 1284 4.3.4.3 A.PhysicalProtection

1285 The assumption **A.PhysicalProtection** is directly and completely covered by the secu-  
1286 rity objective **OE.PhysicalProtection**. The assumption and the objective for the envi-  
1287 ronment are drafted in a way that the correspondence is obvious.

##### 1288 4.3.4.4 A.ProcessProfile

1289 The assumption **A.ProcessProfile** is directly and completely covered by the security  
1290 objective **OE.Profile**. The assumption and the objective for the environment are drafted  
1291 in a way that the correspondence is obvious.

##### 1292 4.3.4.5 A.Update

1293 The assumption **A.Update** is directly and completely covered by the security objective  
1294 **OE.Update**. The assumption and the objective for the environment are drafted in a way  
1295 that the correspondence is obvious.

1296 4.3.4.6 A.Network

1297 The assumption **A.Network** is directly and completely covered by the security objective  
1298 **OE.Network**. The assumption and the objective for the environment are drafted in a way  
1299 that the correspondence is obvious.

1300 4.3.4.7 A.Keygen

1301 The assumption **A.Keygen** is directly and completely covered by the security objective  
1302 **OE.Keygen**. The assumption and the objective for the environment are drafted in a way  
1303 that the correspondence is obvious.

1304

1305 **5 Extended Component definition**

1306 **5.1 Communication concealing (FPR\_CON)**

1307 The additional family Communication concealing (FPR\_CON) of the Class FPR (Pri-  
1308 vacy) is defined here to describe the specific IT security functional requirements of the  
1309 TOE. The TOE shall prevent attacks against Personally Identifiable Information (PII) of  
1310 the Consumer that may be obtained by an attacker by observing the encrypted commu-  
1311 nication of the TOE with remote entities.

1312

1313 **5.2 Family behaviour**

1314 This family defines requirements to mitigate attacks against communication channels in  
1315 which an attacker tries to obtain privacy relevant information based on characteristics of  
1316 an encrypted communication channel. Examples include but are not limited to an analy-  
1317 sis of the frequency of communication or the transmitted workload.

1318

1319 **5.3 Component levelling**

1320 FPR\_CON: Communication concealing -----1

1321

1322 **5.4 Management**

1323 The following actions could be considered for the management functions in FMT:

- 1324 a. Definition of the interval in FPR\_CON.1.2 if definable within the operational  
1325 phase of the TOE.

1326

1327 **5.5 Audit**

1328 There are no auditable events foreseen.

1329

1330 **5.6 Communication concealing (FPR\_CON.1)**

1331 Hierarchical to: No other components.

1332 Dependencies: No dependencies.

1333 FPR\_CON.1.1 The TSF shall enforce the [assignment: *information*  
1334 *flow policy*] in order to ensure that no personally iden-  
1335 tifiable information (PII) can be obtained by an analysis  
1336 of [assignment: *characteristics of the information flow*  
1337 *that need to be concealed*].

1338 FPR\_CON.1.2 The TSF shall connect to [assignment: *list of external*  
1339 *entities*] in intervals as follows [selection: *weekly,*  
1340 *daily, hourly, [assignment: other interval]*] to conceal  
1341 the data flow.



## 1342 6 Security Requirements

### 1343 6.1 Overview

1344 This chapter describes the security functional and the assurance requirements which  
 1345 have to be fulfilled by the TOE. Those requirements comprise functional components  
 1346 from part 2 of [CC] and the assurance components as defined for the Evaluation Assur-  
 1347 ance Level 4 from part 3 of [CC].

1348 The following notations are used:

- 1349 • **Refinement** operation (denoted by **bold text**): is used to add details to a re-  
 1350 quirement, and thus further restricts a requirement. In case that a word has  
 1351 been deleted from the original text this refinement is indicated by crossed out  
 1352 ~~bold text~~.
- 1353 • **Selection** operation (denoted by underlined text): is used to select one or more  
 1354 options provided by the [CC] in stating a requirement.
- 1355 • **Assignment** operation (denoted by *italicised text*): is used to assign a specific  
 1356 value to an unspecified parameter, such as the length of a password.
- 1357 • **Iteration** operation: are identified with a suffix in the name of the SFR (e.g.  
 1358 FDP\_IFC.2/FW).

1359 It should be noted that the requirements in the following chapters are not necessarily be  
 1360 ordered alphabetically. Where useful the requirements have been grouped.

1361 The following table summarises all TOE security functional requirements of this ST:

Class FAU: Security Audit	
FAU_ARP.1/SYS	Security alarms for system log
FAU_GEN.1/SYS	Audit data generation for system log
FAU_SAA.1/SYS	Potential violation analysis for system log
FAU_SAR.1/SYS	Audit review for system log
FAU_STG.4/SYS	Prevention of audit data loss for the system log
FAU_GEN.1/CON	Audit data generation for consumer log

FAU_SAR.1/CON	Audit review for consumer log
FAU_STG.4/CON	Prevention of audit data loss for the consumer log
FAU_GEN.1/CAL	Audit data generation for calibration log
FAU_SAR.1/CAL	Audit review for calibration log
FAU_STG.4/CAL	Prevention of audit data loss for the calibration log
FAU_GEN.2	User identity association
FAU_STG.2	Guarantees of audit data availability
<b>Class FCO: Communication</b>	
FCO_NRO.2	Enforced proof of origin
<b>Class FCS: Cryptographic Support</b>	
FCS_CKM.1/TLS	Cryptographic key generation for TLS
FCS_COP.1/TLS	Cryptographic operation for TLS
FCS_CKM.1/CMS	Cryptographic key generation for CMS
FCS_COP.1/CMS	Cryptographic operation for CMS
FCS_CKM.1/MTR	Cryptographic key generation for Meter communication encryption
FCS_COP.1/MTR	Cryptographic operation for Meter communication encryption
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/HASH	Cryptographic operation for Signatures
FCS_COP.1/MEM	Cryptographic operation for TSF and user data encryption

<b>Class FDP: User Data Protection</b>	
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2/FW	Complete information flow control for firewall
FDP_IFF.1/FW	Simple security attributes for Firewall
FDP_IFC.2/MTR	Complete information flow control for Meter information flow
FDP_IFF.1/MTR	Simple security attributes for Meter information
FDP_RIP.2	Full residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
<b>Class FIA: Identification and Authentication</b>	
FIA_ATD.1	User attribute definition
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-Authenticating
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
<b>Class FMT: Security Management</b>	
FMT_MOF.1	Management of security functions behaviour
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

FMT_MSA.1/AC	Management of security attributes for Gateway access policy
FMT_MSA.3/AC	Static attribute initialisation for Gateway access policy
FMT_MSA.1/FW	Management of security attributes for Firewall policy
FMT_MSA.3/FW	Static attribute initialisation for Firewall policy
FMT_MSA.1/MTR	Management of security attributes for Meter policy
FMT_MSA.3/MTR	Static attribute initialisation for Meter policy
<b>Class FPR: Privacy</b>	
FPR_CON.1	Communication Concealing
FPR_PSE.1	Pseudonymity
<b>Class FPT: Protection of the TSF</b>	
FPT_FLS.1	Failure with preservation of secure state
FPT_RPL.1	Replay Detection
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF testing
FPT_PHP.1	Passive detection of physical attack
<b>Class FTP: Trusted path/channels</b>	
FTP_ITC.1/WAN	Inter-TSF trusted channel for WAN
FTP_ITC.1/MTR	Inter-TSF trusted channel for Meter
FTP_ITC.1/USR	Inter-TSF trusted channel for User

**Table 9: List of Security Functional Requirements**

1363 **6.2 Class FAU: Security Audit**

1364 **6.2.1 Introduction**

1365 The TOE compliant to this Security Target shall implement three different audit logs as  
 1366 defined in **OSP.Log** and **O.Log**. The following table provides an overview over the three  
 1367 audit logs before the following chapters introduce the SFRs related to those audit logs.

	<b>System-Log</b>	<b>Consumer-Log</b>	<b>Calibration-Log</b>
<b>Purpose</b>	<ul style="list-style-type: none"> <li>• Inform the Gateway Administrator about security relevant events</li> <li>• Log all events as defined by Common Criteria [CC] for the used SFR</li> <li>• Log all system relevant events on specific functionality</li> <li>• Automated alarms in case of a cumulation of certain events</li> <li>• Inform the Service Technician about the status of the Gateway</li> </ul>	<ul style="list-style-type: none"> <li>• Inform the Consumer about all information flows to the WAN</li> <li>• Inform the Consumer about the Processing Profiles</li> <li>• Inform the Consumer about other metering data (not billing-relevant)</li> <li>• Inform the Consumer about all billing-relevant data needed to verify an invoice</li> </ul>	<ul style="list-style-type: none"> <li>• Track changes that are relevant for the calibration of the TOE relevant data needed to verify an invoice</li> </ul>
<b>Data</b>	<ul style="list-style-type: none"> <li>• As defined by CC part 2</li> <li>• Augmented by specific events for the security functions</li> </ul>	<ul style="list-style-type: none"> <li>• Information about all information flows to the WAN</li> <li>• Information about the current and the previous Processing Profiles</li> <li>• Non-billing-relevant Meter Data</li> <li>• Information about the system status (including relevant errors)</li> </ul>	<ul style="list-style-type: none"> <li>• Calibration relevant data only</li> </ul>

		<ul style="list-style-type: none"> <li>Billing-relevant data needed to verify an invoice</li> </ul>	
<b>Access</b>	<ul style="list-style-type: none"> <li>Access by authorised Gateway Administrator and via IF_GW_WAN only</li> <li>Events may only be deleted by an authorised Gateway Administrator via IF_GW_WAN</li> <li>Read access by authorised Service Technician via IF_GW_SRV only</li> </ul>	<ul style="list-style-type: none"> <li>Read access by authorised Consumer and via IF_GW_CON only to the data related to the current consumer</li> </ul>	<ul style="list-style-type: none"> <li>Read access by authorised Gateway Administrator and via IF_GW_WAN only</li> </ul>
<b>Deletion</b>	<ul style="list-style-type: none"> <li>Ring buffer.</li> <li>The availability of data has to be ensured for a sufficient amount of time</li> <li>Overwriting old events is possible if the memory is full.</li> </ul>	<ul style="list-style-type: none"> <li>Ring buffer.</li> <li>The availability of data has to be ensured for a sufficient amount of time.</li> <li>Overwriting old events is possible if the memory is full</li> <li>Retention period is set by authorised Gateway Administrator on request by consumer, data older than this are deleted.</li> </ul>	<ul style="list-style-type: none"> <li>The availability of data has to be ensured over the lifetime of the TOE.</li> </ul>

1368

**Table 10: Overview over audit processes**

1369	<b>6.2.2 Security Requirements for the System Log</b>	
1370	6.2.2.1 Security audit automatic response (FAU_ARP)	
1371	<b>6.2.2.1.1 FAU_ARP.1/SYS: Security Alarms for system log</b>	
1372	FAU_ARP.1.1/SYS	The TSF shall <del>take</del> <i>inform an authorised Gateway Administrator and create a log entry in the system log</i> <sup>33</sup>
1373		upon detection of a potential security violation.
1374		
1375	Hierarchical to:	No other components
1376	Dependencies:	FAU_SAA.1 Potential violation analysis
1377		
1378	6.2.2.2 Security audit data generation (FAU_GEN)	
1379	<b>6.2.2.2.1 FAU_GEN.1/SYS: Audit data generation for system log</b>	
1380	FAU_GEN.1.1/SYS	The TSF shall be able to generate an audit record of the
1381		following auditable events:
1382		a) Start-up and shutdown of the audit functions;
1383		b) All auditable events for the <u>basic</u> <sup>34</sup> level of audit; and
1384		c) <i>other non privacy relevant auditable events: none</i> <sup>35</sup> .
1385	FAU_GEN.1.2/SYS	The TSF shall record within each audit record at least the
1386		following information:
1387		a) Date and time of the event, type of event, subject identity
1388		(if applicable), and the outcome (success or failure) of the
1389		event; and
1390		b) For each audit event type, based on the auditable event
1391		definitions of the functional components included in the
1392		<b>PP/ST</b> <sup>36</sup> , <i>other audit relevant information: none</i> <sup>37</sup> .

---

33 [assignment: *list of actions*]

34 [selection, choose one of: *minimum, basic, detailed, not specified*]

35 [assignment: *other specifically defined auditable events*]

36 [refinement: *PP/ST*]

37 [assignment: *other audit relevant information*]

1393	Hierarchical to:	No other components
1394	Dependencies:	FPT_STM.1
1395	6.2.2.3 Security audit analysis (FAU_SAA)	
1396	<b>6.2.2.3.1 FAU_SAA.1/SYS: Potential violation analysis for system</b>	
1397	<b>log</b>	
1398	FAU_SAA.1.1./SYS	The TSF shall be able to apply a set of rules in monitoring
1399		the audited events and based upon these rules indicate a
1400		potential violation of the enforcement of the SFRs.
1401	FAU_SAA.1.2/SYS	The TSF shall enforce the following rules for monitoring
1402		audited events:
1403		a) Accumulation or combination of
1404		<ul style="list-style-type: none"> <li>• <i>Start-up and shutdown of the audit functions</i></li> </ul>
1405		<ul style="list-style-type: none"> <li>• <i>all auditable events for the basic level of audit</i></li> </ul>
1406		<ul style="list-style-type: none"> <li>• <i>all types of failures in the TSF as listed in</i></li> </ul>
1407		<i>FPT_FLS.1</i> <sup>38</sup>
1408		known to indicate a potential security violation.
1409		b) <i>any other rules: none</i> <sup>39</sup> .
1410	Hierarchical to:	No other components
1411	Dependencies:	FAU_GEN.1
1412	6.2.2.4 Security audit review (FAU_SAR)	
1413	<b>6.2.2.4.1 FAU_SAR.1/SYS: Audit Review for system log</b>	
1414	FAU_SAR.1.1/SYS	The TSF shall provide <i>only authorised Gateway</i>
1415		<i>Administrators via the IF_GW_WAN interface and</i>
1416		<i>authorised Service Technicians via the IF_GW_SRV</i>

---

<sup>38</sup> [assignment: *subset of defined auditable events*]

<sup>39</sup> [assignment: *any other rules*]



1417		<i>interface</i> <sup>40</sup> with the capability to read all information <sup>41</sup>
1418		from the <b>system</b> audit records <sup>42</sup> .
1419	FAU_SAR.1.2/SYS	The TSF shall provide the audit records in a manner
1420		suitable for the user to interpret the information.
1421	Hierarchical to:	No other components
1422	Dependencies:	FAU_GEN.1
1423	6.2.2.5 Security audit event storage (FAU_STG)	
1424	<b>6.2.2.5.1 FAU_STG.4/SYS: Prevention of audit data loss for</b>	
1425	<b>systemlog</b>	
1426	FAU_STG.4.1/SYS	The TSF shall <u>overwrite the oldest stored audit records</u> <sup>43</sup>
1427		and other actions to be taken in case of audit storage
1428		failure: none <sup>44</sup> if the <b>system</b> audit trail <sup>45</sup> is full.
1429	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1430	Dependencies:	FAU_STG.1 Protected audit trail storage
1431	<b>Application Note 4:</b>	The size of the audit trail that is available before the oldest
1432		events get overwritten is configurable for the Gateway
1433		Administrator.

---

40 [assignment: *authorised users*]

41 [assignment: *list of audit information*]

42 [refinement: *audit records*]

43 [selection, choose one of: "*ignore audited events*", "*prevent audited events, except those taken by the authorised user with special rights*", "*overwrite the oldest stored audit records*"]

44 [assignment: *other actions to be taken in case of audit storage failure*]

45 [refinement: *audit trail*]

1434	<b>6.2.3 Security Requirements for the Consumer Log</b>	
1435	6.2.3.1 Security audit data generation (FAU_GEN)	
1436	<b>6.2.3.1.1 FAU_GEN.1/CON: Audit data generation for consumer log</b>	
1437	FAU_GEN.1.1/CON	The TSF shall be able to generate an audit record of the
1438		following auditable events:
1439		a) Start-up and shutdown of the audit functions;
1440		b) All auditable events for the <u>not specified</u> <sup>46</sup> level of audit;
1441		and
1442		c) <i>all audit events as listed in Table 11 and additional</i>
1443		<i>events: none</i> <sup>47</sup> .
1444	FAU_GEN.1.2/CON	The TSF shall record within each audit record at least the
1445		following information:
1446		a) Date and time of the event, type of event, subject identity
1447		(if applicable), and the outcome (success or failure) of the
1448		event; and
1449		b) For each audit event type, based on the auditable event
1450		definitions of the functional components included in the
1451		<b>PP/ST</b> <sup>48</sup> , <i>additional information as listed in Table 11 and</i>
1452		<i>additional events: none</i> <sup>49</sup> .
1453	Hierarchical to:	No other components
1454	Dependencies:	FPT_STM.1
1455		

---

<sup>46</sup> [selection, choose one of: *minimum, basic, detailed, not specified*]

<sup>47</sup> [assignment: *other specifically defined auditable events*]

<sup>48</sup> [refinement: *PP/ST*]

<sup>49</sup> [assignment: *other audit relevant information*]

Event	Additional Information
Any change to a Processing Profile	The new and the old Processing Profile
Any submission of Meter Data to an external entity	The Processing Profile that lead to the submission  The submitted values
Any submission of Meter Data that is not billing-relevant	-
Billing-relevant data	-
Any administrative action performed	-
Relevant system status information including relevant errors	-

1456 **Table 11: Events for consumer log**

1457

1458 6.2.3.2 Security audit review (FAU\_SAR)

1459 **6.2.3.2.1 FAU\_SAR.1/CON: Audit Review for consumer log**

1460 FAU\_SAR.1.1/CON The TSF shall provide *only authorised Consumer via the*  
 1461 *IF\_GW\_CON interface*<sup>50</sup> with the capability to read *all*

---

50 [assignment: *authorised users*]

1462		<i>information that are related to them</i> <sup>51</sup> from the <b>consumer</b>
1463		audit records <sup>52</sup> .
1464	FAU_SAR.1.2/CON	The TSF shall provide the audit records in a manner
1465		suitable for the user to interpret the information.
1466	Hierarchical to:	No other components
1467	Dependencies:	FAU_GEN.1
1468	<b>Application Note 5:</b>	FAU_SAR.1.2/CON shall ensure that the Consumer is
1469		able to interpret the information that is provided to him in a
1470		way that allows him to verify the invoice.
1471	6.2.3.3 Security audit event storage (FAU_STG)	
1472	<b>6.2.3.3.1 FAU_STG.4/CON: Prevention of audit data loss for the</b>	
1473	<b>consumer log</b>	
1474	FAU_STG.4.1/CON	The TSF shall <u>overwrite the oldest stored audit records</u> and
1475		<i>interrupt metrological operation in case that the oldest</i>
1476		<i>audit record must still be kept for billing verification</i> <sup>53</sup> if the
1477		<b>consumer</b> audit trail is full.
1478	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1479	Dependencies:	FAU_STG.1 Protected audit trail storage
1480	<b>Application Note 6:</b>	The size of the audit trail that is available before the oldest
1481		events get overwritten is configurable for the Gateway
1482		Administrator.

