



# Security Target

## SMGW Version 2.2.1

## 1 Version History

Version	Datum	Änderungen
1.8	30.10.2025	SMGW 2.2.1

## 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.....	10
8	1.4 TOE Overview .....	12
9	1.4.1 Introduction .....	12
10	1.4.2 Overview of the Gateway in a Smart Metering System .....	13
11	1.4.3 TOE description.....	16
12	1.4.4 TOE Type definition .....	17
13	1.4.5 TOE logical boundary .....	20
14	1.4.6 The logical interfaces of the TOE .....	28
15	1.4.7 The cryptography of the TOE and its Security Module .....	29
16	TOE life-cycle .....	33
17	<b>2 Conformance Claims .....</b>	<b>34</b>
18	2.1 CC Conformance Claim .....	34
19	2.2 PP Claim / Conformance Statement .....	34
20	2.3 Package Claim .....	34
21	2.4 Conformance Claim Rationale .....	34
22	<b>3 Security Problem Definition.....</b>	<b>36</b>
23	3.1 External entities .....	36
24	3.2 Assets.....	36
25	3.3 Assumptions .....	40
26	3.4 Threats.....	42
27	3.5 Organizational Security Policies.....	46
28	<b>4 Security Objectives .....</b>	<b>48</b>
29	4.1 Security Objectives for the TOE .....	48
30	4.2 Security Objectives for the Operational Environment.....	53
31	4.3 Security Objective Rationale.....	55
32	4.3.1 Overview .....	55
33	4.3.2 Countering the threats.....	57
34	4.3.3 Coverage of organisational security policies .....	60
35	4.3.4 Coverage of assumptions .....	60
36	<b>5 Extended Component definition .....</b>	<b>62</b>
37	5.1 Communication concealing (FPR_CON) .....	62
38	5.2 Family behaviour .....	62
39	5.3 Component levelling.....	62
40	5.4 Management.....	62
41	5.5 Audit .....	62
42	5.6 Communication concealing (FPR_CON.1) .....	62
43	<b>6 Security Requirements.....</b>	<b>64</b>
44	6.1 Overview.....	64

45	<b>6.2 Class FAU: Security Audit.....</b>	<b>68</b>
46	6.2.1 Introduction .....	68
47	6.2.2 Security Requirements for the System Log .....	70
48	6.2.3 Security Requirements for the Consumer Log .....	73
49	6.2.4 Security Requirements for the Calibration Log .....	76
50	6.2.5 Security Requirements that apply to all logs .....	81
51	<b>6.3 Class FCO: Communication.....</b>	<b>83</b>
52	6.3.1 Non-repudiation of origin (FCO_NRO).....	83
53	<b>6.4 Class FCS: Cryptographic Support .....</b>	<b>84</b>
54	6.4.1 Cryptographic support for TLS.....	84
55	6.4.2 Cryptographic support for CMS .....	85
56	6.4.3 Cryptographic support for Meter communication encryption .....	87
57	6.4.4 General Cryptographic support.....	89
58	<b>6.5 Class FDP: User Data Protection.....</b>	<b>92</b>
59	6.5.1 Introduction to the Security Functional Policies .....	92
60	6.5.2 Gateway Access SFP .....	92
61	6.5.3 Firewall SFP .....	94
62	6.5.4 Meter SFP.....	97
63	6.5.5 General Requirements on user data protection.....	101
64	<b>6.6 Class FIA: Identification and Authentication .....</b>	<b>102</b>
65	6.6.1 User Attribute Definition (FIA_ATD).....	102
66	6.6.2 Authentication Failures (FIA_AFL).....	103
67	6.6.3 User Authentication (FIA_UAU) .....	103
68	6.6.4 User identification (FIA_UID) .....	105
69	6.6.5 User-subject binding (FIA_USB).....	106
70	<b>6.7 Class FMT: Security Management .....</b>	<b>107</b>
71	6.7.1 Management of the TSF.....	107
72	6.7.2 Security management roles (FMT_SMR) .....	114
73	6.7.3 Management of security attributes for Gateway access SFP.....	115
74	6.7.4 Management of security attributes for Firewall SFP .....	116
75	6.7.5 Management of security attributes for Meter SFP .....	117
76	<b>6.8 Class FPR: Privacy .....</b>	<b>118</b>
77	6.8.1 Communication Concealing (FPR_CON).....	118
78	6.8.2 Pseudonymity (FPR_PSE).....	119
79	<b>6.9 Class FPT: Protection of the TSF .....</b>	<b>120</b>
80	6.9.1 Fail secure (FPT_FLS).....	120
81	6.9.2 Replay Detection (FPT_RPL).....	121
82	6.9.3 Time stamps (FPT_STM) .....	121
83	6.9.4 TSF self test (FPT_TST).....	121
84	6.9.5 TSF physical protection (FPT_PHP).....	122
85	<b>6.10 Class FTP: Trusted path/channels.....</b>	<b>122</b>
86	6.10.1 Inter-TSF trusted channel (FTP_ITC).....	122