---

51 [assignment: *list of audit information*]

52 [refinement: *audit records*]

53 [assignment: *other actions to be taken in case of audit storage failure*]

1483	<b>6.2.4 Security Requirements for the Calibration Log</b>	
1484	6.2.4.1 Security audit data generation (FAU_GEN)	
1485	<b>6.2.4.1.1 FAU_GEN.1/CAL: Audit data generation for calibration log</b>	
1486	FAU_GEN.1.1/CAL	The TSF shall be able to generate an audit record of the
1487		following auditable events:
1488		a) Start-up and shutdown of the audit functions;
1489		b) All auditable events for the <u>not specified</u> <sup>54</sup> level of audit;
1490		and
1491		c) <i>all calibration-relevant information according to Table</i>
1492		<i>12</i> <sup>55</sup> .
1493	FAU_GEN.1.2/CAL	The TSF shall record within each audit record at least the
1494		following information:
1495		a) Date and time of the event, type of event, subject identity
1496		(if applicable), and the outcome (success or failure) of the
1497		event; and
1498		b) For each audit event type, based on the auditable event
1499		definitions of the functional components included in the
1500		<b>PP/ST</b> <sup>56</sup> , <i>other audit relevant information: none</i> <sup>57</sup> .
1501	Hierarchical to:	No other components
1502	Dependencies:	FPT_STM.1
1503	<b>Application Note 7:</b>	The calibration log serves to fulfil national requirements in
1504		the context of the calibration of the TOE.
1505		

---

54 [selection, choose one of: *minimum, basic, detailed, not specified*]

55 [assignment: *other specifically defined auditable events*]

56 [refinement: *PP/ST*]

57 [assignment: *other audit relevant information*]

Event / Parameter	Content
Commissioning	Commissioning of the SMGW MUST be logged in calibration log.
Event of self-test	Initiation of self-test MUST be logged in calibration log.
New meter	Connection and registration of a new meter MUST be logged in calibration log.
Meter removal	Removal of a meter from SMGW MUST be logged in calibration log.
Change of tarification profiles	<p>Every change (incl. parameter change) of a tarification profile according to [TR-03109-1, 4.4], provided the parameter is relevant for calibration regulations (see below) as well as new storage or removal of tarification profiles MUST be logged in calibration log.</p> <p>Parameter relevant for calibration regulations are:</p> <ul style="list-style-type: none"> <li>• Device-ID of a meter - Unique identifier of the meter, which send the input values for a TAF</li> <li>• OBIS value of the measured variable of the meter - Unique value for the measured variable of the meter for the used TAF</li> <li>• Metering point name - Unique name of the metering point</li> <li>• Billing period - Period in which a billing should be done</li> <li>• Consumer ID</li> <li>• Validity period - Period for which the TAF is booked</li> <li>• Definition of tariff stages - Defines different tariff stages and associated OBIS values. Here it will be defined which tariff stage is valid at the time of rule set activation</li> <li>• Tariff switching time - Defines to the split second the switching of tariff stages. The time points can be defined as periodic values</li> <li>• Register period - Time distance of two consecutive measured value acquisitions for meter readings</li> </ul>

Change of meter profiles	<p>Every change (incl. parameter change) of a meter profile according to [TR-03109-1, 4.4], provided the parameter is relevant for calibration regulations (see below) as well as new storage or removal of meter profiles MUST be logged in calibration log.</p> <p>Parameter relevant for legal metrology are:</p> <ul style="list-style-type: none"> <li>• Device-ID - Unique identifier of the meter according to <b>DIN 43863-5</b></li> <li>• Key material - Public key for inner signature (dependent on the used meter in LMN)</li> <li>• Register period - Interval during receipt of meter values</li> <li>• Displaying interval ('Anzeigeintervall') - Interval during which the actual meter value (only during display) must be updated in case of bidirectional communication between meter and SMGW</li> <li>• Balancing ('Saldierend') - Determines if the meter is balancing ('saldierend') and meter values can grow and fall</li> <li>• OBIS values - OBIS values according to <b>IEC-62056-6-1</b> resp. EN 13757-1</li> <li>• Converter factor ('Wandlerfaktor') - Value is 1 in case of directly connected meter. In usage of converter counter ('Wandlerzähler') the value may be different.</li> </ul>
Software update	Every update of the code which touches calibration regulations (serialized COSEM-objects, rules) MUST be logged in calibration log.
Firmware update	Every firmware update (incl. operating system update if applicable) MUST be logged in calibration log.
Error messages of a meter	<p>All FATAL messages of a connected meter MUST be logged in calibration log according to</p> <p>0 - no error</p> <p>1 - Warning, no action to be done according to calibration authority, meter value valid</p>

	<p>2 - Temporal error, send meter value will be marked as invalid, the value in meter field ('Messwertfeld') could be used according to the rules of [VDE4400] resp. [G865] as replacement value ('Ersatzwert') in backend.</p> <p>3 - Temporal error, send meter value is invalid; the value in the meter field ('Messwertfeld') cannot be used as replacement value in backend.</p> <p>4 - Fatal error (meter defect), actual send value is invalid and all future values will be invalid. including the device-ID.</p>
<p>Error messages of a SMGW</p>	<p>All self-test and calibration regulations relevant errors MUST be logged in calibration log.</p>

1506

**Table 12: Content of calibration log**

1507



1508	6.2.4.2 Security audit review (FAU_SAR)	
1509	<b>6.2.4.2.1 FAU_SAR.1/CAL: Audit Review for the calibration log</b>	
1510	FAU_SAR.1.1/CAL	The TSF shall provide <i>only authorised Gateway Administrators via the IF_GW_WAN interface</i> <sup>58</sup> with the capability to read <i>all information</i> <sup>59</sup> from the <b>calibration</b> audit records <sup>60</sup> .
1511		
1512		
1513		
1514	FAU_SAR.1.2/CAL	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
1515		
1516	Hierarchical to:	No other components
1517	Dependencies:	FAU_GEN.1
1518	6.2.4.3 Security audit event storage (FAU_STG)	
1519	<b>6.2.4.3.1 FAU_STG.4/CAL: Prevention of audit data loss for calibration log</b>	
1520		
1521	FAU_STG.4.1/CAL	The TSF shall <u>ignore audited events</u> <sup>61</sup> and <i>stop the operation of the TOE and inform a Gateway Administrator</i> <sup>62</sup> if the <b>calibration</b> audit trail <sup>63</sup> is full.
1522		
1523		
1524	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1525	Dependencies:	FAU_STG.1 Protected audit trail storage
1526	<b>Application Note 8:</b>	As outlined in the introduction it has to be ensured that the events of the calibration log are available over the lifetime of the TOE.
1527		
1528		

---

58 [assignment: *authorised users*]

59 [assignment: *list of audit information*]

60 [refinement: *audit records*]

61 [selection, choose one of: "*ignore audited events*", "*prevent audited events, except those taken by the authorised user with special rights*", "*overwrite the oldest stored audit records*"]

62 [assignment: *other actions to be taken in case of audit storage failure*]

63 [refinement: *audit trail*]

1529	<b>6.2.5 Security Requirements that apply to all logs</b>	
1530	6.2.5.1 Security audit data generation (FAU_GEN)	
1531	<b>6.2.5.1.1 FAU_GEN.2: User identity association</b>	
1532	FAU_GEN.2.1	For audit events resulting from actions of identified users,
1533		the TSF shall be able to associate each auditable event
1534		with the identity of the user that caused the event.
1535	Hierarchical to:	No other components
1536	Dependencies:	FAU_GEN.1
1537		FIA_UID.1
1538	<b>Application Note 9:</b>	Please note that FAU_GEN.2 applies to all audit logs, the
1539		system log, the calibration log, and the consumer log.

1540	6.2.5.2 Security audit event storage (FAU_STG)	
1541	<b>6.2.5.2.1 FAU_STG.2: Guarantees of audit data availability</b>	
1542	FAU_STG.2.1	The TSF shall protect the stored audit records in <b>the all</b>
1543		audit trails <sup>64</sup> from unauthorised deletion.
1544	FAU_STG.2.2	The TSF shall be able to <u>prevent</u> <sup>65</sup> unauthorised
1545		modifications to the stored audit records in <b>the all</b> audit
1546		trails <sup>66</sup> .
1547	FAU_STG.2.3	The TSF shall ensure that <i>all</i> <sup>67</sup> stored audit records will be
1548		maintained when the following conditions occur: <u>audit</u>
1549		<u>storage exhaustion or failure</u> <sup>68</sup> .
1550	Hierarchical to:	FAU_STG.1 Protected audit trail storage
1551	Dependencies:	FAU_GEN.1
1552	<b>Application Note 10:</b>	Please note that FAU_STG.2 applies to all audit logs, the
1553		system log, the calibration log, and the consumer log.

---

64 [refinement: *audit trail*]

65 [selection, choose one of: *prevent, detect*]

66 [refinement: *audit trail*]

67 [assignment: *metric for saving audit records*]

68 [selection: *audit storage exhaustion, failure, attack*]

1554	<b>6.3 Class FCO: Communication</b>	
1555	<b>6.3.1 Non-repudiation of origin (FCO_NRO)</b>	
1556	6.3.1.1 FCO_NRO.2: Enforced proof of origin	
1557	FCO_NRO.2.1	The TSF shall enforce the generation of evidence of origin
1558		for transmitted <i>Meter Data</i> <sup>69</sup> at all times.
1559	FCO_NRO.2.2	The TSF shall be able to relate the <i>key material used for</i>
1560		<i>signature</i> <sup>70, 71</sup> of the originator of the information, and the
1561		<i>signature</i> <sup>72</sup> of the information to which the evidence
1562		applies.
1563	FCO_NRO.2.3	The TSF shall provide a capability to verify the evidence of
1564		origin of information to <u>recipient, Consumer</u> <sup>73</sup> given
1565		<i>limitations of the digital signature according to TR-03109-</i>
1566		<i>1</i> <sup>74</sup> .
1567	Hierarchical to:	FCO_NRO.1 Selective proof of origin
1568	Dependencies:	FIA_UID.1 Timing of identification
1569	<b>Application Note 11:</b>	FCO_NRO.2 requires that the TOE calculates a signature
1570		over Meter Data that is submitted to external entities.
1571		Therefore, the TOE has to create a hash value over the
1572		Data To Be Signed (DTBS) as defined in
1573		FCS_COP.1/HASH. The creation of the actual signature
1574		however is performed by the Security Module.

---

69 [assignment: *list of information types*]

70 [assignment: *list of attributes*]

71 The key material here also represents the identity of the Gateway.

72 [assignment: *list of information fields*]

73 [selection: *originator, recipient, [assignment: list of third parties]*]

74 [assignment: *limitations on the evidence of origin*]

## 1575 6.4 Class FCS: Cryptographic Support

### 1576 6.4.1 Cryptographic support for TLS

#### 1577 6.4.1.1 Cryptographic key management (FCS\_CKM)

##### 1578 6.4.1.1.1 **FCS\_CKM.1/TLS: Cryptographic key generation for TLS**

1579 FCS\_CKM.1.1/TLS The TSF shall generate cryptographic keys in accordance  
 1580 with a specified cryptographic key generation algorithm  
 1581 *TLS-PRF with SHA-256 or SHA-384*<sup>75</sup> and specified  
 1582 cryptographic key sizes *128 bit, 256 bit or 384 bit*<sup>76</sup> that  
 1583 meet the following: *[RFC 5246] in combination with*  
 1584 *[FIPS Pub. 180-4] and [RFC 2104]*<sup>77</sup>.

1585 Hierarchical to: No other components.

1586 Dependencies: [FCS\_CKM.2 Cryptographic key distribution, or  
 1587 FCS\_COP.1 Cryptographic operation], fulfilled by  
 1588 FCS\_COP.1/TLS  
 1589 FCS\_CKM.4 Cryptographic key destruction

1590 **Application Note 12:** The Security Module is used for the generation of random  
 1591 numbers and for all cryptographic operations with the pri-  
 1592 vate key of a TLS certificate.

1593 **Application Note 13:** The TOE uses only cryptographic specifications and  
 1594 algorithms as described in [TR-03109-3].

#### 1595 6.4.1.2 Cryptographic operation (FCS\_COP)

##### 1596 6.4.1.2.1 **FCS\_COP.1/TLS: Cryptographic operation for TLS**

1597 FCS\_COP.1.1/TLS The TSF shall perform *TLS encryption, decryption, and*  
 1598 *integrity protection*<sup>78</sup> in accordance with a specified  
 1599 cryptographic algorithm *TLS cipher suites*

---

75 [assignment: *key generation algorithm*]

76 [assignment: *cryptographic key sizes*]

77 [assignment: *list of standards*]

78 [assignment: *list of cryptographic operations*]

1600		<i>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,</i>
1601		<i>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,</i>
1602		<i>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,</i>
1603		<i>and</i>
1604		<i>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</i>
1605		<sup>79</sup> <i>using elliptic curves BrainpoolP256r1, BrainpoolP384r1,</i>
1606		<i>BrainpoolP512r1 (according to [RFC 5639]), NIST P-256,</i>
1607		<i>and NIST P-384 (according to [RFC 5114]) and</i>
1608		<i>cryptographic key sizes 128 bit or 256 bit</i> <sup>80</sup> <i>that meet the</i>
1609		<i>following: [RFC 2104], [RFC 5114], [RFC 5246],</i>
1610		<i>[RFC 5289], [RFC 5639], [NIST 800-38A], and [NIST 800-</i>
1611		<i>38D]</i> <sup>81</sup> .
1612	Hierarchical to:	No other components.
1613	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1614		or
1615		FDP_ITC.2 Import of user data with security attributes, or
1616		FCS_CKM.1 Cryptographic key generation], fulfilled by
1617		FCS_CKM.1/TLS
1618		FCS_CKM.4 Cryptographic key destruction
1619	<b>Application Note 14:</b>	The TOE uses only cryptographic specifications and
1620		algorithms as described in [TR-03109-3].
1621	<b>6.4.2 Cryptographic support for CMS</b>	
1622	6.4.2.1 Cryptographic key management (FCS_CKM)	
1623	<b>6.4.2.1.1 FCS_CKM.1/CMS: Cryptographic key generation for CMS</b>	
1624	FCS_CKM.1.1/CMS	The TSF shall generate cryptographic keys in accordance
1625		with a specified cryptographic key generation algorithm
1626		<i>ECKA-EG</i> <sup>82</sup> and specified cryptographic key sizes 128

---

79 [assignment: *cryptographic algorithm*]

80 [assignment: *cryptographic key sizes*]

81 [assignment: *list of standards*]

82 [assignment: *cryptographic key generation algorithm*]

1627		<i>bit</i> <sup>83</sup> that meet the following: [X9.63] in combination with
1628		[RFC 3565] <sup>84</sup> .
1629	Hierarchical to:	No other components.
1630	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or
1631		FCS_COP.1 Cryptographic operation], fulfilled by
1632		FCS_COP.1/CMS
1633		FCS_CKM.4 Cryptographic key destruction
1634	<b>Application Note 15:</b>	The TOE utilises the services of its Security Module for the
1635		generation of random numbers and for all cryptographic
1636		operations with the private asymmetric key of a CMS cer-
1637		tificate.
1638	<b>Application Note 16:</b>	The TOE uses only cryptographic specifications and
1639		algorithms as described in [TR-03109-3].
1640		6.4.2.2 Cryptographic operation (FCS_COP)
1641		<b>6.4.2.2.1 FCS_COP.1/CMS: Cryptographic operation for CMS</b>
1642	FCS_COP.1.1/CMS	The TSF shall perform
1643		<i>symmetric encryption, decryption and integrity protection</i>
1644		in accordance with a specified cryptographic algorithm
1645		<i>AES-CBC-CMAC or AES-GCM</i> <sup>85</sup> and cryptographic key
1646		sizes <i>128 bit</i> <sup>86</sup> that meet the following: [FIPS Pub. 197],

---

83 [assignment: *cryptographic key sizes*]

84 [assignment: *list of standards*]

85 [assignment: *list of cryptographic operations*]

86 [assignment: *cryptographic key sizes*]

1647		<i>[NIST 800-38D], [RFC 4493], [RFC 5084], and [RFC 5652]</i>
1648		<i>in combination with [NIST 800-38A]<sup>87</sup>.</i>
1649	Hierarchical to:	No other components.
1650	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1651		or
1652		FDP_ITC.2 Import of user data with security attributes, or
1653		FCS_CKM.1 Cryptographic key generation], fulfilled by
1654		FCS_CKM.1/CMS
1655		FCS_CKM.4 Cryptographic key destruction
1656	<b>Application Note 17:</b>	The TOE uses only cryptographic specifications and
1657		algorithms as described in [TR-03109-3].
1658	<b>6.4.3 Cryptographic support for Meter communication encryption</b>	
1659	6.4.3.1 Cryptographic key management (FCS_CKM)	
1660	<b>6.4.3.1.1 FCS_CKM.1/MTR: Cryptographic key generation for Meter</b>	
1661	<b>communication (symmetric encryption)</b>	
1662	FCS_CKM.1.1/MTR	The TSF shall generate cryptographic keys in accordance
1663		with a specified cryptographic key generation algorithm
1664		<i>AES-CMAC<sup>88</sup> and specified cryptographic key sizes 128</i>
1665		<i>bit<sup>89</sup> that meet the following: [FIPS Pub. 197], and</i>
1666		<i>[RFC 4493]<sup>90</sup>.</i>
1667	Hierarchical to:	No other components.
1668	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or
1669		FCS_COP.1 Cryptographic operation], fulfilled by
1670		FCS_COP.1/MTR
1671		FCS_CKM.4 Cryptographic key destruction

---

87 [assignment: *list of standards*]

88 [assignment: *cryptographic key generation algorithm*]

89 [assignment: *cryptographic key sizes*]

90 [assignment: *list of standards*]





1698 (see FMT\_SMF.1) as defined by  
1699 FCS\_COP.1/MTR.

1700 **Application Note 20:** If the connection between the Meter and TOE is  
1701 unidirectional, the communication between the Meter and  
1702 the TOE is secured by the use of a symmetric AES  
1703 encryption. If a bidirectional connection between the Meter  
1704 and the TOE is established, the communication is secured  
1705 by a TLS channel as described in chapter 6.4.1. As the  
1706 TOE shall be interoperable with all kind of Meters, both  
1707 kinds of encryption are implemented.

1708 **Application Note 21:** The TOE uses only cryptographic specifications and  
1709 algorithms as described in [TR-03109-3].

## 1710 6.4.4 General Cryptographic support

### 1711 6.4.4.1 Cryptographic key management (FCS\_CKM)

#### 1712 6.4.4.1.1 FCS\_CKM.4: Cryptographic key destruction

1713 FCS\_CKM.4.1 The TSF shall destroy cryptographic keys in accordance  
1714 with a specified cryptographic key destruction method  
1715 *Zeroisation*<sup>95</sup> that meets the following: *none*<sup>96</sup>.

1716 Hierarchical to: No other components.

1717 Dependencies: [FDP\_ITC.1 Import of user data without security attributes,  
1718 or

1719 FDP\_ITC.2 Import of user data with security attributes, or  
1720 FCS\_CKM.1 Cryptographic key generation], fulfilled by  
1721 FCS\_CKM.1/TLS and

1722 FCS\_CKM.1/CMS and FCS\_CKM.1/MTR

1723 **Application Note 22:** Please note that as against the requirement FDP\_RIP.2,  
1724 the mechanisms implementing the requirement from  
1725 FCS\_CKM.4 shall be suitable to avoid attackers with

---

95 [assignment: *cryptographic key destruction method*]

96 [assignment: *list of standards*]

1726		physical access to the TOE from accessing the keys after
1727		they are no longer used.
1728		6.4.4.2 Cryptographic operation (FCS_COP)
1729		<b>6.4.4.2.1 FCS_COP.1/HASH: Cryptographic operation, hashing for</b>
1730		<b>signatures</b>
1731	FCS_COP.1.1/HASH	The TSF shall perform <i>hashing for signature creation and</i>
1732		<i>verification</i> <sup>97</sup> in accordance with a specified cryptographic
1733		algorithm <i>SHA-256, SHA-384 and SHA-512</i> <sup>98</sup> and
1734		cryptographic key sizes <i>none</i> <sup>99</sup> that meet the following:
1735		<i>[FIPS Pub. 180-4]</i> <sup>100</sup> .
1736	Hierarchical to:	No other components.
1737	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1738		or
1739		FDP_ITC.2 Import of user data with security attributes, or
1740		FCS_CKM.1 Cryptographic key generation <sup>101</sup> ]
1741		FCS_CKM.4 Cryptographic key destruction
1742	<b>Application Note 23:</b>	The TOE is only responsible for hashing of data in the
1743		context of digital signatures. The actual signature
1744		operation and the handling (i.e. protection) of the
1745		cryptographic keys in this context is performed by the
1746		Security Module.
1747	<b>Application Note 24:</b>	The TOE uses only cryptographic specifications and
1748		algorithms as described in [TR-03109-3].

---

97 [assignment: *list of cryptographic operations*]

98 [assignment: *cryptographic algorithm*]

99 [assignment: *cryptographic key sizes*]

100 [assignment: *list of standards*]

101 The justification for the missing dependency FCS\_CKM.1 can be found in chapter 6.12.1.3.

1749 **6.4.4.2.2 FCS\_COP.1/MEM: Cryptographic operation, encryption of**  
 1750 **TSF and user data**

1751 FCS\_COP.1.1/MEM The TSF shall perform *TSF and user data encryption and*  
 1752 *decryption*<sup>102</sup> in accordance with a specified cryptographic  
 1753 algorithm *AES-XTS*<sup>103</sup> and cryptographic key sizes *128*  
 1754 *bit*<sup>104</sup> that meet the following: [*FIPS Pub. 197*] and  
 1755 [*NIST 800-38E*]<sup>105</sup>.

1756 Hierarchical to: No other components.

1757 Dependencies: [FDP\_ITC.1 Import of user data without security attributes,  
 1758 or

1759 FDP\_ITC.2 Import of user data with security attributes, or

1760 FCS\_CKM.1 Cryptographic key generation], not fulfilled s.  
 1761 Application Note 25

1762 FCS\_CKM.4 Cryptographic key destruction

1763 **Application Note 25:** Please note that for the key generation process an external  
 1764 security module is used during TOE production.

1765 **Application Note 26:** The TOE encrypts its local TSF and user data while it is  
 1766 not in use (i.e. while stored in a persistent memory).

1767 It shall be noted that this kind of encryption cannot provide  
 1768 an absolute protection against physical manipulation and  
 1769 does not aim to. It however contributes to the security  
 1770 concept that considers the protection that is provided by  
 1771 the environment.

---

102 [assignment: *list of cryptographic operations*]

103 [assignment: *cryptographic algorithm*]

104 [assignment: *cryptographic key sizes*]

105 [assignment: *list of standards*]

## 1772 6.5 Class FDP: User Data Protection

### 1773 6.5.1 Introduction to the Security Functional Policies

1774 The security functional requirements that are used in the following chapters implicitly  
 1775 define a set of Security Functional Policies (SFP). These policies are introduced in the  
 1776 following paragraphs in more detail to facilitate the understanding of the SFRs:

- 1777 • The **Gateway access SFP** is an access control policy to control the access to  
 1778 objects under the control of the TOE. The details of this access control policy  
 1779 highly depend on the concrete application of the TOE. The access control policy  
 1780 is described in more detail in [TR-03109-1].
- 1781 • The **Firewall SFP** implements an information flow policy to fulfil the objective  
 1782 O.Firewall. All requirements around the communication control that the TOE  
 1783 poses on communications between the different networks are defined in this  
 1784 policy.
- 1785 • The **Meter SFP** implements an information flow policy to fulfil the objective  
 1786 O.Meter. It defines all requirements concerning how the TOE shall handle Meter  
 1787 Data.

### 1788 6.5.2 Gateway Access SFP

#### 1789 6.5.2.1 Access control policy (FDP\_ACC)

##### 1790 6.5.2.1.1 FDP\_ACC.2: Complete access control

1791 FDP\_ACC.2.1 The TSF shall enforce the *Gateway access SFP*<sup>106</sup> on  
 1792 *subjects: external entities in WAN, HAN and LMN*  
 1793 *objects: any information that is sent to, from or via*  
 1794 *the TOE and any information that is stored in the*  
 1795 *TOE*<sup>107</sup> and all operations among subjects and  
 1796 objects covered by the SFP.

1797 FDP\_ACC.2.2 The TSF shall ensure that all operations between any  
 1798 subject controlled by the TSF and any object controlled by  
 1799 the TSF are covered by an access control SFP.

---

106 [assignment: *access control SFP*]

107 [assignment: *list of subjects and objects*]

1800	Hierarchical to:	FDP_ACC.1 Subset access control
1801	Dependencies:	FDP_ACF.1 Security attribute based access control
1802	<b>6.5.2.1.2 FDP_ACF.1: Security attribute based access control</b>	
1803	FDP_ACF.1.1	The TSF shall enforce the <i>Gateway access SFP</i> <sup>108</sup> to
1804		objects based on the following:
1805		<i>subjects: external entities on the WAN, HAN or</i>
1806		<i>LMN side</i>
1807		<i>objects: any information that is sent to, from or via</i>
1808		<i>the TOE</i>
1809		<i>attributes: destination interface</i> <sup>109</sup> .
1810	FDP_ACF.1.2	The TSF shall enforce the following rules to determine if
1811		an operation among controlled subjects and controlled
1812		objects is allowed:
1813		• <i>an authorised Consumer is only allowed to have</i>
1814		<i>read access to his own User Data via the interface</i>
1815		<i>IF_GW_CON,</i>
1816		• <i>an authorised Service Technician is only allowed to</i>
1817		<i>have read access to the system log via the interface</i>
1818		<i>IF_GW_SRV, the Service Technician must not be</i>
1819		<i>allowed to read, modify or delete any other TSF</i>
1820		<i>data,</i>
1821		• <i>an authorised Gateway Administrator is allowed to</i>
1822		<i>interact with the TOE only via IF_GW_WAN,</i>
1823		• <i>only authorised Gateway Administrators are</i>
1824		<i>allowed to establish a wake-up call,</i>
1825		• <i>additional rules governing access among controlled</i>
1826		<i>subjects and controlled objects using controlled</i>

---

<sup>108</sup> [assignment: *access control SFP*]

<sup>109</sup> [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

1827		<i>operations on controlled objects or none:</i>
1828		<i>none</i> <sup>110, 111</sup>
1829	FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to
1830		objects based on the following additional rules: <i>none</i> <sup>112</sup> .
1831	FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects
1832		based on the following additional rules:
1833		<ul style="list-style-type: none"> <li>• <i>the Gateway Administrator is not allowed to read</i></li> </ul>
1834		<i>consumption data or the Consumer Log,</i>
1835		<ul style="list-style-type: none"> <li>• <i>nobody must be allowed to read the symmetric</i></li> </ul>
1836		<i>keys used for encryption</i> <sup>113</sup> .
1837	Hierarchical to:	No other components
1838	Dependencies:	FDP_ACC.1 Subset access control
1839		FMT_MSA.3 Static attribute initialisation
1840	<b>6.5.3 Firewall SFP</b>	
1841	6.5.3.1 Information flow control policy (FDP_IFC)	
1842	<b>6.5.3.1.1 FDP_IFC.2/FW: Complete information flow control for</b>	
1843	<b><i>firewall</i></b>	
1844	FDP_IFC.2.1/FW	The TSF shall enforce the <i>Firewall SFP</i> <sup>114</sup> on <i>the TOE,</i>
1845		<i>external entities on the WAN side, external entities on the</i>
1846		<i>LAN side and all information flowing between them</i> <sup>115</sup> and
1847		all operations that cause that information to flow to and
1848		from subjects covered by the SFP.

---

<sup>110</sup> [assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects or none*]

<sup>111</sup> [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

<sup>112</sup> [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

<sup>113</sup> [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

<sup>114</sup> [assignment: *information flow control SFP*]

<sup>115</sup> [assignment: *list of subjects and information*]

1849 FDP\_IFC.2.2/FW The TSF shall ensure that all operations that cause any  
 1850 information in the TOE to flow to and from any subject in  
 1851 the TOE are covered by an information flow control SFP.

1852 Hierarchical to: FDP\_IFC.1 Subset information flow control

1853 Dependencies: FDP\_IFF.1 Simple security attributes

1854 6.5.3.2 Information flow control functions (FDP\_IFF)

1855 **6.5.3.2.1 FDP\_IFF.1/FW: Simple security attributes for Firewall**

1856 FDP\_IFF.1.1/FW The TSF shall enforce the *Firewall SFP* <sup>116</sup> based on the  
 1857 following types of subject and information security  
 1858 attributes:

1859 *subjects: The TOE and external entities on the*  
 1860 *WAN, HAN or LMN side*

1861 *information: any information that is sent to, from or*  
 1862 *via the TOE*

1863 *attributes: destination\_interface (TOE, LMN, HAN*  
 1864 *or WAN), source\_interface (TOE, LMN, HAN or*  
 1865 *WAN), destination\_authenticated,*  
 1866 *source\_authenticated* <sup>117</sup>.

1867 FDP\_IFF.1.2/FW The TSF shall permit an information flow between a  
 1868 controlled subject and controlled information via a  
 1869 controlled operation if the following rules hold:

1870 *(if source\_interface=HAN or*  
 1871 *source\_interface=TOE) and*

1872 *destination\_interface=WAN and*

1873 *destination\_authenticated = true*

1874 *Connection establishment is allowed*  
 1875

---

116 [assignment: *information flow control SFP*]

117 [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]



1876 *if source\_interface=LMN and*  
1877 *destination\_interface= TOE and*  
1878 *source\_authenticated = true*  
1879 *Connection establishment is allowed*  
1880  
1881 *if source\_interface=TOE and*  
1882 *destination\_interface= LMN and*  
1883 *destination\_authenticated = true*  
1884 *Connection establishment is allowed*  
1885  
1886 *if source\_interface=HAN and*  
1887 *destination\_interface= TOE and*  
1888 *source\_authenticated = true*  
1889 *Connection establishment is allowed*  
1890  
1891 *if source\_interface=TOE and*  
1892 *destination\_interface= HAN and*  
1893 *destination\_authenticated = true*  
1894 *Connection establishment is allowed*  
1895 *else*  
1896 *Connection establishment is denied*<sup>118</sup>.  
1897 FDP\_IFF.1.3/FW The TSF shall enforce the *establishment of a connection*  
1898 *to a configured external entity in the WAN after having*  
1899 *received a wake-up message on the WAN interface*<sup>119</sup>.

---

<sup>118</sup> [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

<sup>119</sup> [assignment: *additional information flow control SFP rules*]

1900	FDP_IFF.1.4/FW	The TSF shall explicitly authorise an information flow
1901		based on the following rules: <i>none</i> <sup>120</sup> .
1902	FDP_IFF.1.5/FW	The TSF shall explicitly deny an information flow based on
1903		the following rules: <i>none</i> <sup>121</sup> .
1904	Hierarchical to:	No other components
1905	Dependencies:	FDP_IFC.1 Subset information flow control
1906		FMT_MSA.3 Static attribute initialisation
1907	<b>Application Note 27:</b>	It should be noted that the FDP_IFF.1.1/FW facilitates
1908		different interfaces of the origin and the destination of an
1909		information flow implicitly requires the TOE to implement
1910		physically separate ports for WAN, LMN and HAN.
1911	<b>6.5.4 Meter SFP</b>	
1912	6.5.4.1 Information flow control policy (FDP_IFC)	
1913	<b>6.5.4.1.1 FDP_IFC.2/MTR: Complete information flow control for</b>	
1914	<b>Meter information flow</b>	
1915	FDP_IFC.2.1/MTR	The TSF shall enforce the <i>Meter SFP</i> <sup>122</sup> on <i>the TOE,</i>
1916		<i>attached Meters, authorized External Entities in the WAN</i>
1917		<i>and all information flowing between them</i> <sup>123</sup> and all
1918		operations that cause that information to flow to and from
1919		subjects covered by the SFP.
1920	FDP_IFC.2.2/MTR	The TSF shall ensure that all operations that cause any
1921		information in the TOE to flow to and from any subject in
1922		the TOE are covered by an information flow control SFP.
1923	Hierarchical to:	FDP_IFC.1 Subset information flow control
1924	Dependencies:	FDP_IFF.1 Simple security attributes

---

<sup>120</sup> [assignment: *rules, based on security attributes, that explicitly authorise information flows*]

<sup>121</sup> [assignment: *rules, based on security attributes, that explicitly deny information flows*]

<sup>122</sup> [assignment: *information flow control SFP*]

<sup>123</sup> [assignment: *list of subjects and information*]

1925	6.5.4.2 Information flow control functions (FDP_IFF)	
1926	<b>6.5.4.2.1 FDP_IFF.1/MTR: Simple security attributes for Meter</b>	
1927	<b>information</b>	
1928	FDP_IFF.1.1/MTR	The TSF shall enforce the <i>Meter SFP</i> <sup>124</sup> based on the
1929		following types of subject and information security
1930		attributes:
1931		<ul style="list-style-type: none"> <li>• <i>subjects: TOE, external entities in WAN, Meters located in LMN</i></li> </ul>
1932		
1933		<ul style="list-style-type: none"> <li>• <i>information: any information that is sent via the TOE</i></li> </ul>
1934		
1935		<ul style="list-style-type: none"> <li>• <i>attributes: destination interface, source interface (LMN or WAN), Processing Profile</i><sup>125</sup>.</li> </ul>
1936		
1937	FDP_IFF.1.2/MTR	The TSF shall permit an information flow between a
1938		controlled subject and controlled information via a
1939		controlled operation if the following rules hold:
1940		<ul style="list-style-type: none"> <li>• <i>an information flow shall only be initiated if allowed by a corresponding Processing Profile</i><sup>126</sup>.</li> </ul>
1941		
1942	FDP_IFF.1.3/MTR	The TSF shall enforce the following rules:
1943		<ul style="list-style-type: none"> <li>• Data received from Meters shall be processed as defined in the corresponding Processing Profiles,</li> </ul>
1944		
1945		<ul style="list-style-type: none"> <li>• Results of processing of Meter Data shall be submitted to external entities as defined in the Processing Profiles,</li> </ul>
1946		
1947		
1948		<ul style="list-style-type: none"> <li>• The internal system time shall be synchronised as follows:</li> </ul>
1949		

---

124 [assignment: *information flow control SFP*]

125 [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

126 [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

1950			○ <i>The TOE shall compare the system time to a</i>
1951			<i>reliable external time source every 24</i>
1952			<i>hours</i> <sup>127</sup> .
1953			○ <i>If the deviation between the local time and the</i>
1954			<i>remote time is acceptable</i> <sup>128</sup> , <i>the local system</i>
1955			<i>time shall be updated according to the remote</i>
1956			<i>time.</i>
1957			○ <i>If the deviation is not acceptable the TOE</i>
1958			<i>shall ensure that any following Meter Data is</i>
1959			<i>not used, stop operation</i> <sup>129</sup> <i>and</i>
1960			<i>inform a Gateway Administrator</i> <sup>130</sup> .
1961	FDP_IFF.1.4/MTR		The TSF shall explicitly authorise an information flow
1962			based on the following rules: <i>none</i> <sup>131</sup> .
1963	FDP_IFF.1.5/MTR		The TSF shall explicitly deny an information flow based on
1964			the following rules: <i>The TOE shall deny any acceptance of</i>
1965			<i>information by external entities in the LMN unless the</i>
1966			<i>authenticity, integrity and confidentiality of the Meter Data</i>
1967			<i>could be verified</i> <sup>132</sup> .
1968	Hierarchical to:		No other components
1969	Dependencies:		FDP_IFC.1 Subset information flow control
1970			FMT_MSA.3 Static attribute initialisation
1971	<b>Application Note 28:</b>		FDP_IFF.1.3 defines that the TOE shall update the local
1972			system time regularly with reliable external time sources if
1973			the deviation is acceptable. In the context of this
1974			functionality two aspects should be mentioned:

---

<sup>127</sup> [assignment: *synchronization interval between 1 minute and 24 hours*]

<sup>128</sup> Please refer to the following application note for a detailed definition of “acceptable”.

<sup>129</sup> Please note that this refers to the complete functional operation of the TOE and not only to the update of local time. However, an administrative access shall still be possible.

<sup>130</sup> [assignment: *additional information flow control SFP rules*]

<sup>131</sup> [assignment: *rules, based on security attributes, that explicitly authorise information flows*]

<sup>132</sup> [assignment: *rules, based on security attributes, that explicitly deny information flows*]

1975		<b>Reliability of external source</b>
1976		<p>There are several ways to achieve the reliability of the external source. On the one hand, there may be a source in the WAN that has an acceptable reliability on its own (e.g. because it is operated by a very trustworthy organisation (an official legal time issued by the calibration authority would be a good example for such a source<sup>133</sup>)).</p> <p>On the other hand a developer may choose to maintain multiple external sources that all have a certain level of reliability but no absolute reliability. When using such sources the TOE shall contact more than one source and harmonize the results in order to ensure that no attack happened.</p>
1977		
1978		
1979		
1980		
1981		
1982		
1983		
1984		
1985		
1986		<p><b>Acceptable deviation</b></p> <p>For the question whether a deviation between the time source(s) in the WAN and the local system time is still acceptable, normative or legislative regulations shall be considered. If no regulation exists, a maximum deviation of 3% of the measuring period is allowed to be in conformance with [PP_GW]. It should be noted that depending on the kind of application a more accurate system time is needed. For doing so, the intervall for the comparison of the system time to a reliable external time source is configurable. But this aspect is not within the scope of this Security Target.</p> <p>Please further note that – depending on the exactness of the local clock – it may be required to synchronize the time more often than every 24 hours.</p>
1987		
1988		
1989		
1990		
1991		
1992		
1993		
1994		
1995		
1996		<p><b>Application Note 29:</b></p> <p>In FDP_IFF.1.5/MTR the TOE is required to verify the authenticity, integrity and confidentiality of the Meter Data</p>
1997		
1998		
1999		
2000		
2001		
2002		
2003		
2004		

---

<sup>133</sup> By the time that this ST is developed however, this time source is not yet available.

2005 received from the Meter. The TOE has two options to do  
 2006 so:

- 2007 1. To implement a channel between the Meter and the
- 2008 TOE using the functionality as described in
- 2009 FCS\_COP.1/TLS.
- 2010 2. To accept, decrypt and verify data that has been
- 2011 encrypted by the Meter as required in
- 2012 FCS\_COP.1/MTR if a wireless connection to the
- 2013 meters is established.

2014 The latter possibility can be used only if a wireless  
 2015 connection between the Meter and the TOE is established.

## 2016 **6.5.5 General Requirements on user data protection**

### 2017 6.5.5.1 Residual information protection (FDP\_RIP)

#### 2018 **6.5.5.1.1 FDP\_RIP.2: Full residual information protection**

2019 FDP\_RIP.2.1 The TSF shall ensure that any previous information  
 2020 content of a resource is made unavailable upon the  
 2021 deallocation of the resource from <sup>134</sup> all objects.

2022 Hierarchical to: FDP\_RIP.1 Subset residual information protection

2023 Dependencies: No dependencies.

2024 **Application Note 30:** Please refer to chapter F.9 of part 2 of [CC] for more  
 2025 detailed information about what kind of information this  
 2026 requirement applies to.

2027 Please further note that this SFR has been used in order  
 2028 to ensure that information that is no longer used is made  
 2029 unavailable from a logical perspective. Specifically, it has  
 2030 to be ensured that this information is no longer available  
 2031 via an external interface (even if an access control or  
 2032 information flow policy would fail). However, this does not  
 2033 necessarily mean that the information is overwritten in a

---

134 [selection: *allocation of the resource to, deallocation of the resource from*]

2034 way that makes it impossible for an attacker to get access  
 2035 to is assuming a physical access to the memory of the  
 2036 TOE.

2037 6.5.5.2 Stored data integrity (FDP\_SDI)

#### 2038 **6.5.5.2.1 FDP\_SDI.2: Stored data integrity monitoring and action**

2039 FDP\_SDI.2.1 The TSF shall monitor user data stored in containers  
 2040 controlled by the TSF for *integrity errors*<sup>135</sup> on all objects,  
 2041 based on the following attributes: *cryptographical check*  
 2042 *sum*<sup>136</sup>.

2043 FDP\_SDI.2.2 Upon detection of a data integrity error, the TSF shall  
 2044 *create a system log entry*<sup>137</sup>.

2045 Hierarchical to: FDP\_SDI.1 Stored data integrity monitoring

2046 Dependencies: No dependencies.

## 2047 **6.6 Class FIA: Identification and Authentication**

### 2048 **6.6.1 User Attribute Definition (FIA\_ATD)**

2049 6.6.1.1 FIA\_ATD.1: User attribute definition

2050 FIA\_ATD.1.1 The TSF shall maintain the following list of security  
 2051 attributes belonging to individual users:

- 2052 • *User Identity*
- 2053 • *Status of Identity (Authenticated or not)*
- 2054 • *Connecting network (WAN, HAN or LMN)*
- 2055 • *Role membership*
- 2056 • *none*<sup>138</sup>.

2057 Hierarchical to: No other components.

2058 Dependencies: No dependencies.

---

135 [assignment: *integrity errors*]

136 [assignment: *user data attributes*]

137 [assignment: *action to be taken*]

138 [assignment: *list of security attributes*]

2059	<b>6.6.2 Authentication Failures (FIA_AFL)</b>	
2060	6.6.2.1 FIA_AFL.1: Authentication failure handling	
2061	FIA_AFL.1.1	The TSF shall detect when <u>5</u> <sup>139</sup> unsuccessful authentication attempts occur related to <i>authentication attempts at IF_GW_CON</i> <sup>140</sup> .
2062		
2063		
2064	FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been <u>met</u> <sup>141</sup> , the TSF shall <i>block IF_GW_CON for 5 minutes</i> <sup>142</sup> .
2065		
2066		
2067	Hierarchical to:	No other components
2068	Dependencies:	FIA_UAU.1 Timing of authentication
2069	<b>6.6.3 User Authentication (FIA_UAU)</b>	
2070	6.6.3.1 FIA_UAU.2: User authentication before any action	
2071	FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
2072		
2073		
2074	Hierarchical to:	FIA_UAU.1
2075	Dependencies:	FIA_UID.1 Timing of identification
2076	<b>Application Note 31:</b>	Please refer to [TR-03109-1] for a more detailed overview on the authentication of TOE users.
2077		
2078	6.6.3.2 FIA_UAU.5: Multiple authentication mechanisms	
2079	FIA_UAU.5.1	The TSF shall provide
2080		<ul style="list-style-type: none"> <li>• <i>authentication via certificates at the IF_GW_MTR interface</i></li> </ul>
2081		
2082		<ul style="list-style-type: none"> <li>• <i>TLS-authentication via certificates at the IF_GW_WAN interface</i></li> </ul>
2083		

---

139 [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

140 [assignment: list of authentication events]

141 [selection: met, surpassed]

142 [assignment: list of actions]



- 2084
- 2085
- 2086
- 2087
- 2088
- 2089
- 2090
- 2091
- 2092
- 2093
- 2094
- 2095
- 2096
- 2097
- 2098
- 2099
- 2100
- 2101
- 2102
- 2103
- 2104
- 2105
- 2106
- 2107
- 2108
- 2109
- 2110
- *TLS-authentication via HAN-certificates at the IF\_GW\_CON interface*
  - *authentication via password at the IF\_GW\_CON interface*
  - *TLS-authentication via HAN-certificates at the IF\_GW\_SRV interface*
  - *authentication at the IF\_GW\_CLS interface*
  - *verification via a commands' signature* <sup>143</sup>
- to support user authentication.
- FIA\_UAU.5.2
- The TSF shall authenticate any user's claimed identity according to the
- *meters shall be authenticated via certificates at the IF\_GW\_MTR interface only*
  - *Gateway Administrators shall be authenticated via TLS-certificates at the IF\_GW\_WAN interface only*
  - *Consumers shall be authenticated via TLS-certificates or via password at the IF\_GW\_CON interface only*
  - *Service Technicians shall be authenticated via TLS-certificates at the IF\_GW\_SRV interface only*
  - *CLS shall be authenticated at the IF\_GW\_CLS only*
  - *each command of an Gateway Administrator shall be authenticated by verification of the commands' signature,*
  - *other external entities shall be authenticated via TLS-certificates at the IF\_GW\_WAN interface only* <sup>144</sup>.

---

143 [assignment: *list of multiple authentication mechanisms*]

144 [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

2111	Hierarchical to:	No other components.
2112	Dependencies:	No dependencies.
2113	<b>Application Note 32:</b>	Please refer to [TR-03109-1] for a more detailed overview
2114		on the authentication of TOE users.
2115	6.6.3.3 FIA_UAU.6: Re-authenticating	
2116	FIA_UAU.6.1	The TSF shall re-authenticate <b>an external entity</b> <sup>145</sup> under
2117		the conditions
2118		<ul style="list-style-type: none"> <li>• <i>TLS channel to the WAN shall be disconnected</i></li> </ul>
2119		<i>after 48 hours,</i>
2120		<ul style="list-style-type: none"> <li>• <i>TLS channel to the LMN shall be disconnected after</i></li> </ul>
2121		<i>5 MB of transmitted information,</i>
2122		<ul style="list-style-type: none"> <li>• <i>other local users shall be re-authenticated after at</i></li> </ul>
2123		<i>least 10 minutes</i> <sup>146</sup> <i>of inactivity</i> <sup>147</sup> .
2124	Hierarchical to:	No other components.
2125	Dependencies:	No dependencies.
2126	<b>Application Note 33:</b>	This requirement on re-authentication for external entities
2127		in the WAN and LMN is addressed by disconnecting the
2128		TLS channel even though a re-authentication is - strictly
2129		speaking - only achieved if the TLS channel is build up
2130		again.
2131	<b>6.6.4 User identification (FIA_UID)</b>	
2132	6.6.4.1 FIA_UID.2: User identification before any action	
2133	FIA_UID.2.1	The TSF shall require each user to be successfully
2134		identified before allowing any other TSF-mediated actions
2135		on behalf of that user.
2136	Hierarchical to:	FIA_UID.1
2137	Dependencies:	No dependencies.