87      **6.11 Security Assurance Requirements for the TOE..... 124**

88          6.11.1 Refinement for ALC\_DEL.1 for the following assurance elements ..... 126

89      **6.12 Security Requirements rationale ..... 126**

90          6.12.1 Security Functional Requirements rationale..... 126

91          6.12.2 Security Assurance Requirements rationale ..... 139

92      **7 TOE Summary Specification..... 140**

93          7.1 SF.1: Authentication of Communication and Role Assignment for external

94          entities..... 140

95          7.2 SF.2: Acceptance and Deposition of Meter Data, Encryption of Meter Data for

96          WAN transmission..... 147

97          7.3 SF.3: Administration, Configuration and SW Update ..... 149

98          7.4 SF.4: Displaying Consumption Data..... 151

99          7.5 SF.5: Audit and Logging..... 152

100          7.6 SF.6: TOE Integrity Protection ..... 154

101          7.7 TSS Rationale..... 155

102      **8 List of Tables..... 159**

103      **9 List of Figures ..... 160**

104      **10 Appendix ..... 161**

105          10.1 Mapping from English to German terms ..... 161

106          10.2 Glossary ..... 163

107      **11 Literature ..... 168**

108

# 109 1 Introduction

## 110 1.1 ST reference

111	Title:	Security Target, SMGW Version 2.2.1
112	Editors:	Power Plus Communications AG
113	CC-Version:	3.1 Revision 5
114	Assurance Level:	EAL 4+, augmented by AVA_VAN.5 and ALC_FLR.2
115	General Status:	Final
116	Document Version:	1.8
117	Document Date:	30.10.2025
118	TOE:	SMGW Version 2.2.1
119	Certification ID:	BSI-DSZ-CC-0831-V10-2024

120 This document contains the security target of the *SMGW Version 2.2.1*.

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

123

## 124 1.2 TOE reference

125 The TOE described in this security target is the *SMGW Version 2.2.1*.

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

- 127 • *BPL Smart Meter Gateway* (BPL-SMGW), SMGW-B-2A-111-00, SMGW-B-2B-  
128 111-00, SMGW-H-2B-111-00
- 129 • *ETH Smart Meter Gateway* (ETH-SMGW), SMGW-E-2A-111-00, SMGW-E-2B-  
130 111-00
- 131 • *LTE Smart Meter Gateway* (LTE-SMGW), SMGW-J-2A-111-10, SMGW-J-2A-  
132 111-30, SMGW-K-2A-111-10, SMGW-K-2A-111-30, SMGW-J-2B-111-10,  
133 SMGW-J-2B-111-30, SMGW-K-2B-111-10, SMGW-K-2B-111-20, SMGW-K-