---

<sup>145</sup> [refinement: *the user*]

<sup>146</sup> [refinement: *after at least 10 minutes*]. This value is configurable by the authorised Gateway Administrator.

<sup>147</sup> [assignment: *list of conditions under which re-authentication is required*]

2138	<b>6.6.5 User-subject binding (FIA_USB)</b>	
2139	6.6.5.1 FIA_USB.1: User-subject binding	
2140	FIA_USB.1.1	The TSF shall associate the following user security
2141		attributes with subjects acting on the behalf of that user:
2142		<i>attributes as defined in FIA_ATD.1 <sup>148</sup>.</i>
2143	FIA_USB.1.2	The TSF shall enforce the following rules on the initial
2144		association of user security attributes with subjects acting
2145		on the behalf of users:
2146		<ul style="list-style-type: none"><li>• <i>The initial value of the security attribute ‘connecting</i></li></ul>
2147		<i>network’ is set to the corresponding physical</i>
2148		<i>interface of the TOE (HAN, WAN, or LMN).</i>
2149		<ul style="list-style-type: none"><li>• <i>The initial value of the security attribute ‘role</i></li></ul>
2150		<i>membership’ is set to the user role claimed on basis</i>
2151		<i>of the credentials used for authentication at the</i>
2152		<i>connecting network as defined in FIA_UAU.5.2. For</i>
2153		<i>role membership ‘Gateway Administrators’,</i>
2154		<i>additionally the remote network endpoint <sup>149</sup>used</i>
2155		<i>and configured in the TSF data must be identical.</i>
2156		<ul style="list-style-type: none"><li>• <i>The initial value of the security attribute ‘user</i></li></ul>
2157		<i>identity’ is set to the identification attribute of the</i>
2158		<i>credentials used by the subject. The security</i>
2159		<i>attribute ‘user identity’ is set to the subject key ID of</i>
2160		<i>the certificate in case of a certificate-based</i>
2161		<i>authentication, the meter-ID for wired Meters and</i>
2162		<i>the user name owner in case of a password-based</i>
2163		<i>authentication at interface IF_GW_CON.</i>
2164		<ul style="list-style-type: none"><li>• <i>The initial value of the security attribute ‘status of</i></li></ul>
2165		<i>identity’ is set to the authentication status of the</i>
2166		<i>claimed identity. If the authentication is successful</i>
2167		<i>on basis of the used credentials, the status of</i>

---

<sup>148</sup> [assignment: *list of user security attributes*]

<sup>149</sup> The remote network endpoint can be either the remote IP address or the remote host name.

2168 *identity is 'authenticated', otherwise it is*  
 2169 *'not authenticated'* <sup>150</sup>.

2170 FIA\_USB.1.3 The TSF shall enforce the following rules governing  
 2171 changes to the user security attributes associated with  
 2172 subjects acting on the behalf of users:

- 2173 • *security attribute 'connecting network' is not*  
 2174 *changeable.*
- 2175 • *security attribute 'role membership' is not*  
 2176 *changeable.*
- 2177 • *security attribute 'user identity' is not changeable.*
- 2178 • *security attribute 'status of identity' is not*  
 2179 *changeable*<sup>151</sup>.

2180 Hierarchical to: No other components.

2181 Dependencies: FIA\_ATD.1 User attribute definition

## 2182 **6.7 Class FMT: Security Management**

### 2183 **6.7.1 Management of the TSF**

#### 2184 6.7.1.1 Management of functions in TSF (FMT\_MOF)

##### 2185 **6.7.1.1.1 FMT\_MOF.1: Management of security functions** 2186 ***behaviour***

2187 FMT\_MOF.1.1 The TSF shall restrict the ability to modify the behaviour  
 2188 of <sup>152</sup> the functions *for management as defined in*

---

150 [assignment: *rules for the initial association of attributes*]

151 [assignment: *rules for the changing of attributes*]

152 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

2189 *FMT\_SMF.1*<sup>153</sup> to roles and criteria as defined in Table  
 2190 13<sup>154</sup>.

2191 Hierarchical to: No other components.

2192 Dependencies: *FMT\_SMR.1* Security roles

2193 *FMT\_SMF.1* Specification of Management Functions

Function	Limitation
Display the version number of the TOE  Display the current time	The management functions must only be accessible for an authorised Consumer and only via the interface IF_GW_CON. <b>An authorized Service Technician is also able to access the version number of the TOE and the current time of the TOE via interface IF_GW_SRV</b> <sup>155</sup> .
All other management functions as defined in <i>FMT_SMF.1</i>	The management functions must only be accessible for an authorised Gateway Administrator and only via the interface IF_GW_WAN <sup>156</sup> .
Firmware Update	The firmware update must only be possible after the authenticity of the firmware update has been verified (using the services of the Security Module and the trust anchor of the Gateway developer) and if the version number of the new firmware is higher to the version of the installed firmware.
Deletion or modification of events from the Calibration Log	A deletion or modification of events from the calibration log must not be possible.

2194 **Table 13: Restrictions on Management Functions**

153 [assignment: *list of functions*]

154 [assignment: *the authorised identified roles*]

155 The TOE displays the version number of the TOE and the current time of the TOE also to the authorized service technician via the interface IF\_GW\_SRV because the service technician must be able to determine if the current time of the TOE is correct or if the version number of the TOE is correct.

156 This criterion applies to all management functions. The following entries in this table only augment this restriction further.

2195 6.7.1.2 Specification of Management Functions (FMT\_SMF)

2196 **6.7.1.2.1 FMT\_SMF.1: Specification of Management Functions**

2197 FMT\_SMF.1.1 The TSF shall be capable of performing the following  
 2198 management functions: *list of management functions as*  
 2199 *defined in Table 14 and Table 15 and additional*  
 2200 *functionalities: none* <sup>157</sup>.

2201 Hierarchical to: No other components.

2202 Dependencies: No dependencies.

SFR	Management functionality
FAU_ARP.1/SYS	<ul style="list-style-type: none"> <li><del>The management (addition, removal, or modification) of actions</del> <sup>158</sup></li> </ul>
FAU_GEN.1/SYS FAU_GEN.1/CON FAU_GEN.1/CAL	-
FAU_SAA.1/SYS	<ul style="list-style-type: none"> <li><del>Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules</del> <sup>158</sup></li> </ul>
FAU_SAR.1/SYS FAU_SAR.1/CON FAU_SAR.1/CAL	- <sup>159</sup>
FAU_STG.4/SYS FAU_STG.4/CON	<ul style="list-style-type: none"> <li><del>Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure</del> <sup>158</sup></li> <li><del>Size configuration of the audit trail that is available before the oldest events get overwritten</del> <sup>158</sup></li> </ul>

157 [assignment: *list of management functions to be provided by the TSF*]

158 The TOE does not have the indicated management ability since there exist no standard method calls for the Gateway Administrator to enforce such management ability.

159 As the rules for audit review are fixed within [PP\_GW], the management functions as defined by [CC, part 2] do not apply.

FAU_STG.4/CAL	- 160
FAU_GEN.2	-
FAU_STG.2	<ul style="list-style-type: none"> <li>Maintenance of the parameters that control the audit storage capability for the consumer log <del>and the system log</del><sup>158</sup></li> </ul>
FCO_NRO.2	<ul style="list-style-type: none"> <li>The management of changes to <del>information types, fields,</del><sup>158</sup> originator attributes and recipients of evidence</li> </ul>
FCS_CKM.1/TLS	-
FCS_COP.1/TLS	<ul style="list-style-type: none"> <li>Management of key material including key material stored in the Security Module</li> </ul>
FCS_CKM.1/CMS	-
FCS_COP.1/CMS	<ul style="list-style-type: none"> <li>Management of key material including key material stored in the Security Module</li> </ul>
FCS_CKM.1/MTR	-
FCS_COP.1/MTR	<ul style="list-style-type: none"> <li>Management of key material stored in the Security Module and key material brought into the gateway during the pairing process</li> </ul>
FCS_CKM.4	-
FCS_COP.1/HASH	-
FCS_COP.1/MEM	<ul style="list-style-type: none"> <li><del>Management of key material</del></li> </ul>
FDP_ACC.2	-
FDP_ACF.1	-
FDP_IFC.2/FW	-

---

<sup>160</sup> As the actions that shall be performed if the audit trail is full are fixed within [PP\_GW], the management functions as defined by [CC, part 2] do not apply.

FDP_IFF.1/FW	<ul style="list-style-type: none"> <li>Managing the attributes used to make explicit access based decisions</li> <li>Add authorised units for communication (pairing)</li> <li>Management of endpoint to be contacted after successful wake-up call</li> <li>Management of CLS systems</li> </ul>
FDP_IFC.2/MTR	-
FDP_IFF.1/MTR	<ul style="list-style-type: none"> <li>Managing the attributes (including Processing Profiles) used to make explicit access based decisions</li> </ul>
FDP_RIP.2	-
FDP_SDI.2	<ul style="list-style-type: none"> <li><del>The actions to be taken upon the detection of an integrity error shall be configurable.</del><sup>158</sup></li> </ul>
FIA_ATD.1	<ul style="list-style-type: none"> <li>If so indicated in the assignment, the authorised Gateway Administrator might be able to define additional security attributes for users<sup>161</sup>.</li> </ul>
FIA_AFL.1	<ul style="list-style-type: none"> <li><del>Management of the threshold for unsuccessful authentication attempts</del><sup>158</sup></li> <li><del>Management of actions to be taken in the event of an authentication failure</del><sup>158</sup></li> </ul>
FIA_UAU.2	<ul style="list-style-type: none"> <li>Management of the authentication data by an Gateway Administrator</li> </ul>
FIA_UAU.5	- 162
FIA_UAU.6	<ul style="list-style-type: none"> <li>Management of re-authentication time</li> </ul>

<sup>161</sup> In the assignment it is not indicated that the authorized Gateway Administrator might be able to define additional security attributes for users.

<sup>162</sup> As the rules for re-authentication are fixed within [PP\_GW], the management functions as defined by [CC, part 2] do not apply.



FIA_UID.2	<ul style="list-style-type: none"> <li>The management of the user identities</li> </ul>
FIA_USB.1	<ul style="list-style-type: none"> <li><del>An authorised Gateway Administrator can define default subject security attributes, if so indicated in the assignment of FIA_ATD.1.</del><sup>158</sup></li> <li><del>An authorised Gateway Administrator can change subject security attributes, if so indicated in the assignment of FIA_ATD.1.</del><sup>158</sup></li> </ul>
FMT_MOF.1	<ul style="list-style-type: none"> <li><del>Managing the group of roles that can interact with the functions in the TSF</del></li> </ul>
FMT_SMF.1	-
FMT_SMR.1	<ul style="list-style-type: none"> <li>Managing the group of users that are part of a role</li> </ul>
FMT_MSA.1/AC	<ul style="list-style-type: none"> <li><del>Management of rules by which security attributes inherit specified values</del><sup>163,158</sup></li> </ul>
FMT_MSA.3/AC	- <sup>164</sup>
FMT_MSA.1/FW	<ul style="list-style-type: none"> <li><del>Management of rules by which security attributes inherit specified values</del><sup>165,158</sup></li> </ul>
FMT_MSA.3/FW	- <sup>166</sup>
FMT_MSA.1/MTR	<ul style="list-style-type: none"> <li><del>Management of rules by which security attributes inherit specified values</del><sup>167,158</sup></li> </ul>

163 As the role that can interact with the security attributes is restricted to the Gateway Administrator within [PP\_GW], not all management functions as defined by [CC, part 2] do apply.

164 As no role is allowed to specify alternative initial values within [PP\_GW], the management functions as defined by [CC, part 2] do not apply.

165 As the role that can read, modify, delete or add the security attributes is restricted to the Gateway Administrator within [PP\_GW], not all management functions as defined by [CC, part 2] do apply.

166 As no role is allowed to specify alternative initial values within [PP\_GW], the management functions as defined by [CC, part 2] do not apply.

167 As the role that can read, modify, delete or add the security attributes is restricted to the Gateway Administrator within [PP\_GW], not all management functions as defined by [CC, part 2] do apply.

FMT_MSA.3/MTR	- 168
FPR_CON.1	<ul style="list-style-type: none"> <li><del>Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE</del> <sup>158</sup></li> </ul>
FPR_PSE.1	-
FPT_FLS.1	-
FPT_RPL.1	-
FPT_STM.1	<ul style="list-style-type: none"> <li>Management a time source</li> </ul>
FPT_TST.1	- 169
FPT_PHP.1	<ul style="list-style-type: none"> <li><del>Management of the user or role that determines whether physical tampering has occurred</del> <sup>158</sup></li> </ul>
FTP_ITC.1/WAN	- 170
FTP_ITC.1/MTR	- 171
FTP_ITC.1/USR	- 172

2203

**Table 14: SFR related Management Functionalities**

---

168 As no role is allowed to specify alternative initial values within [PP\_GW], the management functions as defined by [CC, part 2] do not apply.

169 As the rules for TSF testing are fixed within [PP\_GW], the management functions as defined by [CC, part 2] do not apply.

170 As the configuration of the actions that require a trusted channel is fixed by [PP\_GW], the management functions as defined in [CC, part 2] do not apply.

171 As the configuration of the actions that require a trusted channel is fixed by [PP\_GW], the management functions as defined in [CC, part 2] do not apply.

172 As the configuration of the actions that require a trusted channel is fixed by [PP\_GW], the management functions as defined in [CC, part 2] do not apply.

2204

<b>Gateway specific Management functionality</b>
Pairing of a Meter
Performing a firmware update
Displaying the current version number of the TOE
Displaying the current time
Management of certificates of external entities in the WAN for communication
Resetting of the TOE <sup>173</sup>

2205

**Table 15: Gateway specific Management Functionalities**

2206

**6.7.2 Security management roles (FMT\_SMR)**

2207

6.7.2.1 FMT\_SMR.1: Security roles

2208

FMT\_SMR.1.1                      The TSF shall maintain the roles *authorised Consumer, authorised Gateway Administrator, authorised Service Technician, the authorised identified roles: authorised external entity, CLS, and Meter* <sup>174</sup>.

2209

2210

2211

2212

FMT\_SMR.1.2                      The TSF shall be able to associate users with roles.

2213

Hierarchical to:                      No other components.

2214

Dependencies:                      No dependencies.

---

<sup>173</sup> Resetting the TOE will be necessary when the TOE stopped operation due to a critical deviation between local and remote time (see FDP\_IFF.1.3/MTR) ~~or when the calibration log is full.~~

<sup>174</sup> [assignment: *the authorised identified roles*]

2215	<b>6.7.3 Management of security attributes for Gateway access SFP</b>	
2216	6.7.3.1 Management of security attributes (FMT_MSA)	
2217	<b>6.7.3.1.1 FMT_MSA.1/AC: Management of security attributes for</b>	
2218	<b>Gateway access SFP</b>	
2219	FMT_MSA.1.1/AC	The TSF shall enforce the <i>Gateway access SFP</i> <sup>175</sup> to
2220		restrict the ability to <u>query, modify, delete, other</u>
2221		<u>operations: none</u> <sup>176</sup> the security attributes <i>all relevant</i>
2222		<i>security attributes</i> <sup>177</sup> to <i>authorised Gateway</i>
2223		<i>Administrators</i> <sup>178</sup> .
2224	Hierarchical to:	No other components.
2225	Dependencies:	[FDP_ACC.1 Subset access control, or
2226		FDP_IFC.1 Subset information flow control], fulfilled by
2227		FDP_ACC.2
2228		FMT_SMR.1 Security roles
2229		FMT_SMF.1 Specification of Management Functions
2230	<b>6.7.3.1.2 FMT_MSA.3/AC: Static attribute initialisation for Gateway</b>	
2231	<b>access SFP</b>	
2232	FMT_MSA.3.1/AC	The TSF shall enforce the <i>Gateway access SFP</i> <sup>179</sup> to
2233		provide <u>restrictive</u> <sup>180</sup> default values for security attributes
2234		that are used to enforce the SFP.
2235	FMT_MSA.3.2/AC	The TSF shall allow the <i>no role</i> <sup>181</sup> to specify alternative
2236		initial values to override the default values when an object
2237		or information is created.

---

175 [assignment: *access control SFP(s), information flow control SFP(s)*]

176 [selection: *change\_default, query, modify, delete, [assignment: other operations]*]

177 [assignment: *list of security attributes*]

178 [assignment: *the authorised identified roles*]

179 [assignment: *access control SFP, information flow control SFP*]

180 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

181 [assignment: *the authorised identified roles*]

2238	Hierarchical to:	No other components.
2239	Dependencies:	FMT_MSA.1 Management of security attributes
2240		FMT_SMR.1 Security roles
2241		<b>6.7.4 Management of security attributes for Firewall SFP</b>
2242		6.7.4.1 Management of security attributes (FMT_MSA)
2243		<b>6.7.4.1.1 FMT_MSA.1/FW: Management of security attributes for</b>
2244		<b>firewall policy</b>
2245	FMT_MSA.1.1/FW	The TSF shall enforce the <i>Firewall SFP</i> <sup>182</sup> to restrict the
2246		ability to <u>query, modify, delete, other operations: none</u> <sup>183</sup>
2247		the security attributes <i>all relevant security attributes</i> <sup>184</sup> to
2248		<i>authorised Gateway Administrators</i> <sup>185</sup> .
2249	Hierarchical to:	No other components.
2250	Dependencies:	[FDP_ACC.1 Subset access control, or
2251		FDP_IFC.1 Subset information flow control], fulfilled by
2252		FDP_IFC.2/FW
2253		FMT_SMR.1 Security roles
2254		FMT_SMF.1 Specification of Management Functions
2255		<b>6.7.4.1.2 FMT_MSA.3/FW: Static attribute initialisation for Firewall</b>
2256		<b>policy</b>
2257	FMT_MSA.3.1/FW	The TSF shall enforce the <i>Firewall SFP</i> <sup>186</sup> to provide
2258		<u>restrictive</u> <sup>187</sup> default values for security attributes that are
2259		used to enforce the SFP.

---

182 [assignment: *access control SFP(s), information flow control SFP(s)*]

183 [selection: *change\_default, query, modify, delete, [assignment: other operations]*]

184 [assignment: *list of security attributes*]

185 [assignment: *the authorised identified roles*]

186 [assignment: *access control SFP, information flow control SFP*]

187 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

2260	FMT_MSA.3.2/FW	The TSF shall allow the <i>no role</i> <sup>188</sup> to specify alternative
2261		initial values to override the default values when an object
2262		or information is created.
2263	Hierarchical to:	No other components.
2264	Dependencies:	FMT_MSA.1 Management of security attributes
2265		FMT_SMR.1 Security roles
2266	<b>Application Note 34:</b>	The definition of restrictive default rules for the firewall
2267		information flow policy refers to the rules as defined in
2268		FDP_IFF.1.2/FW and FDP_IFF.1.5/FW. Those rules apply
2269		to all information flows and must not be overwritable by
2270		anybody.
2271	<b>6.7.5 Management of security attributes for Meter SFP</b>	
2272	6.7.5.1 Management of security attributes (FMT_MSA)	
2273	<b>6.7.5.1.1 FMT_MSA.1/MTR: Management of security attributes for</b>	
2274	<b>Meter policy</b>	
2275	FMT_MSA.1.1/MTR	The TSF shall enforce the <i>Meter SFP</i> <sup>189</sup> to restrict the
2276		ability to <u>change default, query, modify, delete, other</u>
2277		<u>operations: none</u> <sup>190</sup> the security attributes <i>all relevant</i>
2278		<i>security attributes</i> <sup>191</sup> to <i>authorised Gateway</i>
2279		<i>Administrators</i> <sup>192</sup> .
2280	Hierarchical to:	No other components.
2281	Dependencies:	[FDP_ACC.1 Subset access control, or
2282		FDP_IFC.1 Subset information flow control], fulfilled by
2283		FDP_IFC.2/FW
2284		FMT_SMR.1 Security roles

---

<sup>188</sup> [assignment: *the authorised identified roles*]

<sup>189</sup> [assignment: *access control SFP(s), information flow control SFP(s)*]

<sup>190</sup> [selection: *change\_default, query, modify, delete, [assignment: other operations]*]

<sup>191</sup> [assignment: *list of security attributes*]

<sup>192</sup> [assignment: *the authorised identified roles*]

2285		FMT_SMF.1 Specification of Management Functions
2286	<b>6.7.5.1.2</b>	<b><i>FMT_MSA.3/MTR: Static attribute initialisation for Meter</i></b>
2287		<b><i>policy</i></b>
2288	FMT_MSA.3.1/MTR	The TSF shall enforce the <i>Meter SFP</i> <sup>193</sup> to provide
2289		<u>restrictive</u> <sup>194</sup> default values for security attributes that are
2290		used to enforce the SFP.
2291	FMT_MSA.3.2/MTR	The TSF shall allow the <i>no role</i> <sup>195</sup> to specify alternative
2292		initial values to override the default values when an object
2293		or information is created.
2294	Hierarchical to:	No other components.
2295	Dependencies:	FMT_MSA.1 Management of security attributes
2296		FMT_SMR.1 Security roles
2297		
2298	<b>6.8</b>	<b>Class FPR: Privacy</b>
2299	<b>6.8.1</b>	<b>Communication Concealing (FPR_CON)</b>
2300	6.8.1.1	FPR_CON.1: Communication Concealing
2301	FPR_CON.1.1	The TSF shall enforce the <i>Firewall SFP</i> <sup>196</sup> in order to
2302		ensure that no personally identifiable information (PII) can
2303		be obtained by an analysis of <i>frequency, load, size or the</i>
2304		<i>absence of external communication</i> <sup>197</sup> .
2305	FPR_CON.1.2	The TSF shall connect to <i>the Gateway Administrator,</i>
2306		<i>authorized External Entity in the WAN</i> <sup>198</sup> in intervals as

---

<sup>193</sup> [assignment: *access control SFP, information flow control SFP*]

<sup>194</sup> [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

<sup>195</sup> [assignment: *the authorised identified roles*]

<sup>196</sup> [assignment: *information flow policy*]

<sup>197</sup> [assignment: *characteristics of the information flow that need to be concealed*]

<sup>198</sup> [assignment: *list of external entities*]

2307		follows <u>daily, other interval: none</u> <sup>199</sup> to conceal the data
2308		flow <sup>200</sup> .
2309	Hierarchical to:	No other components.
2310	Dependencies:	No dependencies.
2311	<b>6.8.2 Pseudonymity (FPR_PSE)</b>	
2312	6.8.2.1 FPR_PSE.1 Pseudonymity	
2313	FPR_PSE.1.1	The TSF shall ensure that <i>external entities in the WAN</i> <sup>201</sup>
2314		are unable to determine the real user name bound to
2315		<i>information neither relevant for billing nor for a secure</i>
2316		<i>operation of the Grid sent to parties in the WAN</i> <sup>202</sup> .
2317	FPR_PSE.1.2	The TSF shall be able to provide <i>aliases as defined by the</i>
2318		<i>Processing Profiles</i> <sup>203</sup> <del>of the real user name for the</del>
2319		<b>Meter and Gateway identity</b> <sup>204</sup> to <i>external entities in the</i>
2320		<i>WAN</i> <sup>205</sup> .
2321	FPR_PSE.1.3	The TSF shall <u>determine an alias for a user</u> <sup>206</sup> and verify
2322		that it conforms to the <i>alias given by the Gateway</i>
2323		<i>Administrator in the Processing Profile</i> <sup>207</sup> .
2324	Hierarchical to:	No other components.
2325	Dependencies:	No dependencies.
2326	<b>Application Note 35:</b>	When the TOE submits information about the consumption
2327		or production of a certain commodity that is not relevant for
2328		the billing process nor for a secure operation of the Grid,
2329		there is no need that this information is sent with a direct

---

199 [selection: *weekly, daily, hourly, [assignment: other interval]*]

200 The TOE uses a randomized value of about ±50 percent per delivery.

201 [assignment: *set of users and/or subjects*]

202 [assignment: *list of subjects and/or operations and/or objects*]

203 [assignment: *number of aliases*]

204 [refinement: *of the real user name*]

205 [assignment: *list of subjects*]

206 [selection, choose one of: *determine an alias for a user, accept the alias from the user*]

207 [assignment: *alias metric*]



2330 link to the identity of the consumer. In those cases, the  
 2331 TOE shall replace the identity of the Consumer by a  
 2332 pseudonymous identifier. Please note that the identity of  
 2333 the Consumer may not be their name but could also be a  
 2334 number (e.g. consumer ID) used for billing purposes.

2335 A Gateway may use more than one pseudonymous  
 2336 identifier.

2337 A complete anonymisation would be beneficial in terms of  
 2338 the privacy of the consumer. However, a complete  
 2339 anonymous set of information would not allow the external  
 2340 entity to ensure that the data comes from a trustworthy  
 2341 source.

2342 Please note that an information flow shall only be initiated  
 2343 if allowed by a corresponding Processing Profile.

2344

## 2345 **6.9 Class FPT: Protection of the TSF**

### 2346 **6.9.1 Fail secure (FPT\_FLS)**

2347 6.9.1.1 FPT\_FLS.1: Failure with preservation of secure state

2348 FPT\_FLS.1.1 The TSF shall preserve a secure state when the following  
 2349 types of failures occur:

- 2350 • *the deviation between local system time of the TOE*
- 2351 *and the reliable external time source is too large,*
- 2352 • *TOE hardware / firmware integrity violation or*
- 2353 • *TOE software application integrity violation* <sup>208</sup>.

2354 Hierarchical to: No other components.

2355 Dependencies: No dependencies.

2356 **Application Note 36:** The local clock shall be as exact as required by normative  
 2357 or legislative regulations. If no regulation exists, a

---

208 [assignment: *list of types of failures in the TSF*]

2358 maximum deviation of 3% of the measuring period is  
 2359 allowed to be in conformance with [PP\_GW].

## 2360 **6.9.2 Replay Detection (FPT\_RPL)**

### 2361 6.9.2.1 FPT\_RPL.1: Replay detection

2362 FPT\_RPL.1.1 The TSF shall detect replay for the following entities: *all*  
 2363 *external entities* <sup>209</sup>.

2364 FPT\_RPL.1.2 The TSF shall perform *ignore replayed data* <sup>210</sup> when  
 2365 replay is detected.

2366 Hierarchical to: No other components.

2367 Dependencies: No dependencies.

## 2368 **6.9.3 Time stamps (FPT\_STM)**

### 2369 6.9.3.1 FPT\_STM.1: Reliable time stamps

2370 FPT\_STM.1.1 The TSF shall be able to provide reliable time stamps.

2371 Hierarchical to: No other components.

2372 Dependencies: No dependencies.

2373

## 2374 **6.9.4 TSF self test (FPT\_TST)**

### 2375 6.9.4.1 FPT\_TST.1: TSF testing

2376 FPT\_TST.1.1 The TSF shall run a suite of self tests during initial startup,  
 2377 at the request of a user and periodically during normal  
 2378 operation <sup>211</sup> to demonstrate the correct operation of the  
 2379 TSF <sup>212</sup>.

---

209 [assignment: *list of identified entities*]

210 [assignment: *list of specific actions*]

211 [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*[assignment: *conditions under which self test should occur*]]

212 [selection: [assignment: *parts of TSF*], *the TSF*]

2380 FPT\_TST.1.2 The TSF shall provide authorised users with the capability  
 2381 to verify the integrity of TSF data <sup>213</sup>.

2382 FPT\_TST.1.3 The TSF shall provide authorised users with the capability  
 2383 to verify the integrity of TSF <sup>214</sup>.

2384 Hierarchical to: No other components.

2385 Dependencies: No dependencies.

## 2386 **6.9.5 TSF physical protection (FPT\_PHP)**

2387 6.9.5.1 FPT\_PHP.1: Passive detection of physical attack

2388 FPT\_PHP.1.1 The TSF shall provide unambiguous detection of physical  
 2389 tampering that might compromise the TSF.

2390 FPT\_PHP.1.2 The TSF shall provide the capability to determine whether  
 2391 physical tampering with the TSF's devices or TSF  
 2392 elements has occurred.

2393 Hierarchical to: No other components.

2394 Dependencies: No dependencies.

2395

## 2396 **6.10 Class FTP: Trusted path/channels**

### 2397 **6.10.1 Inter-TSF trusted channel (FTP\_ITC)**

2398 6.10.1.1 FTP\_ITC.1/WAN: Inter-TSF trusted channel for WAN

2399 FTP\_ITC.1.1/WAN The TSF shall provide a communication channel between  
 2400 itself and another trusted IT product that is logically distinct  
 2401 from other communication channels and provides assured  
 2402 identification of its end points and protection of the channel  
 2403 data from modification or disclosure.

---

213 [selection: [assignment: parts of TSF data], TSF data]

214 [selection: [assignment: parts of TSF], TSF]

2404	FTP_ITC.1.2/WAN	The TSF shall permit <u>the TSF</u> <sup>215</sup> to initiate communication
2405		via the trusted channel.
2406	FTP_ITC.1.3/WAN	The TSF shall initiate communication via the trusted
2407		channel for <i>all communications to external entities in the</i>
2408		<i>WAN</i> <sup>216</sup> .
2409	Hierarchical to:	No other components
2410	Dependencies:	No dependencies.
2411	6.10.1.2 FTP_ITC.1/MTR:	Inter-TSF trusted channel for Meter
2412	FTP_ITC.1.1/MTR	The TSF shall provide a communication channel between
2413		itself and another trusted IT product that is logically distinct
2414		from other communication channels and provides assured
2415		identification of its end points and protection of the channel
2416		data from modification or disclosure.
2417	FTP_ITC.1.2/MTR	The TSF shall permit <b>the Meter and the TOE</b> <sup>217</sup> to initiate
2418		communication via the trusted channel.
2419	FTP_ITC.1.3/MTR	The TSF shall initiate communication via the trusted
2420		channel for <i>any communication between a Meter and the</i>
2421		<i>TOE</i> <sup>218</sup> .
2422	Hierarchical to:	No other components.
2423	Dependencies:	No dependencies.
2424	<b>Application Note 37:</b>	The corresponding cryptographic primitives are defined by
2425		FCS_COP.1/MTR.
2426	6.10.1.3 FTP_ITC.1/USR:	Inter-TSF trusted channel for User
2427	FTP_ITC.1.1/USR	The TSF shall provide a communication channel between
2428		itself and another trusted IT product that is logically distinct
2429		from other communication channels and provides assured

---

<sup>215</sup> [selection: *the TSF, another trusted IT product*]

<sup>216</sup> [assignment: *list of functions for which a trusted channel is required*]

<sup>217</sup> [selection: *the TSF, another trusted IT product*]

<sup>218</sup> [assignment: *list of functions for which a trusted channel is required*]

2430		identification of its end points and protection of the channel
2431		data from modification or disclosure.
2432	FTP_ITC.1.2/USR	The TSF shall permit <b>the Consumer, the Service</b>
2433		<b>Technician</b> <sup>219</sup> to initiate communication via the trusted
2434		channel.
2435	FTP_ITC.1.3/USR	The TSF shall initiate communication via the trusted
2436		channel for <i>any communication between a Consumer and</i>
2437		<i>the TOE and the Service Technician and the TOE</i> <sup>220</sup> .
2438	Hierarchical to:	No other components.
2439	Dependencies:	No dependencies.
2440		

## 6.11 Security Assurance Requirements for the TOE

2442 The minimum Evaluation Assurance Level for this Security Target is **EAL 4 augmented**  
 2443 **by AVA\_VAN.5 and ALC\_FLR.2**. The following table lists the assurance components  
 2444 which are therefore applicable to this ST.

Assurance Class	Assurance Component
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4

219 [selection: *the TSF, another trusted IT product*]

220 [assignment: *list of functions for which a trusted channel is required*]

Assurance Class	Assurance Component
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
	<b>ALC_FLR.2</b>
Security Target Evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	<b>AVA_VAN.5</b>

2446 **6.12 Security Requirements rationale**

2447 **6.12.1 Security Functional Requirements rationale**

2448 6.12.1.1 Fulfilment of the Security Objectives

2449 This chapter proves that the set of security requirements (TOE) is suited to fulfil the  
 2450 security objectives described in chapter 4 and that each SFR can be traced back to the  
 2451 security objectives. At least one security objective exists for each security requirement.

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FAU_ARP.1/SYS									X	
FAU_GEN.1/SYS									X	
FAU_SAA.1/SYS									X	
FAU_SAR.1/SYS									X	
FAU_STG.4/SYS									X	
FAU_GEN.1/CON									X	
FAU_SAR.1/CON									X	
FAU_STG.4/CON									X	
FAU_GEN.1/CAL									X	
FAU_SAR.1/CAL									X	
FAU_STG.4/CAL									X	
FAU_GEN.2									X	
FAU_STG.2									X	
FCO_NRO.2				X						

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FCS_CKM.1/TLS					X					
FCS_COP.1/TLS					X					
FCS_CKM.1/CMS					X					
FCS_COP.1/CMS					X					
FCS_CKM.1/MTR					X					
FCS_COP.1/MTR					X					
FCS_CKM.4					X					
FCS_COP.1/HASH					X					
FCS_COP.1/MEM					X		X			
FDP_ACC.2										X
FDP_ACF.1										X
FDP_IFC.2/FW	X	X								
FDP_IFF.1/FW	X	X								
FDP_IFC.2/MTR				X		X				
FDP_IFF.1/MTR				X		X				
FDP_RIP.2							X			
FDP_SDI.2							X			
FIA_ATD.1								X		



	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FIA_AFL.1								X		
FIA_UAU.2								X		
FIA_UAU.5										X
FIA_UAU.6										X
FIA_UID.2								X		
FIA_USB.1								X		
FMT_MOF.1								X		
FMT_SMF.1								X		
FMT_SMR.1								X		
FMT_MSA.1/AC								X		
FMT_MSA.3/AC								X		
FMT_MSA.1/FW								X		
FMT_MSA.3/FW								X		
FMT_MSA.1/MTR								X		
FMT_MSA.3/MTR								X		
FPR_CON.1			X							
FPR_PSE.1				X						
FPT_FLS.1							X			

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FPT_RPL.1					X					
FPT_STM.1						X			X	
FPT_TST.1		X					X			
FPT_PHP.1							X			
FTP_ITC.1/WAN	X									
FTP_ITC.1/MTR				X						
FTP_ITC.1/USR									X	

2452 **Table 17: Fulfilment of Security Objectives**

2453 The following paragraphs contain more details on this mapping.

2454 **6.12.1.1.1 O.Firewall**

2455 O.Firewall is met by a combination of the following SFRs:

- 2456 • **FDP\_IFC.2/FW** defines that the TOE shall implement an information flow policy
- 2457 for its firewall functionality.
- 2458 • **FDP\_IFF.1/FW** defines the concrete rules for the firewall information flow policy.
- 2459 • **FTP\_ITC.1/WAN** defines the policy around the trusted channel to parties in the
- 2460 WAN.

2461 **6.12.1.1.2 O.SeparateIF**

2462 O.SeparateIF is met by a combination of the following SFRs:

- 2463 • **FDP\_IFC.2/FW** and **FDP\_IFF.1/FW** implicitly require the TOE to implement
- 2464 physically separate ports for WAN and LMN.
- 2465 • **FPT\_TST.1** implements a self test that also detects whether the ports for WAN
- 2466 and LAN have been interchanged.

2467 **6.12.1.1.3 O.Conceal**2468 O.Conceal is completely met by **FPR\_CON.1** as directly follows.2469 **6.12.1.1.4 O.Meter**

2470 O.Meter is met by a combination of the following SFRs:

- 2471 • **FDP\_IFC.2/MTR** and **FDP\_IFF.1/MTR** define an information flow policy to  
2472 introduce how the Gateway shall handle Meter Data.
- 2473 • **FCO\_NRO.2** ensure that all Meter Data will be signed by the Gateway (invoking  
2474 the services of its Security Module) before being submitted to external entities.
- 2475 • **FPR\_PSE.1** defines requirements around the pseudonymization of Meter  
2476 identities for Status data.
- 2477 • **FTP\_ITC.1/MTR** defines the requirements around the Trusted Channel that  
2478 shall be implemented by the Gateway in order to protect information submitted  
2479 via the Gateway and external entities in the WAN or the Gateway and a  
2480 distributed Meter.

2481

2482        **6.12.1.1.5 O.Crypt**

2483        O.Crypt is met by a combination of the following SFRs:

- 2484            • **FCS\_CKM.4** defines the requirements around the secure deletion of ephemeral  
2485            cryptographic keys.
- 2486            • **FCS\_CKM.1/TLS** defines the requirements on key negotiation for the TLS  
2487            protocol.
- 2488            • **FCS\_CKM.1/CMS** defines the requirements on key generation for symmetric  
2489            encryption within CMS.
- 2490            • **FCS\_COP.1/TLS** defines the requirements around the encryption and  
2491            decryption capabilities of the Gateway for communications with external parties  
2492            and to Meters.
- 2493            • **FCS\_COP.1/CMS** defines the requirements around the encryption and  
2494            decryption of content and administration data.
- 2495            • **FCS\_CKM.1/MTR** defines the requirements on key negotiation for meter com-  
2496            munication encryption.
- 2497            • **FCS\_COP.1/MTR** defines the cryptographic primitives for meter  
2498            communication encryption.
- 2499            • **FCS\_COP.1/HASH** defines the requirements on hashing that are needed in the  
2500            context of digital signatures (which are created and verified by the Security  
2501            Module).
- 2502            • **FCS\_COP.1/MEM** defines the requirements around the encryption of TSF data.
- 2503            • **FPT\_RPL.1** ensures that a replay attack for communications with external  
2504            entities is detected.

2505        **6.12.1.1.6 O.Time**

2506        O.Time is met by a combination of the following SFRs:

- 2507            • **FDP\_IFC.2/MTR** and **FDP\_IFF.1/MTR** define the required update functionality  
2508            for the local time as part of the information flow control policy for handling Meter  
2509            Data.
- 2510            • **FPT\_STM.1** defines that the TOE shall be able to provide reliable time stamps.

2511

2512 **6.12.1.1.7 O.Protect**

2513 O.Protect is met by a combination of the following SFRs:

- 2514 • **FCS\_COP.1/MEM** defines that the TOE shall encrypt its TSF and user data as  
2515 long as it is not in use.
- 2516 • **FDP\_RIP.2** defines that the TOE shall make information unavailable as soon  
2517 as it is no longer needed.
- 2518 • **FDP\_SDI.2** defines requirements around the integrity protection for stored data.
- 2519 • **FPT\_FLS.1** defines requirements that the TOE falls back to a safe state for  
2520 specific error cases.
- 2521 • **FPT\_TST.1** defines the self testing functionality to detect whether the interfaces  
2522 for WAN and LAN are separate.
- 2523 • **FPT\_PHP.1** defines the exact requirements around the physical protection that  
2524 the TOE has to provide.

2525 **6.12.1.1.8 O.Management**

2526 O.Management is met by a combination of the following SFRs:

- 2527 • **FIA\_ATD.1** defines the attributes for users.
- 2528 • **FIA\_AFL.1** defines the requirements if the authentication of users fails multiple  
2529 times.
- 2530 • **FIA\_UAU.2** defines requirements around the authentication of users.
- 2531 • **FIA\_UID.2** defines requirements around the identification of users.
- 2532 • **FIA\_USB.1** defines that the TOE must be able to associate users with subjects  
2533 acting on behalf of them.
- 2534 • **FMT\_MOF.1** defines requirements around the limitations for management of  
2535 security functions.
- 2536 • **FMT\_MSA.1/AC** defines requirements around the limitations for management  
2537 of attributes used for the Gateway access SFP.
- 2538 • **FMT\_MSA.1/FW** defines requirements around the limitations for management  
2539 of attributes used for the Firewall SFP.
- 2540 • **FMT\_MSA.1/MTR** defines requirements around the limitations for management  
2541 of attributes used for the Meter SFP.
- 2542 • **FMT\_MSA.3/AC** defines the default values for the Gateway access SFP.
- 2543 • **FMT\_MSA.3/FW** defines the default values for the Firewall SFP.
- 2544 • **FMT\_MSA.3/MTR** defines the default values for the Meter SFP.

- 2545
- **FMT\_SMF.1** defines the management functionalities that the TOE must offer.
- 2546
- **FMT\_SMR.1** defines the role concept for the TOE.

2547

#### **6.12.1.1.9 O.Log**

2548 O.Log defines that the TOE shall implement three different audit processes that are  
2549 covered by the Security Functional Requirements as follows:

2550

##### **System Log**

2551 The implementation of the system log itself is covered by the use of **FAU\_GEN.1/SYS**.  
2552 **FAU\_ARP.1/SYS** and **FAU\_SAA.1/SYS** allow to define a set of criteria for automated  
2553 analysis of the audit and a corresponding response. **FAU\_SAR.1/SYS** defines the  
2554 requirements around the audit review functions and that access to them shall be limited  
2555 to authorised Gateway Administrators via the IF\_GW\_WAN interface and to authorised  
2556 Service Technicians via the IF\_GW\_SRV interface. Finally, **FAU\_STG.4/SYS** defines  
2557 the requirements on what should happen if the audit log is full.

2558

##### **Consumer Log**

2559 The implementation of the consumer log itself is covered by the use of  
2560 **FAU\_GEN.1/CON**. **FAU\_STG.4/CON** defines the requirements on what should happen  
2561 if the audit log is full. **FAU\_SAR.1/CON** defines the requirements around the audit review  
2562 functions for the consumer log and that access to them shall be limited to authorised  
2563 Consumer via the IF\_GW\_CON interface. **FTP\_ITC.1/USR** defines the requirements on  
2564 the protection of the communication of the Consumer with the TOE.

2565

##### **Calibration Log**

2566 The implementation of the calibration log itself is covered by the use of  
2567 **FAU\_GEN.1/CAL**. **FAU\_STG.4/CAL** defines the requirements on what should happen  
2568 if the audit log is full. **FAU\_SAR.1/CAL** defines the requirements around the audit review  
2569 functions for the calibration log and that access to them shall be limited to authorised  
2570 Gateway Administrators via the IF\_GW\_WAN interface.

2571 **FAU\_GEN.2**, **FAU\_STG.2** and **FPT\_STM.1** apply to all three audit processes.

2572

#### **6.12.1.1.10 O.Access**

2573 **FDP\_ACC.2** and **FDP\_ACF.1** define the access control policy as required to address  
2574 O.Access. **FIA\_UAU.5** ensures that entities that would like to communicate with the TOE  
2575 are authenticated before any action whereby **FIA\_UAU.6** ensures that external entities

2576 in the WAN are re-authenticated after the session key has been used for a certain  
 2577 amount of time.

2578 6.12.1.2 Fulfilment of the dependencies

2579 The following table summarises all TOE functional requirements dependencies of this  
 2580 ST and demonstrates that they are fulfilled.