- 134 2B-111-30, SMGW-D-2B-111-10, SMGW-D-2B-111-20, SMGW-D-2B-111-30,  
 135 SMGW-O-2B-111-10, SMGW-O-2B-111-20 oder SMGW-O-2B-111-30
- 136 • G.hn Smart Meter Gateway (G.hn-SMGW), SMGW-N-2A-111-00, SMGW-N-  
 137 2B-111-00
  - 138 • LTE450 Smart Meter Gateway (LTE450-SMGW), SMGW-V-2A-111-20,  
 139 SMGW-V-2B-111-20
  - 140 • *pWE Smart Meter Gateway* (pWE-SMGW), SMGW-P-2A-111-00, SMGW-P-  
 141 2B-111-00

142 The TOE comprises the following parts:

- 143 • hardware device of the hardware generation 2A or 2B according to Table 1,  
 144 including the TOE's main circuit board, a carrier board, a power-supply unit and  
 145 a radio module for communication with wireless meter (included in the hardware  
 146 device "*Smart Meter Gateway*")
- 147 • firmware including software application (loaded into the circuit board)
  - 148 ○ "*SMGW Software Version 2.2.3*", identified by the value 00950-34900  
 149 which comprises of two revision numbers of the underlying version control sys-  
 150 tem for the TOE, where the first part is for the operating system and the second  
 151 part is for the SMGW application
  - 152 • manuals
    - 153 ○ „Handbuch für Verbraucher, Smart Meter Gateway“ [AGD\_CON-  
 154 SUMER], identified by the SHA-256 hash value  
 155 c98c8697b851c3622a4eb4a0692ea98048e0455a5a38f27984c73e9b32fa3ef0
    - 156 ○ „Handbuch für Service-Techniker, Smart Meter Gateway“ [AGD\_Techni-  
 157 ker], identified by the SHA-256 hash value  
 158 53074ebd01b733a3218dd8923f34c74995ac9908ace2f6c2472889e92c844703
    - 159 ○ „Handbuch für Hersteller von Smart-Meter Gateway-Administrations-  
 160 Software, Smart Meter Gateway“ [AGD\_GWA], identified by the SHA-  
 161 256 hash value  
 162 ceb48353011c7511b9e00dc3a3b88ef3d2036a048912cc8ab46680635c39d8ff
    - 163 ○ „Logmeldungen, SMGW “ [SMGW\_Logging] identified by the SHA-256  
 164 hash value  
 165 132352ca781817706b5a83490f92b92f4e5ff9327c6533b49637efb0085a7e25

- 166 ○ „Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Ausliefe-
- 167 rung“ [AGD\_SEC], identified by the SHA-256 hash value
- 168 88ec18e33637440cca7f93456789b33819c3dc4fcd46a2c711e50e235756aa8

169 The hardware device “*Smart Meter Gateway*” includes a secure module with the product  
 170 name “*TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE*” which  
 171 is not part of the TOE but has its own certification id “BSI-DSZ-CC-0957-V2-2016” or the  
 172 security module with the product name “*TCOS eEnergy Security Module Version 2.0*  
 173 *Release 1/P71*” which is not part of the TOE but has its own certification id “BSI-DSZ-  
 174 CC-1217-2024”. Moreover, a hard-wired communication adapter is connected to the  
 175 TOE via [USB] as shown in Figure 3 which is not part of the TOE (but always an insepa-  
 176 rable part of the delivered entity). This communication adapter can be either a LTE  
 177 communication adapter, a LTE450 communication adapter, a BPL [IEEE 1901] commu-  
 178 nication adapter, a GPRS communication adapter, a CDMA communication adapter, a  
 179 powerWAN-Ethernet communication adapter, a G.hn [ITU G.hn] communication adapter  
 180 or an ethernet communication adapter. There might be not every communication adapter  
 181 available for each Hardware Generation.