SFR	Dependencies	Fulfilled by
FAU_ARP.1/SYS	FAU_SAA.1 Potential violation analysis	FAU_SAA.1/SYS
FAU_GEN.1/SYS	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAA.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_SAR.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_STG.4/SYS	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.1/CON	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR.1/CON	FAU_GEN.1 Audit data generation	FAU_GEN.1/CON
FAU_STG.4/CON	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.1/CAL	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR.1/CAL	FAU_GEN.1 Audit data generation	FAU_GEN.1/CAL
FAU_STG.4/CAL	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1/SYS FAU_GEN.1/CON FIA_UID.2
FAU_STG.2	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS FAU_GEN.1/CON FAU_GEN.1/CAL

FCO_NRO.2	FIA_UID.1 Timing of identification	FIA_UID.2
FCS_CKM.1/TLS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TLS  FCS_CKM.4
FCS_COP.1/TLS	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/TLS  FCS_CKM.4
FCS_CKM.1/CMS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CMS  FCS_CKM.4
FCS_COP.1/CMS	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/CMS  FCS_CKM.4
FCS_CKM.1/MTR	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/MTR  FCS_CKM.4
FCS_COP.1/MTR	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or	FCS_CKM.1/TLS  FCS_CKM.4



	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/TLS FCS_CKM.1/CMS FCS_CKM.1/MTR
FCS_COP.1/HASH	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Please refer to chapter 6.12.1.3 for missing dependency FCS_CKM.4
FCS_COP.1/MEM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	not fulfilled <sup>221</sup> FCS_CKM.4
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.2 FMT_MSA.3/AC
FDP_IFC.2/FW	FDP_IFF.1 Simple security attributes	FDP_IFF.1/FW

<sup>221</sup> The key will be generated by secure production environment and not the TOE itself.

FDP_IFF.1/FW	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2/FW FMT_MSA.3/FW
FDP_IFC.2/MTR	FDP_IFF.1 Simple security attributes	FDP_IFF.1/MTR
FDP_IFF.1/MTR	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2/MTR FMT_MSA.3/MTR
FDP_RIP.2	-	-
FDP_SDI.2	-	-
FIA_ATD.1	-	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.5	-	-
FIA_UAU.6	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FMT_MSA.1/AC	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1

	FMT_SMF.1 Specification of Management Functions	
FMT_MSA.3/AC	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/AC FMT_SMR.1
FMT_MSA.1/FW	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/WAN  FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/FW	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/FW FMT_SMR.1
FMT_MSA.1/MTR	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/MTR  FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/MTR	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/MTR FMT_SMR.1
FPR_CON.1	-	-
FPR_PSE.1	-	-
FPT_FLS.1	-	-
FPT_RPL.1	-	-
FPT_STM.1	-	-
FPT_TST.1	-	-

FPT_PHP.1	-	-
FTP_ITC.1/WAN	-	-
FTP_ITC.1/MTR	-	-
FTP_ITC.1/USR	-	-

2581 **Table 18: SFR Dependencies**

2582 6.12.1.3 Justification for missing dependencies

2583 Dependency FCS\_CKM.1 for FCS\_COP.1/MEM ist not fulfilled. For the key generation  
 2584 process an external security module (“D-HSM”) is used so that the key is imported from  
 2585 an HSM during TOE production.

2586 The hash algorithm as defined in FCS\_COP.1/HASH does not need any key material.  
 2587 As such the dependency to an import or generation of key material is omitted for this  
 2588 SFR.

2589 **6.12.2 Security Assurance Requirements rationale**

2590 The decision on the assurance level has been mainly driven by the assumed attack  
 2591 potential. As outlined in the previous chapters of this Security Target it is assumed that  
 2592 – at least from the WAN side – a high attack potential is posed against the security  
 2593 functions of the TOE. This leads to the use of AVA\_VAN.5 (Resistance against high  
 2594 attack potential).

2595 In order to keep evaluations according to this Security Target commercially feasible EAL  
 2596 4 has been chosen as assurance level as this is the lowest level that provides the  
 2597 prerequisites for the use of AVA\_VAN.5.

2598 Eventually, the augmentation by ALC\_FLR.2 has been chosen to emphasize the  
 2599 importance of a structured process for flaw remediation at the developer’s side,  
 2600 specifically for such a new technology.

2601 6.12.2.1 Dependencies of assurance components

2602 The dependencies of the assurance requirements taken from EAL 4 are fulfilled  
 2603 automatically. The augmentation by AVA\_VAN.5 and ALC\_FLR.2 does not introduce  
 2604 additional assurance components that are not contained in EAL 4.

## 2605 7 TOE Summary Specification

2606 The following paragraph provides a TOE summary specification describing how the TOE  
2607 meets each SFR.

2608

### 2609 7.1 SF.1: Authentication of Communication and Role Assignment 2610 for external entities

2611 The TOE contains a software module that authenticates all communication channels  
2612 with WAN, HAN and LMN networks. The authentication is based on the TLS 1.2 protocol  
2613 compliant to [RFC 5246]. According to [TR-03109], this TLS authentication mechanism  
2614 is used for all TLS secured communications channels with external entities. The TOE  
2615 does always implement the bidirectional authentication as required by [TR-03109-1] with  
2616 one exception: if the Consumer requests a password-based authentication from the  
2617 GWA according to [TR-03109-1], and the GWA activates this authentication method for  
2618 this Consumer, the TOE uses a unidirectional TLS authentication. Thus, although the  
2619 client has not sent a valid certificate, the TOE continues the TLS authentication process  
2620 with the password authentication process for this client (see [RFC 5246, chap. 7.4.6.]).  
2621 The password policy to be fulfilled hereby is that the password must be at least 10 char-  
2622 acters long containing at least one character of each of the following character groups:  
2623 capital letters, small letters, digits, and special characters (!"§\$%&/()=?+\*~#',;:-\_). Fur-  
2624 ther characters could also be used.

2625 [TR-03109-1] requires the TOE to use elliptical curves conforming to [RFC 5289]  
2626 whereas the following cipher suites are supported:

- 2627 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,
- 2628 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,
- 2629 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, and
- 2630 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384.

2631 The following elliptical curves are supported by the TOE

- 2632 • BrainpoolP256r1 (according to [RFC 5639]),
- 2633 • BrainpoolP384r1 (according to [RFC 5639]),
- 2634 • BrainpoolP512r1 (according to [RFC 5639]),
- 2635 • NIST P-256 (according to [RFC 5114]), and
- 2636 • NIST P-384 (according to [RFC 5114]).

2637 Alongside, the TOE supports the case of unidirectional communication with wireless me-  
2638 ter (via the wM-Bus protocol), where the external entity is authenticated via AES with  
2639 CMAC authentication. In this case, the AES algorithm is operating in CBC mode with  
2640 128-bit symmetric keys. The authentication is successful in case that the CMAC has  
2641 been successfully verified by the use of a cryptographic key  $K_{\text{mac}}$ . The cryptographic key  
2642 for CMAC authentication ( $K_{\text{mac}}$ ) is derived from the meter individual key MK conformant  
2643 to [TR-03116-3, chap. 7.2]. The meter individual key MK (brought into the TOE by the  
2644 GWA) is selected by the TOE through the MAC-protected but unencrypted meter-id sub-  
2645 mitted by the meter.

2646 The generation of the cryptographic key material for TLS secured communication chan-  
2647 nels utilizes a Security Module. This Security Module is compliant to [TR-03109-2] and  
2648 evaluated according to [SecModPP].

2649 The destruction of cryptographic key material used by the TOE is performed through  
2650 “zeroisation”. The TOE stores all ephemeral keys used for TLS secured communication  
2651 or other cryptographic operations in the RAM only. For instance, whenever a TLS se-  
2652 cured communication is terminated, the TOE wipes the RAM area used for the crypto-  
2653 graphic key material with 0-bytes directly after finishing the usage of that material.

2654 The TOE receives the authentication certificate of the external entity during the hand-  
2655 shake phase of the TLS protocol. For the establishment of the TLS secured communi-  
2656 cation channel, the TOE verifies the correctness of the signed data transmitted during  
2657 the TLS protocol handshake phase. While importing an authentication certificate the  
2658 TOE verifies the certificate chain of the certificate for all certificates of the SM-PKI ac-  
2659 cording to [TR-03109-4]. Note, that the certificate used for the TLS-based authentication  
2660 of wired meters is self-signed and not part of the SM-PKI. Additionally, the TOE checks  
2661 whether the certificate is configured by the Gateway Administrator for the used interface,  
2662 and whether the remote IP address used and configured in the TSF data are identical  
2663 (**FIA\_USB.1**). The TOE does not check the certificate’s revocation status. In order to  
2664 authenticate the external entity, the key material of the TOE’s communication partner  
2665 must be known and trusted.

2666 The following communication types are known to the TOE <sup>222</sup>:

2667 a) WAN communication via IF\_GW\_WAN

---

<sup>222</sup> Please note that the TOE additionally offers the interface IF\_GW\_SM to the certified Security Module built into the TOE.

- 2668                   b) LMN communication via IF\_GW\_MTR (wireless or wired Meter)  
2669                   c) HAN communication via IF\_GW\_CON, IF\_GW\_CLS or IF\_GW\_SRV

2670                   Except the communication with wireless meters at IF\_GW\_MTR, all communication  
2671                   types are TLS-based. In order to accept a TLS communication connection as being au-  
2672                   thenticated, the following conditions must be fulfilled:

- 2673                   a) The TLS channel must have been established successfully with the required  
2674                   cryptographic mechanisms.  
2675                   b) The certificate of the external entity must be known and trusted through config-  
2676                   uration by the Gateway Administrator, and associated with the according com-  
2677                   munication type<sup>223</sup>.

2678                   For the successfully authenticated external entity, the TOE performs an internal assign-  
2679                   ment of the communication type based on the certificate received at the external inter-  
2680                   face if applicable. The user identity is associated with the name of the certificate owner  
2681                   in case of a certificate-based authentication or with the user name in case of a password-  
2682                   based authentication at interface IF\_GW\_CON.

2683                   For the LMN communication of the TOE with wireless (a.k.a. wM-Bus-based) meters,  
2684                   the external entity is authenticated by the use of the AES-CMAC algorithm and the me-  
2685                   ter-ID for wired Meters is used for association to the user identity (**FIA\_USB.1**). This  
2686                   communication is only allowed for meters not supporting TLS-based communication  
2687                   scenarios.

2688                   **FCS\_CKM.1/TLS** is fulfilled by the TOE through the implementation of the pseudoran-  
2689                   dom function of the TLS protocol compliant to [RFC 5246] while the Security Module is  
2690                   used by the TOE for the generation of the cryptographic key material. The use of TLS  
2691                   according to [RFC 5246] and the use of the postulated cipher suites according to  
2692                   [RFC 5639] fulfill the requirement **FCS\_COP.1/TLS**. The requirements  
2693                   **FCS\_CKM.1/MTR** and **FCS\_COP.1/MTR** are fulfilled by the use of AES-CMAC-secured  
2694                   communication for wireless meters. The requirement **FCS\_CKM.4** is fulfilled by the de-  
2695                   scribed method of “zeroisation” when destroying cryptographic key material. The imple-  
2696                   mentation of the described mechanisms (especially the use of TLS and AES-CBC with  
2697                   CMAC) fulfills the requirements **FTP\_ITC.1/WAN**, **FTP\_ITC.1/MTR**, and

---

<sup>223</sup> Of course, this does not apply if password-based authentication is configured at IF\_GW\_CON.

2698 **FTP\_ITC.1/USR. FPT\_RPL.1** is fulfilled by the use of the TLS protocol respectively the  
2699 integration of transmission counters according to [TR-03116-3, chap. 7.3].

2700 A successfully established connection will be automatically disconnected by the TOE if  
2701 a TLS channel to the WAN is established more than 48 hours, if a TLS channel to the  
2702 LMN has transmitted more than 5 MB of information or if a channel to a local user is  
2703 inactive for a time configurable by the authorised Gateway Administrator of up to 10  
2704 minutes, and a new connection establishment will require a new full authentication pro-  
2705 cedure (**FIA\_UAU.6**). In any case – whether the connection has been successfully es-  
2706 tablished or not – all associated resources related with the connection or connection  
2707 attempt are freed. The implementation of this requirement is done by means of the TOE's  
2708 operation system monitoring and limiting the resources of each process. This means  
2709 that with each connection (or connection attempt) an internal session is created that is  
2710 associated with resources monitored and limited by the TOE. All resources are freed  
2711 even before finishing a session if the respective resource is no longer needed so that no  
2712 previous information content of a resource is made available. Especially, the associated  
2713 cryptographic key material is wiped as soon it is no longer needed. As such, the TOE  
2714 ensures that during the phase of connection termination the internal session is also ter-  
2715 minated and by this, all internal data (associated cryptographic key material and volatile  
2716 data) is wiped by the zeroisation procedure described. Allocated physical resources are  
2717 also freed. In case non-volatile data is no longer needed, the associated resources data  
2718 are freed, too. The TOE doesn't reuse any objects after deallocation of the resource  
2719 (**FDP\_RIP.2**).

2720 If the external entity can be successfully authenticated on basis of the received certificate  
2721 (or the password in case of a consumer using password authentication) and the ac-  
2722 claimed identity could be approved for the used external interface, the TOE associates  
2723 the user identity, the authentication status and the connecting network to the role ac-  
2724 cording to the internal role model (**FIA\_ATD.1**). In order to implement this, the TOE uti-  
2725 lizes an internal data model which supplies the allowed communication network and  
2726 other restricting properties linked with the submitted security attribute on the basis of the  
2727 submitted authentication data providing the multiple mechanisms for authentication of  
2728 any user's claimed identity according to the necessary rules according to [TR-03109-1]  
2729 (**FIA\_UAU.5**).

2730 In case of wireless meter communication (via the wM-Bus protocol), the security attribute  
2731 of the Meter is the meter-id authenticated by the CMAC, where the meter-id is the identity  
2732 providing criterion that is used by the TOE. The identity of the Meter is associated to the



2733 successfully authenticated external entity by the TOE and linked to the respective role  
2734 according to Table 5 and its active session. In this case, the identity providing criterion  
2735 is also the meter-id.

2736 The TOE enforces an explicit and complete security policy protecting the data flow for  
2737 all external entities (**FDP\_IFC.2/FW**, **FDP\_IFF.1/FW**, **FDP\_IFC.2/MTR**,  
2738 **FDP\_IFF.1/MTR**). The security policy defines the accessibility of data for each external  
2739 entity and additionally the permitted actions for these data. Moreover, the external enti-  
2740 ties do also underlie restrictions for the operations which can be executed with the TOE  
2741 (**FDP\_ACF.1**). In case that it is not possible to authenticate an external entity success-  
2742 fully (e.g. caused by unknown authentication credentials), no other action is allowed on  
2743 behalf of this user and the concerning connection is terminated (**FIA\_UAU.2**). Any com-  
2744 munication is only possible after successful authentication and identification of the ex-  
2745 ternal entity (**FIA\_UID.2**, **FIA\_USB.1**).

2746 The reception of the wake-up service data package is a special case that requests the  
2747 TOE to establish a TLS authenticated and protected connection to the Gateway Admin-  
2748 istrator. The TOE validates the data package due to its compliance to the structure de-  
2749 scribed in [TR-03109-1] and verifies the ECDSA signature with the public key of the  
2750 Gateway Administrator's certificate which must be known and trusted to the TOE. The  
2751 TOE does not perform a revocation check or any validity check compliant to the shell  
2752 model. The TOE verifies the electronic signature successfully when the certificate is  
2753 known, trusted and associated to the Gateway Administrator. The TOE establishes the  
2754 connection to the Gateway Administrator when the package has been validated due to  
2755 its structural conformity, the signature has been verified and the integrated timestamp  
2756 fulfills the requirements of [TR-03109-1]. Receiving the data package and the successful  
2757 validation of the wake-up package does not mean that the Gateway Administrator has  
2758 successfully been authenticated.

2759 If the Gateway Administrator could be successfully authenticated based on the certificate  
2760 submitted during the TLS handshake phase, the role will be assigned by the TOE ac-  
2761 cording to now approved identity based on the internal role model and the TLS channel  
2762 will be established.

### 2763 **WAN roles**

2764 The TOE assigns the following roles in the WAN communication (**FMT\_SMR.1**):

- 2765 • authorised Gateway Administrator,
- 2766 • authorised External Entity.

2767 The role assignment is based on the X.509 certificate used by the external entity during  
2768 TLS connection establishment. The TOE has explicit knowledge of the Gateway Admin-  
2769 istrator's certificate and the assignment of the role "Gateway Administrator" requires the  
2770 successful authentication of the WAN connection.

2771 The assignment of the role "Authorized External Entity" requires the X.509 certificate  
2772 that is used during the TLS handshake to be part of an internal trust list that is under  
2773 control of the TOE.

2774 The role "Authorized External Entity" can be assigned to more than one external entity.

#### 2775 **HAN roles**

2776 The TOE differentiates and assigns the following roles in the HAN communication  
2777 (**FMT\_SMR.1**):

- 2778 • authorised Consumer
- 2779 • authorised Service Technician

2780 The role assignment is based on the X.509 certificate used by the external entity for  
2781 TLS-secured communication channels or on password-based authentication at interface  
2782 IF\_GW\_CON if configured (**FIA\_USB.1**).

2783 The assignment of roles in the HAN communication requires the successful identification  
2784 of the external entity as a result of a successful authentication based on the certificate  
2785 used for the HAN connection. The certificates used to authenticate the "Consumer" or  
2786 the "Service Technician" are explicitly known to the TOE through configuration by the  
2787 Gateway Administrator.

#### 2788 **Multi-client capability in the HAN**

2789 The HAN communication might use more than one, parallel and independent authenti-  
2790 cated communication channels. The TOE ensures that the certificates that are used for  
2791 the authentication are different from each other.

2792 The role "Consumer" can be assigned to multiple, parallel sessions. The TOE ensures  
2793 that these parallel sessions are logically distinct from each other by the use of different  
2794 authentication information. This ensures that only the Meter Data associated with the  
2795 authorized user are provided and Meter Data of other users are not accessible.

#### 2796 **LMN roles**

2797 One of the following authentication mechanisms is used for Meters:

- 2798 a) authentication by the use of TLS according to [RFC 5246] for wired Meters  
2799 a) authentication by the use of AES with CMAC authentication according to  
2800 [RFC 3394] for wireless Meters.

2801 The TOE explicitly knows the identification credentials needed for authentication (X.509  
2802 certificate when using TLS; meter-id in conjunction with CMAC and known  $K_{mac}$  when  
2803 using AES) through configuration by the Gateway Administrator. If the Meter could be  
2804 successfully authenticated and the claimed identity could thus be proved, the according  
2805 role “Authorised External Entity” is assigned by the TOE for this Meter at IF\_GW\_MTR  
2806 based on the internal role model.

### 2807 **LMN multi-client capabilities**

2808 The LMN communication can be run via parallel, logically distinct and separately au-  
2809 thenticated communication channels. The TOE ensures that the authentication creden-  
2810 tials of each separate channel are different.

2811 The TOE’s internal policy for access to data and objects under control of the TOE is  
2812 closely linked with the identity of the external entity at IF\_GW\_MTR according to the  
2813 TOE-internal role model. Based on the successfully verified authentication data, a per-  
2814 mission catalogue with security attributes is internally assigned, which defines the al-  
2815 lowed actions and access permissions within a communication channel.

2816 The encapsulation of the TOE processes run by this user is realized through the mech-  
2817 anisms offered by the TOE’s operating system and very restrictive user rights for each  
2818 process. Each role is assigned to a separate, limited user account in the TOE’s operating  
2819 system. For all of these accounts, it is only allowed to read, write or execute the files  
2820 absolutely necessary for implementing the program logic. For each identity interacting  
2821 with the TOE, a separate operating system process is started. Especially, the databases  
2822 used by the TOE and the logging service are adequately separated for enforcement of  
2823 the necessary security domain separation (**FDP\_ACF.1**). The allowed actions and ac-  
2824 cess permissions and associated objects are assigned to the successfully approved  
2825 identity of the user based on the used authentication credentials and the resulting asso-  
2826 ciated role. The current session is unambiguously associated with this user. No interac-  
2827 tion (e.g. access to Meter Data) is possible without an appropriate permission catalogue  
2828 (**FDP\_ACC.2**). The freeing of the role assignment and associated resources are ensured  
2829 through the monitoring of the current session.

## 2830 7.2SF.2: Acceptance and Deposition of Meter Data, Encryption of 2831 Meter Data for WAN transmission

2832 The TOE receives Meter Data from an LMN communication channel and deposits these  
2833 Meter Data with the associated data for tariffing in a database especially assigned to this  
2834 individual Meter residing in an encrypted file system (**FCS\_COP.1/MEM**). The time in-  
2835 terval for receiving or retrieving Meter Data can be configured individually per meter  
2836 through a successfully authenticated Gateway Administrator and are initialized by the  
2837 TOE during the setup procedure with pre-defined values.

2838 The Meter Data are cryptographically protected and their integrity is verified by the TOE  
2839 before the tariffing and deposition is performed. In case of a TLS secured communica-  
2840 tion, the integrity and confidentiality of the transmitted data is protected by the TLS pro-  
2841 tocol according to [RFC 5246]. In case of a unidirectional communication at  
2842 IF\_GW\_MTR/wireless, the integrity is verified by the verification of the CMAC check sum  
2843 whereas the protection of the confidentiality is given by the use of AES in CBC mode  
2844 with 128 bit key length in combination with the CMAC authentication (**FCS\_CKM.1/MTR**,  
2845 **FCS\_COP.1/MTR**). The AES encryption key has been brought into the TOE via a man-  
2846 agement function during the pairing process for the Meter. In the TOE's internal data  
2847 model, the used cryptographic keys  $K_{mac}$  and  $K_{enc}$  are associated with the meter-id due  
2848 to the fact of the unidirectional communication. The TOE contains a packet monitor for  
2849 Meter Data to avoid replay attacks based on the re-sending of Meter Data packages. In  
2850 case of recognized data packets which have already been received and processed by  
2851 the TOE, these data packets are blocked by the packet monitor (**FPT\_RPL.1**).

2852 Concerning the service layers, the TOE detects replay attacks that can occur during  
2853 authentication processes against the TOE or for example receiving data from one of the  
2854 involved communication networks. This is for instance achieved through the correct in-  
2855 terpretation of the strictly increasing ordering numbers for messages from the meters (in  
2856 case that a TLS-secured communication channel is not used), through the enforcement  
2857 of an appropriate time slot of execution for successfully authenticated wake-up calls, and  
2858 of course through the use of the internal means of the TLS protocol according to  
2859 [RFC 5246] (**FPT\_RPL.1**).

2860 The deposition of Meter Data is performed in a way that these Meter Data are associated  
2861 with a permission profile. This means that all of the operations and actions that can be  
2862 taken with these data as described afterwards (e.g. sending via WAN to an Authenti-  
2863 cated External Entity) depend on the permissions which are associated with the

2864 Meter Data. For metrological purposes, the Meter Data's security attribute - if applicable  
2865 - will be persisted associated with its corresponding Meter Data by the TOE. All user  
2866 associated data stored by the TOE are protected by an AES-128-CMAC value. Before  
2867 accessing these data, the TOE verifies the CMAC value that has been applied to the  
2868 user data and detects integrity errors on any data and especially on user associated  
2869 Meter Data in a reliable manner (**FDP\_SDI.2**).

2870 Closely linked with the deposition of the Meter Data is the assignment of an unambigu-  
2871 ous and reliable timestamp on these data. The reliability grounds on the regular use of  
2872 an external time source offering a sufficient exactness (**FPT\_STM.1**) which is used to  
2873 synchronize the operating system of the TOE. A maximum deviation of 3% of the meas-  
2874 uring period is allowed to be in conformance with [PP\_GW]. The data set (Meter Data  
2875 and tariff data) is associated with the timestamp in an inseparably manner because each  
2876 Meter Data entry in the database includes the corresponding time stamp and the data-  
2877 base is cryptographically protected through the encrypted file system. For details about  
2878 database encryption please see page 150).

2879 For transmission of consumption data (tariffed Meter Data) or status data into the WAN,  
2880 the TOE ensures that the data are encrypted and digitally signed (**FCO\_NRO.2**,  
2881 **FCS\_CKM.1/CMS**, **FCS\_COP.1/CMS**, **FCS\_COP.1/HASH**, **FCS\_COP.1/MEM**). In case  
2882 of a successful transmission of consumption data into the WAN, beside the transmitted  
2883 data the data's signature applied by the TOE is logged in the Consumer-Log for the  
2884 respective Consumer at IF\_GW\_CON thus providing the possibility not only for the re-  
2885 cipient to verify the evidence of origin for the transmitted data but to the Consumer at  
2886 IF\_GW\_CON, too (**FCO\_NRO.2**). The encryption is performed with the hybrid encryption  
2887 as specified in [TR-03109-1-I] in combination with [TR-03116-3]. The public key of the  
2888 external entity, the data have to be encrypted for, is known by the TOE through the  
2889 authentication data configured by the Gateway Administrator and its assigned identity.  
2890 This public key is assumed by the TOE to be valid because the TOE does not verify the  
2891 revocation status of certificates. The public key used for the encryption of the derived  
2892 symmetric key used for transmission of consumption data is different from the public key  
2893 in the TLS certificate of the external entity used for the TLS secured communication  
2894 channel. The derivation of the hybrid key used for transmission of consumption data is  
2895 done according to [TR-03116-3, chapter 8].

2896 The TOE does also foresee the case that the data is encrypted for an external entity that  
2897 is not directly assigned to the external entity holding the active communication channel.  
2898 The electronic signature is created through the utilization of the Security Module whereas

2899 the TOE is responsible for the computation of the hash value for the data to be signed.  
2900 Therefore, the TOE utilizes the SHA-256 or SHA-384 hash algorithm. The SHA-512 hash  
2901 algorithm is available in the TOE but not yet used (**FCS\_COP.1/HASH**). The data to be  
2902 sent to the external entity are prepared on basis of the tariffed meter data. The data to  
2903 be transmitted are removed through deallocation of the resources after the (successful  
2904 or unsuccessful) transmission attempt so that afterwards no previous information will be  
2905 available (**FDP\_RIP.2**). The created temporary session keys which have been used for  
2906 encryption of the data are also deleted by the already described zeroisation mechanism  
2907 as soon they are no longer needed (**FCS\_CKM.4**).

2908 The time interval for transmission of the data is set for a daily transmission, and can be  
2909 additionally configured by the Gateway Administrator. The TOE sends randomly gener-  
2910 ated messages into the WAN, so that through this the analysis of frequency, load, size  
2911 or the absence of external communication is concealed (**FPR\_CON.1**). Data that are not  
2912 relevant for accounting are aliased for transmission so that no personally identifiable  
2913 information (PII) can be obtained by an analysis of not billing-relevant information sent  
2914 to parties in the WAN. Therefore, the TOE utilizes the alias as defined by the Gateway  
2915 Administrator in the Processing Profile for the Meter identity to external parties in the  
2916 WAN. Thereby, the TOE determines the alias for a user and verifies that it conforms to  
2917 the alias given in the Processing Profile (**FPR\_PSE.1**).

2918

### 2919 **7.3SF.3: Administration, Configuration and SW Update**

2920 The TOE includes functionality that allows its administration and configuration as well as  
2921 updating the TOE's complete firmware ("firmware updates") or only the software appli-  
2922 cation including the service layer ("software updates"). This functionality is only provided  
2923 for the authenticated Gateway Administrator (**FMT\_MOF.1**, **FMT\_MSA.1/AC**,  
2924 **FMT\_MSA.1/FW**, **FMT\_MSA.1/MTR**).

2925 The following operations can be performed by the successfully authenticated Gateway  
2926 Administrator:

- 2927 a) Definition and deployment of Processing Profiles including user administration,  
2928 rights management and setting configuration parameters of the TOE
- 2929 b) Deployment of tariff information
- 2930 c) Deployment and installation of software/firmware updates



2931 A complete overview of the possible management functions is given in Table 14 and  
2932 Table 15 (**FMT\_SMF.1**). Beside the possibility for a successfully authenticated Service  
2933 Technician to view the system log via interface IF\_GW\_SRV, administrative or configu-  
2934 ration measures on the TOE can only be taken by the successfully authenticated Gate-  
2935 way Administrator.

2936 In order to perform these measures, the TOE has to establish a TLS secured channel  
2937 to the Gateway Administrator and must authenticate the Gateway Administrator suc-  
2938 cessfully. There are two possibilities:

- 2939 a) The TOE independently contacts the Gateway Administrator at a certain time  
2940 specified in advance by the Gateway Administrator.
- 2941 b) Through a message sent to the wake-up service, the TOE is requested to con-  
2942 tact the Gateway Administrator.

2943 In the second case, the wake-up data packet is received by the TOE from the WAN and  
2944 checked by the TOE for structural correctness according to [TR-03109-1]. Afterwards,  
2945 the TOE verifies the correctness of the electronic signature applied to the wake-up mes-  
2946 sage data packet using the certificate of the Gateway Administrator stored in the TSF  
2947 data. Afterwards, a TLS connection to the Gateway Administrator is established by the  
2948 TOE and the above mentioned operations can be performed.

2949 Software/firmware updates always have to be signed by the TOE manufacturer.

2950 Software/firmware updates can be of different content:

- 2951 a) The whole boot image of the TOE is changed.
- 2952 b) Only individual components of the TOE are changed. These components can  
2953 be the boot loader plus the static kernel or the SMGW application.

2954 The update packet is realized in form of an archive file enveloped into a CMS signature  
2955 container according to [RFC 5652]. The electronic signature of the update packet is cre-  
2956 ated using signature keys from the TOE manufacturer. The verification of this signature  
2957 is performed by the TOE using the TOE's Security Module using the trust anchor of the  
2958 TOE manufacturer. If the signature of the transferred data could not be successfully  
2959 verified by the TOE or if the version number of the new firmware is not higher than the  
2960 version number of the installed firmware, the received data is rejected by the TOE and  
2961 not used for further processing. Any administrator action is entered in the System Log of  
2962 the TOE. Additionally, an authorised Consumer can interact with the TOE via the

2963 interface IF\_GW\_CON to get the version number and the current time displayed  
2964 (**FMT\_MOF.1**).

2965 The signature of the update packet is immediately verified after receipt. After successful  
2966 verification of the update packet the update process is immediately performed. In each  
2967 case, the Gateway Administrator gets notified by the TOE and an entry in the TOE's  
2968 system log will be written.

2969 All parameters that can be changed by the Gateway Administrator are preset with re-  
2970 strictive values by the TOE. No role can specify alternative initial values to override these  
2971 restrictive default values (**FMT\_MSA.3/AC**, **FMT\_MSA.3/FW**, **FMT\_MSA.3/MTR**).

2972 This mechanism is supported by the TOE-internal resource monitor that internally mon-  
2973 itors existing connections, assigned roles and operations allowed at a specific time.

2974

#### 2975 **7.4 SF.4: Displaying Consumption Data**

2976 The TOE offers the possibility of displaying consumption data to authenticated Consum-  
2977 ers at interface IF\_GW\_CON. Therefore, the TOE contains a web server that implements  
2978 TLS-based communication with mutual authentication (**FTP\_ITC.1/USR**). If the Con-  
2979 sumer requests a password-based authentication from the GWA according to [TR-  
2980 03109-1] and the GWA activates this authentication method for this Consumer, the TOE  
2981 uses TLS authentication with server-side authentication and HTTP digest access au-  
2982 thentication according to [RFC 7616]. In both cases, the requirement **FCO\_NRO.2** is  
2983 fulfilled through the use of TLS-based communication and through encryption and digital  
2984 signature of the (tariffed) Meter Data to be displayed using **FCS\_COP.1/HASH**.

2985 To additionally display consumption data, a connection at interface IF\_GW\_CON must  
2986 be established and the role "(authorised) Consumer" is assigned to the user with his  
2987 used display unit by the TOE. Different Consumer can use different display units. The  
2988 amount of allowed connection attempts at IF\_GW\_CON is set to 5. In case the amount  
2989 of allowed connection attempts is reached, the TOE blocks IF\_GW\_CON (**FIA\_AFL.1**).  
2990 The display unit has to technically support the applied authentication mechanism and  
2991 the HTTP protocol version 1.1 according to [RFC 2616] as communication protocol. Data  
2992 is provided as HTML data stream and transferred to the display unit. In this case, further  
2993 processing of the transmitted data stream is carried out by the display unit.

2994 According to [TR-03109-1], the TOE exclusively transfers Consumer specific consump-  
2995 tion data to the display unit. The Consumer can be identified in a clear and unambiguous



2996 manner due to the applied authentication mechanism. Moreover, the TOE ensures that  
2997 exclusively the data actually assigned to the Consumer is provided at the display unit  
2998 via IF\_GW\_CON (**FIA\_USB.1**).

2999

## 3000 **7.5 SF.5: Audit and Logging**

3001 The TOE generates audit data for all actions assigned in the System-Log  
3002 (**FAU\_GEN.1/SYS**), the Consumer-Log (**FAU\_GEN.1/CON**), and the Calibration-Log  
3003 (**FAU\_GEN.1/CAL**) as well. On the one hand, this applies to the values measured by  
3004 the Meter (Consumer-Log) and on the other hand to system data (System-Log) used by  
3005 the Gateway Administrator of the TOE in order to check the TOE's current functional  
3006 status. In addition, metrological entries are created in the Calibration-Log. The TOE thus  
3007 distinguishes between the following log classes:

- 3008 a) System-Log
- 3009 b) Consumer-Log
- 3010 c) Calibration-Log

3011 The TOE audits and logs all security functions that are used. Thereby, the TOE compo-  
3012 nent accomplishing this security audit functionality includes the necessary rules moni-  
3013 toring these audited events and through this indicating a potential violation of the en-  
3014 forcement of the TOE security functionality (e. g. in case of an integrity violation, replay  
3015 attack or an authentication failure). If such a security breach is detected, it is shown as  
3016 such in the log entry (**FAU\_SAA.1/SYS**).

3017 The System-Log can only be read by the authorized Gateway Administrator via interface  
3018 IF\_GW\_WAN or by an authorized Service Technician via interface IF\_GW\_SRV  
3019 (**FAU\_SAR.1/SYS**). Potential security breaches are separately indicated and identified  
3020 as such in the System-Log and the GWA gets informed about this potential security  
3021 breach (**FAU\_ARP.1/SYS**, **FDP\_SDI.2**). Data of the Consumer-Log can exclusively be  
3022 viewed by authenticated Consumers via interface IF\_GW\_CON designed to display con-  
3023 sumption data (**FAU\_SAR.1/CON**). The data included in the Calibration-Log can only be  
3024 read by the authenticated Gateway Administrator via interface IF\_GW\_WAN  
3025 (**FAU\_SAR.1/CAL**).

3026 If possible, each log entry is assigned to an identity that is known to the TOE. For audit  
3027 events resulting from actions of identified users resp. roles, the TOE associates the

3028 generated log information to the identified users while generating the audit information  
3029 (**FAU\_GEN.2**).

3030 Generated audit and log data are stored in a cryptographically secured storage. For this  
3031 purpose, a file-based SQL database system is used securing its' data using an AES-  
3032 XTS-128 encrypted file system (AES in XTS mode with 128-bit keys) according to  
3033 [FIPS Pub. 197] and [NIST 800-38E]. This is achieved by using device-specific AES  
3034 keys so that the secure environment can only be accessed with the associated symmet-  
3035 ric key available. Using an appropriately limited access of this symmetric, the TOE im-  
3036 plements the necessary rules so that it can be ensured that unauthorised modification  
3037 or deletion is prohibited (**FAU\_STG.2**).

3038 Audit and log data are stored in separate locations: One location is used to store Con-  
3039 sumer-specific log data (Consumer-Log) whereas device status data and metrological  
3040 data are stored in a separate location: status data are stored in the System-Log and  
3041 metrological data are stored in the Calibration-Log. Each of these logs is located in phys-  
3042 ically separate databases secured by different cryptographic keys. In case of several  
3043 external meters, a separate database is created for each Meter to store the respective  
3044 consumption and log data (**FAU\_GEN.2**).

3045 If the audit trail of the System-Log or the Consumer-Log is full (so that no further data  
3046 can be added), the oldest entries in the audit trail are overwritten (**FAU\_STG.2**,  
3047 **FAU\_STG.4/SYS**, **FAU\_STG.4/CON**). If the Consumer-Log's oldest audit record must  
3048 be kept because the period of billing verification (of usually 15 months) has not been  
3049 reached, the TOE's metrological activity is paused until the oldest audit record gets  
3050 deletable. Thereafter, the TOE's metrological activity is started again through an internal  
3051 timer. Moreover, the mechanism for storing log entries is designed in a way that these  
3052 entries are cryptographically protected against unauthorized deletion. This is especially  
3053 achieved by assigning cryptographic keys to each of the individual databases for the  
3054 System-Log, Consumer-Log and Calibration-Log.

3055 If the Calibration-Log cannot store any further data, the operation of the TOE is stopped  
3056 through the termination of its metering services and the TOE informs the Gateway Ad-  
3057 ministrator by creating an entry in the System-Log, so that additional measures can be  
3058 taken by the Gateway Administrator. Calibration-Log entries are never overwritten by  
3059 the TOE (**FAU\_STG.2**, **FAU\_STG.4/CAL**, **FMT\_MOF.1**).

3060 The TOE anonymizes the data in a way that no conclusions about a specific person or  
3061 user can be drawn from the log or recorded not billing relevant data. Stored consumption

3062 data are exclusively intended for accounting with the energy supplier. The data stored  
3063 in the System-Log are used for analysis purposes concerning necessary technical anal-  
3064 yses and possible security-related information.

## 3065 **7.6 SF.6: TOE Integrity Protection**

3066 The TOE makes physical tampering detectable through the TOE's sealed packaging of  
3067 the device. So if an attacker opens the case, this can be physically noticed, e. g. by the  
3068 Service Technician (**FPT\_PHP.1**).

3069 The TOE provides a secure boot mechanism. Beginning from the AES-128-encrypted  
3070 bootloader protected by a digital signature applied by the TOE manufacturer, each sub-  
3071 sequent step during the boot process is based on the previous step establishing a con-  
3072 tinuous forward-concatenation of cryptographical verification procedures. Thus, it is en-  
3073 sured that each part of the firmware, that means the operating system, the service layers  
3074 and the software application in general, is tested by the TOE during initial startup.  
3075 Thereby, a test of the TSF data being part of the software application is included. During  
3076 this complete self-test, it is checked that the electronic system of the physical device,  
3077 and all firmware components of the TOE are in authentic condition. This complete self-  
3078 test can also be run at the request of the successfully authenticated Gateway Adminis-  
3079 trator via interface IF\_GW\_WAN or at the request of the successfully authenticated Ser-  
3080 vice Technician via interface IF\_GW\_SRV. At the request of the successfully authenti-  
3081 cated Consumer via interface IF\_GW\_CON, the TOE will only test the integrity of the  
3082 Smart Metering software application including the service layers (without the operating  
3083 system) and the completeness of the TSF data stored in the TOE's database. Addition-  
3084 ally, the TOE itself runs a complete self-test periodically at least once a month during  
3085 normal operation. The integrity of TSF data stored in the TOE's database is always  
3086 tested during read access of that part of TSF data (**FPT\_TST.1**). **FPT\_RPL.1** is fulfilled  
3087 by the use of the TLS protocol respectively the integration of transmission counters ac-  
3088 cording to [TR-03116-3, chap. 7.3], and through the enforcement of an appropriate time  
3089 slot of execution for successfully authenticated wake-up calls.

3090 If an integrity violation of the TOE's hardware or firmware is detected or if the deviation  
3091 between local system time of the TOE and the reliable external time source is too large,  
3092 further use of the TOE for the purpose of gathering Meter Data is not possible. Also in  
3093 this case, the TOE signals the incorrect status via a suitable signal output on the case

3094 of the device, and the further use of the TOE for the purpose of gathering Meter Data is  
 3095 not allowed (**FPT\_FLS.1**).

3096 Basically, if an integrity violation is detected, the TOE will create an entry in the System  
 3097 Log to document this status for the authorised Gateway Administrator on interface  
 3098 IF\_GW\_WAN resp. for the authorised Service Technician on interface IF\_GW\_SRV, and  
 3099 will inform the Gateway Administrator on this incident (**FAU\_ARP.1/SYS,**  
 3100 **FAU\_GEN.1/SYS, FAU\_SAR.1/SYS, FPT\_TST.1**).

3101 **7.7 TSS Rationale**

3102 The following table shows the correspondence analysis for the described TOE security  
 3103 functionalities and the security functional requirements.

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FAU_ARP.1/SYS					X	(X)
FAU_GEN.1/SYS					X	(X)
FAU_SAA.1/SYS					X	
FAU_SAR.1/SYS					X	(X)
FAU_STG.4/SYS					X	
FAU_GEN.1/CON					X	
FAU_SAR.1/CON					X	
FAU_STG.4/CON					X	
FAU_GEN.1/CAL					X	
FAU_SAR.1/CAL					X	
FAU_STG.4/CAL					X	
FAU_GEN.2					X	

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FAU_STG.2					X	
FCO_NRO.2		X		X		
FCS_CKM.1/TLS	X					
FCS_COP.1/TLS	X					
FCS_CKM.1/CMS		X				
FCS_COP.1/CMS		X				
FCS_CKM.1/MTR	X	X				
FCS_COP.1/MTR	X	X				
FCS_CKM.4	X	X				
FCS_COP.1/HASH		X				
FCS_COP.1/MEM		X				
FDP_ACC.2	X					
FDP_ACF.1	X					
FDP_IFC.2/FW	X					
FDP_IFF.1/FW	X					
FDP_IFC.2/MTR	X					
FDP_IFF.1/MTR	X					
FDP_RIP.2	X	X				
FDP_SDI.2		X			X	

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FIA_ATD.1	X					
FIA_AFL.1				X		
FIA_UAU.2	X					
FIA_UAU.5	X					
FIA_UAU.6	X					
FIA_UID.2	X					
FIA_USB.1	X			X		
FMT_MOF.1			X		X	
FMT_SMF.1			X			
FMT_SMR.1	X					
FMT_MSA.1/AC			X			
FMT_MSA.3/AC			X			
FMT_MSA.1/FW			X			
FMT_MSA.3/FW			X			
FMT_MSA.1/MTR			X			
FMT_MSA.3/MTR			X			
FPR_CON.1		X				
FPR_PSE.1		X				
FPT_FLS.1						X

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FPT_RPL.1	X	X				X
FPT_STM.1		X				
FPT_TST.1						X
FPT_PHP.1						X
FTP_ITC.1/WAN	X					
FTP_ITC.1/MTR	X					
FTP_ITC.1/USR	X			X		

3104 **Table 19: Rationale for the SFR and the TOE Security Functionalities** <sup>224</sup>

---

<sup>224</sup> Please note that SFRs marked with “(X)” only have supporting effect on the fulfilment of the TSF.

## 3105 8 List of Tables

3106	TABLE 1: SMART METER GATEWAY PRODUCT CLASSIFICATIONS.....	9
3107	TABLE 2: COMMUNICATION FLOWS BETWEEN DEVICES IN DIFFERENT NETWORKS .....	23
3108	TABLE 3: MANDATORY TOE EXTERNAL INTERFACES.....	28
3109	TABLE 4: CRYPTOGRAPHIC SUPPORT OF THE TOE AND ITS SECURITY MODULE .....	29
3110	TABLE 5: ROLES USED IN THE SECURITY TARGET .....	34
3111	TABLE 6: ASSETS (USER DATA).....	36
3112	TABLE 7: ASSETS (TSF DATA) .....	37
3113	TABLE 8: RATIONALE FOR SECURITY OBJECTIVES .....	53
3114	TABLE 9: LIST OF SECURITY FUNCTIONAL REQUIREMENTS .....	64
3115	TABLE 10: OVERVIEW OVER AUDIT PROCESSES .....	66
3116	TABLE 11: EVENTS FOR CONSUMER LOG .....	71
3117	TABLE 12: CONTENT OF CALIBRATION LOG .....	76
3118	TABLE 13: RESTRICTIONS ON MANAGEMENT FUNCTIONS.....	105
3119	TABLE 14: SFR RELATED MANAGEMENT FUNCTIONALITIES .....	110
3120	TABLE 15: GATEWAY SPECIFIC MANAGEMENT FUNCTIONALITIES .....	111
3121	TABLE 16: ASSURANCE REQUIREMENTS.....	122
3122	TABLE 17: FULFILMENT OF SECURITY OBJECTIVES .....	126
3123	TABLE 18: SFR DEPENDENCIES .....	136
3124	TABLE 19: RATIONALE FOR THE SFR AND THE TOE SECURITY FUNCTIONALITIES .....	155
3125		



3126 **9 List of Figures**

3127 FIGURE 1: THE TOE AND ITS DIRECT ENVIRONMENT ..... 12  
3128 FIGURE 2: THE LOGICAL INTERFACES OF THE TOE ..... 14  
3129 FIGURE 3: THE PRODUCT WITH ITS TOE AND NON-TOE PARTS ..... 16  
3130 FIGURE 4: THE TOE'S PROTOCOL STACK..... 18  
3131 FIGURE 5: CRYPTOGRAPHIC INFORMATION FLOW FOR DISTRIBUTED METERS AND GATEWAY  
3132 ..... 31  
3133

3134 **10 Appendix**3135 **10.1 Mapping from English to German terms**

English term	German term
billing-relevant	abrechnungsrelevant
CLS, Controllable Local System	dezentral steuerbare Verbraucher- oder Erzeugersysteme
Consumer	Anschlussnutzer; Letztverbraucher (im verbrauchenden Sinne); u.U. auch Einspeiser
Consumption Data	Verbrauchsdaten
Gateway	Kommunikationseinheit
Grid	Netz (für Strom/Gas/Wasser)
Grid Status Data	Zustandsdaten des Versorgungsnetzes
LAN, Local Area Network	Lokales Kommunikationsnetz
LMN, Local Metrological Network	Lokales Messeinrichtungsnetz
Meter	Messeinrichtung (Teil eines Messsystems)
Processing Profiles	Konfigurationsprofile
Security Module	Sicherheitsmodul (z.B. eine Smart Card)
Service Provider	Diensteanbieter
Smart Meter, Smart Metering System <sup>225</sup>	Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsystem)
TOE	EVG ( <b>E</b> valuierungs <b>g</b> egenstand)

---

<sup>225</sup> Please note that the terms "Smart Meter" and "Smart Metering System" are used synonymously within this document.

WAN, Wide Area Network	Weitverkehrsnetz (für Kommunikation)
------------------------	--------------------------------------

3136

3137 **10.2 Glossary**

Term	Description
Authenticity	property that an entity is what it claims to be (according to [SD_6])
Block Tariff	Tariff in which the charge is based on a series of different energy/volume rates applied to successive usage blocks of given size and supplied during a specified period. (according to [CEN])
BPL	<i>Broadband Over Power Lines</i> , a method of power line communication
CA	Certification Authority, an entity that issues digital certificates.  CLS config
CDMA	<i>Code Division Multiple Access</i>
CLS config (secondary asset)	See chapter 3.2
CMS	Cryptographic Message Syntax
Confidentiality	the property that information is not made available or disclosed to unauthorised individuals, entities, or processes (according to [SD_6])
Consumer	End user of electricity, gas, water or heat (according to [CEN]). See chapter 3.1
DCP	<i>Data Co-Processor</i> , security hardware of the CPU
DLMS	Device Language Message Specification
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level

Term	Description
Energy Service Provider	Organisation offering energy related services to the Consumer (according to [CEN])
ETH	Ethernet
external entity	See chapter 3.1
firmware update	See chapter 3.2
Gateway Administrator (GWA)	See chapter 3.1
Gateway config (secondary asset)	See chapter 3.2
Gateway time	See chapter 3.2
G.hn	Gigabit Home Networks
GPRS	<i>General Packet Radio Service</i> , a packet oriented mobile data service
Home Area Network (HAN)	In-house data communication network which interconnects domestic equipment and can be used for energy management purposes (adopted according to [CEN]).
Integrity	property that sensitive data has not been modified or deleted in an unauthorised and undetected manner (according to [SD_6])
IT-System	Computersystem
Local Area Network (LAN)	Data communication network, connecting a limited number of communication devices (Meters and other devices) and covering a moderately sized geographical area within the premises of the consumer. In the context of this ST, the term LAN is used as a hypernym for HAN and LMN (according to [CEN], adopted).

Term	Description
Local attacker	See chapter 3.4
LTE	<i>Long Term Evolution</i> mobile broadband communication standard
Meter config (secondary asset)	See chapter 3.2
Local Metrological Network (LMN)	In-house data communication network which interconnects metrological equipment.
Meter Data	See chapter 3.2
Meter Data Aggregator (MDA)	Entity which offers services to aggregate metering data by grid supply point on a contractual basis.  NOTE: The contract is with a supplier. The aggregate is of all that supplier's consumers connected to that particular grid supply point. The aggregate may include both metered data and data estimated by reference to standard load profiles (adopted from [CEN])
Meter Data Collector (MDC)	Entity which offers services on a contractual basis to collect metering data related to a supply and provide it in an agreed format to a data aggregator (that can also be the DNO).  NOTE: The contract is with a supplier or a pool. The collection may be carried out by manual or automatic means. ([CEN])
Meter Data Management System (MDMS)	System for validating, storing, processing and analysing large quantities of Meter Data. ([CEN])
Metrological Area Network	In-house data communication network which interconnects metrological equipment (i.e. Meters)
OEM	Original Equipment Manufacturer
OMS	Open Metering System

Term	Description
OCOTP	On-Chip One-time-programmable
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
RJ45	registered jack #45; a standardized physical network interface
RMII	Reduced Media Independent Interface
RTC	Real Time Clock
Service Technician	Human entity being responsible for diagnostic purposes.
Smart Metering System	The Smart Metering System consists of a Smart Meter Gateway and connected to one or more meters. In addition, CLS (i.e. generation plants) may be connected with the gateway for dedicated communication purposes.
SML	Smart Message Language
Tariff	Price structure (normally comprising a set of one or more rates of charge) applied to the consumption or production of a product or service provided to a Consumer (according to [CEN]).
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security protocol according to [RFC 5246]
TOE	Target of Evaluation - set of software, firmware and/or hardware possibly accompanied by guidance
TSF	TOE security functionality
UART	Universal Asynchronous Receiver Transmitter

Term	Description
WAN attacker	See chapter 3.4
WLAN	Wireless Local Area Network



## 3138 11 Literature

- 3139 [CC] Common Criteria for Information Technology Security  
3140 Evaluation –  
3141 Part 1: Introduction and general model, April 2017, ver-  
3142 sion 3.1, Revision 5, CCMB-2017-04-001,  
3143 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf)  
3144 [tal.org/files/ccfiles/CCPART1V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf)
- 3145 Part 2: Security functional requirements, April 2017, ver-  
3146 sion 3.1, Revision 5, CCMB-2017-04-002,  
3147 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf)  
3148 [tal.org/files/ccfiles/CCPART2V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf)
- 3149 Part 3: Security assurance requirements, April 2017, ver-  
3150 sion 3.1, Revision 5, CCMB-2017-04-003,  
3151 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf)  
3152 [tal.org/files/ccfiles/CCPART3V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf)
- 3153 [CEN] SMART METERS CO-ORDINATION GROUP (SM-CG)  
3154 Item 5. M/441 first phase deliverable – Communication –  
3155 Annex: Glossary (SMCG/Sec0022/DC)
- 3156 [PP\_GW] Protection Profile for the Gateway of a Smart Metering  
3157 System (Smart Meter Gateway PP), Schutzprofil für die  
3158 Kommunikationseinheit eines intelligenten Messsystems  
3159 für Stoff- und Energiemengen, SMGW-PP, v.1.3, Bundes-  
3160 amt für Sicherheit in der Informationstechnik, 31.03.2014
- 3161 [SecModPP] Protection Profile for the Security Module of a Smart Me-  
3162 ter Gateway (Security Module PP), Schutzprofil für das  
3163 Sicherheitsmodul der Kommunikationseinheit eines intelli-  
3164 genten Messsystems für Stoff- und Energiemengen,  
3165 SecMod-PP, Version 1.0.2, Bundesamt für Sicherheit in  
3166 der Informationstechnik, 18.10.2013
- 3167 [SD\_6] ISO/IEC JTC 1/SC 27 N7446, Standing Document 6  
3168 (SD6): Glossary of IT Security Terminology 2009-04-29,  
3169 available at

3170		<a href="http://www.teletrust.de/uploads/media/ISOIEC_JTC1_SC27_IT_Security_Glossary_TeleTrusT_Documentation.pdf">http://www.teletrust.de/uploads/me-</a>
3171		<a href="http://www.teletrust.de/uploads/media/ISOIEC_JTC1_SC27_IT_Security_Glossary_TeleTrusT_Documentation.pdf">dia/ISOIEC_JTC1_SC27_IT_Security_Glossary_Tele-</a>
3172		<a href="http://www.teletrust.de/uploads/media/ISOIEC_JTC1_SC27_IT_Security_Glossary_TeleTrusT_Documentation.pdf">TrusT_Documentation.pdf</a>
3173	[TR-02102]	Technische Richtlinie BSI TR-02102, Kryptographische
3174		Verfahren: Empfehlungen und Schlüssellängen, Bundes-
3175		amt für Sicherheit in der Informationstechnik, Version
3176		2022-01
3177	[TR-03109]	Technische Richtlinie BSI TR-03109, Version 1.1, Bun-
3178		desamt für Sicherheit in der Informationstechnik,
3179		22.09.2021
3180	[TR-03109-1]	Technische Richtlinie BSI TR-03109-1, Anforderungen an
3181		die Interoperabilität der Kommunikationseinheit eines
3182		Messsystems, Version 1.1, Bundesamt für Sicherheit in
3183		der Informationstechnik, 17.09.2021
3184	[TR-03109-1-I]	Technische Richtlinie BSI TR-03109-1 Anlage I, CMS-
3185		Datenformat für die Inhaltsdatenverschlüsselung und -
3186		signatur, Version 1.0.9, Bundesamt für Sicherheit in der
3187		Informationstechnik, 18.03.2013
3188	[TR-03109-1-VI]	Technische Richtlinie BSI TR-03109-1 Anlage VI, Be-
3189		triebsprozesse, Version 1.0, Bundesamt für Sicherheit in
3190		der Informationstechnik, 18.03.2013
3191	[TR-03109-2]	Technische Richtlinie BSI TR-03109-2, Smart Meter Ga-
3192		teway – Anforderungen an die Funktionalität und In-
3193		teroperabilität des Sicherheitsmoduls, Version 1.1, Bun-
3194		desamt für Sicherheit in der Informationstechnik,
3195		15.12.2014
3196	[TR-03109-3]	Technische Richtlinie BSI TR-03109-3, Kryptographische
3197		Vorgaben für die Infrastruktur von intelligenten Messsys-
3198		temen, Version 1.1, Bundesamt für Sicherheit in der Infor-
3199		mationstechnik, 17.04.2014
3200	[TR-03109-4]	Technische Richtlinie BSI TR-03109-4, Smart Metering
3201		PKI - Public Key Infrastruktur für Smart Meter Gateways,

3202		Version 1.2.1, Bundesamt für Sicherheit in der Informationstechnik, 09.08.2017
3203		
3204	[TR-03109-6]	Technische Richtlinie BSI TR-03109-6, Smart Meter Gateway Administration, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, 26.11.2015
3205		
3206		
3207	[TR-03111]	Technische Richtlinie BSI TR-03111, Elliptic Curve Cryptography (ECC), Version 2.1, 01.06.2018
3208		
3209	[TR-03116-3]	Technische Richtlinie BSI TR-03116-3, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3 - Intelligente Messsysteme, Stand 2023, Bundesamt für Sicherheit in der Informationstechnik, 06.12.2022
3210		
3211		
3212		
3213	[AGD_Consumer]	Handbuch für Verbraucher, Smart Meter Gateway, Version 4.11, 02.06.2023, Power Plus Communications AG
3214		
3215	[AGD_Techniker]	Handbuch für Service-Techniker, Smart Meter Gateway, Version 5.9, 06.06.2024, Power Plus Communications AG
3216		
3217		
3218	[AGD_GWA]	Handbuch für Hersteller von Smart-Meter Gateway-Administrations-Software, Smart Meter Gateway, Version 4.13, 01.09.2023, Power Plus Communications AG
3219		
3220		
3221	[AGD_SEC]	Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung, Version 1.13, 08.07.2024, Power Plus Communications AG
3222		
3223		
3224	[SMGW_Logging]	Logmeldungen, SMGW Version 1.3 & 2.1 & 2.1.1, Version 3.4, 11.05.2023, Power Plus Communications AG
3225		
3226	[FIPS Pub. 140-2]	NIST, FIPS 140-3, Security Requirements for cryptographic modules, 2019
3227		
3228	[FIPS Pub. 180-4]	NIST, FIPS 180-4, Secure Hash Standard, 2015
3229	[FIPS Pub. 197]	NIST, FIPS 197, Advances Encryption Standard (AES), 2001
3230		
3231	[IEEE 1901]	IEEE Std 1901-2010, IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications, 2010
3232		
3233		

3234	[IEEE 802.3]	IEEE Std 802.3-2008, IEEE Standard for Information
3235		technology, Telecommunications and information ex-
3236		change between systems, Local and metropolitan area
3237		networks, Specific requirements, 2008
3238	[ISO 10116]	ISO/IEC 10116:2006, Information technology -- Security
3239		techniques -- Modes of operation for an n-bit block cipher,
3240		2006
3241	[NIST 800-38A]	NIST Special Publication 800-38A, Recommendation for
3242		Block Cipher Modes of Operation: Methods and Tech-
3243		niques, December 2001, <a href="http://nvl-pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf">http://nvl-</a>
3244		<a href="http://nvl-pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf">pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublica-</a>
3245		<a href="http://nvl-pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf">tion800-38a.pdf</a>
3246	[NIST 800-38D]	NIST Special Publication 800-38D, Recommendation for
3247		Block Cipher Modes of Operation: Galois/Counter Mode
3248		(GCM) and GMAC, M. Dworkin, November 2007,
3249		<a href="http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf">http://csrc.nist.gov/publications/nistpubs/800-38D/SP-</a>
3250		<a href="http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf">800-38D.pdf</a>
3251	[NIST 800-38E]	NIST Special Publication 800-38E, Recommendation for
3252		Block Cipher Modes of Operation: The XTS-AES Mode
3253		for Confidentiality on Storage Devices, M. Dworkin, Janu-
3254		ary, 2010, <a href="http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf">http://csrc.nist.gov/publications/nistpubs/800-</a>
3255		<a href="http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf">38E/nist-sp-800-38E.pdf</a>
3256	[RFC 2104]	RFC 2104, HMAC: Keyed-Hashing for Message Authenti-
3257		cation, M. Bellare, R. Canetti und H. Krawczyk, February
3258		1997, <a href="http://rfc-editor.org/rfc/rfc2104.txt">http://rfc-editor.org/rfc/rfc2104.txt</a>
3259	[RFC 2616]	RFC 2616, Hypertext Transfer Protocol - HTTP/1.1, R.
3260		Fielding, J. Gettys, J. Mogul, H. Frystyk, P. Masinter, P.
3261		Leach, T. Berners-Lee, June 1999, <a href="http://rfc-editor.org/rfc/rfc2616.txt">http://rfc-edi-</a>
3262		<a href="http://rfc-editor.org/rfc/rfc2616.txt">tor.org/rfc/rfc2616.txt</a>
3263	[RFC 7616]	RFC 7616, HTTP Digest Access Authentication, R.
3264		Shekh-Yusef, D. Ahrens, S. Bremer, September 2015,
3265		<a href="http://rfc-editor.org/rfc/rfc7616.txt">http://rfc-editor.org/rfc/rfc7616.txt</a>

3266	[RFC 3394]	RFC 3394, Schaad, J. and R. Housley, Advanced Encryption Standard (AES) Key Wrap Algorithm, September 2002, <a href="http://rfc-editor.org/rfc/rfc3394.txt">http://rfc-editor.org/rfc/rfc3394.txt</a>
3267		
3268		
3269	[RFC 3565]	RFC 3565, J. Schaad, Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS), July 2003, <a href="http://rfc-editor.org/rfc/rfc3565.txt">http://rfc-editor.org/rfc/rfc3565.txt</a>
3270		
3271		
3272		
3273	[RFC 4493]	IETF RFC 4493, The AES-CMAC Algorithm, J. H. Song, J. Lee, T. Iwata, June 2006, <a href="http://www.rfc-editor.org/rfc/rfc4493.txt">http://www.rfc-editor.org/rfc/rfc4493.txt</a>
3274		
3275		
3276	[RFC 5083]	RFC 5083, R. Housley, Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type, November 2007, <a href="http://www.ietf.org/rfc/rfc5083.txt">http://www.ietf.org/rfc/rfc5083.txt</a>
3277		
3278		
3279		
3280	[RFC 5084]	RFC 5084, R. Housley, Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), November 2007, <a href="http://www.ietf.org/rfc/rfc5084.txt">http://www.ietf.org/rfc/rfc5084.txt</a>
3281		
3282		
3283		
3284	[RFC 5114]	RFC 5114, Additional Diffie-Hellman Groups for Use with IETF Standards, M. Lepinski, S. Kent, January 2008, <a href="http://www.ietf.org/rfc/rfc5114.txt">http://www.ietf.org/rfc/rfc5114.txt</a>
3285		
3286		
3287	[RFC 5246]	RFC 5246, T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008, <a href="http://www.ietf.org/rfc/rfc5246.txt">http://www.ietf.org/rfc/rfc5246.txt</a>
3288		
3289		
3290	[RFC 5289]	RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), E. Rescorla, RTFM, Inc., August 2008, <a href="http://www.ietf.org/rfc/rfc5289.txt">http://www.ietf.org/rfc/rfc5289.txt</a>
3291		
3292		
3293		
3294	[RFC 5639]	RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter, BSI, J. Merkle, secunet Security Networks, March 2010, <a href="http://www.ietf.org/rfc/rfc5639.txt">http://www.ietf.org/rfc/rfc5639.txt</a>
3295		
3296		
3297		

3298	[RFC 5652]	RFC 5652, Cryptographic Message Syntax (CMS), R.
3299		Housley, Vigil Security, September 2009,
3300		<a href="http://www.ietf.org/rfc/rfc5652.txt">http://www.ietf.org/rfc/rfc5652.txt</a>
3301	[EIA RS-485]	EIA Standard RS-485, Electrical Characteristics of Gener-
3302		ators and Receivers for Use in Balanced Multipoint Sys-
3303		tems, ANSI/TIA/EIA-485-A-98, 1983/R2003
3304	[EN 13757-1]	M-Bus DIN EN 13757-1: Kommunikationssysteme für
3305		Zähler und deren Fernablesung Teil 1: Datenaustausch
3306	[EN 13757-3]	M-Bus DIN EN 13757-3, Kommunikationssysteme für
3307		Zähler und deren Fernablesung Teil 3: Spezielle Anwen-
3308		dungsschicht
3309	[EN 13757-4]	M-Bus DIN EN 13757-4, Kommunikationssysteme für
3310		Zähler und deren Fernablesung Teil 4: Zählerauslesung
3311		über Funk, Fernablesung von Zählern im SRD-Band von
3312		868 MHz bis 870 MHz
3313	[IEC-62056-5-3-8]	Electricity metering – Data exchange for meter reading,
3314		tariff and load control – Part 5-3-8: Smart Message Lan-
3315		guage SML, 2012
3316	[IEC-62056-6-1]	IEC-62056-6-1, Datenkommunikation der elektrischen
3317		Energiemessung, Teil 6-1: OBIS Object Identification Sys-
3318		tem, 2017, International Electrotechnical Commission
3319	[IEC-62056-6-2]	IEC-62056-6-2, Datenkommunikation der elektrischen
3320		Energiemessung - DLMS/COSEM, Teil 6-2: COSEM Inter-
3321		face classes, 2017, International Electrotechnical Commis-
3322		sion
3323	[IEC-62056-21]	IEC-62056-21, Direct local data exchange - Mode C, 2011,
3324		International Electrotechnical Commission
3325	[LUKS]	LUKS On-Disk Format Specification Version 1.2.1, Clem-
3326		ens Fruhwirth, October 16th, 2011
3327	[PACE]	The PACE-AA Protocol for Machine Readable Travel Doc-
3328		uments, and its Security, Jens Bender, Ozgur Dagdelen,

3329		Marc Fischlin and Dennis Kügler, <a href="http://fc12.ifca.ai/pre-proceedings/paper_49.pdf">http://fc12.ifca.ai/pre-proceedings/paper_49.pdf</a>
3330		
3331	[X9.63]	ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011
3332		
3333		
3334	[G865]	DVGW-Arbeitsblatt G865 Gasabrechnung, 11/2008
3335	[VDE4400]	VDE-AR-N 4400:2011-09, Messwesen Strom, VDE-Anwendungsregel, 01.09.2011
3336		
3337	[DIN 43863-5]	DIN: Herstellerübergreifende Identifikationsnummer für Messeinrichtungen, 2012
3338		
3339	[USB]	Universal Serial Bus Specification, Revision 2.0, April 27, 2000, USB Communications CLASS Specification for Ethernet Devices, <a href="http://www.usb.org/developers/docs/usb20_docs/#usb20spec">http://www.usb.org/developers/docs/usb20_docs/#usb20spec</a>
3340		
3341		
3342		
3343	[ITU G.hn]	G.996x Unified high-speed wireline-based home networking transceivers, 2018
3344		



**Power Plus Communications AG**

Dudenstraße 6, 68167 Mannheim

Tel. 00 49 621 40165 100 | Fax. 00 49 621 40165 111

info@ppc-ag.de | www.ppc-ag.de