182 The following table shows the different “*Smart Meter Gateway*” product classifications  
 183 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“
		H	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”

#	Characteristic	Value	Description
		K	Product Type „LTE Smart Meter Gateway“
		D	Product Type „LTE Smart Meter Gateway“
		O	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)
		2A	Identification of hardware generation; version 2.0 of “SMGW Hardware”
		2B	Identification of hardware generation; version 2B 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>

#	Characteristic	Value	Description
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	

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

185 **1.3 Introduction**

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

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

198 In the past, the production of electricity followed the demand/consumption of the con-  
 199 sumers. Considering the strong increase in renewable energy and the production of en-  
 200 ergy as a side effect in heat generation today, the consumption/demand has to follow  
 201 the – often externally controlled – production of energy. Similar mechanisms can exist

---

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

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

202 for the gas network to control the feed of biogas or hydrogen based on information sub-  
203 mitted by consumer devices.

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

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

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

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

- 218 • protection of confidentiality, authenticity, integrity of data and
- 219 • information flow control

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

223

---

<sup>3</sup> 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.

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

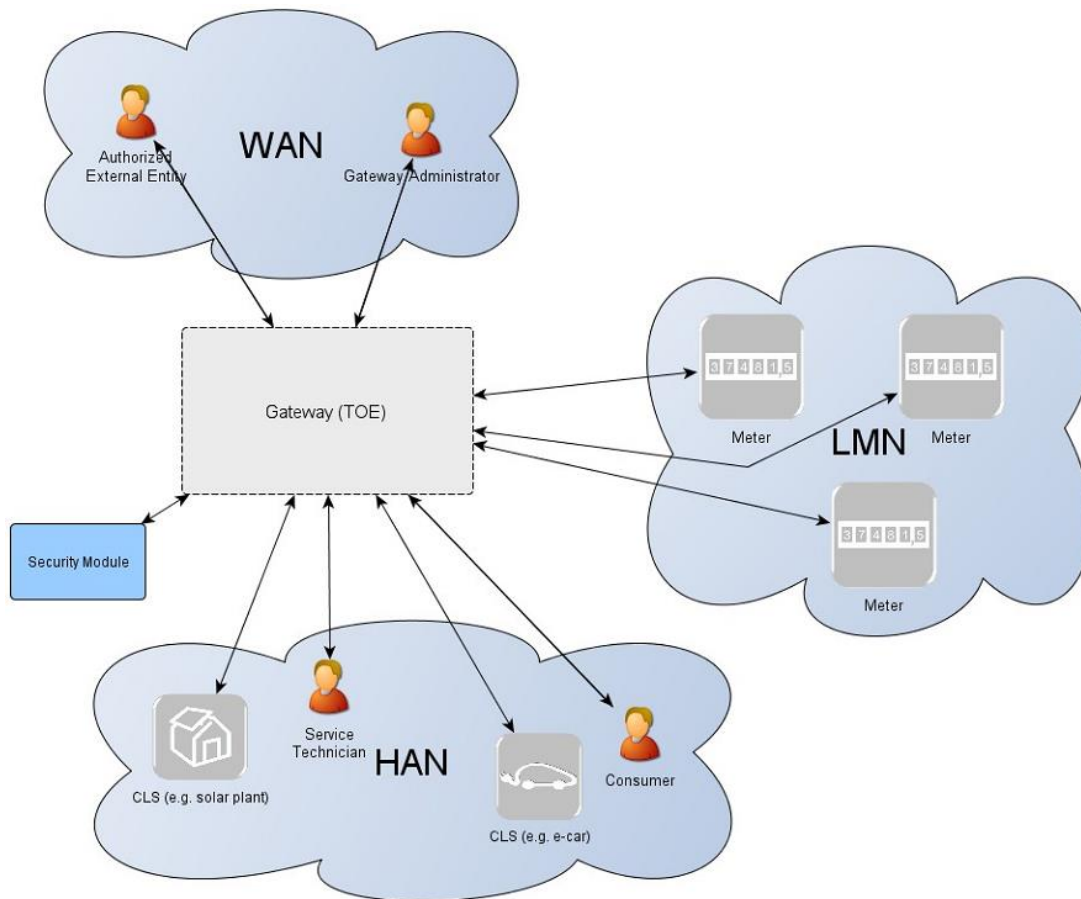
## 224 **1.4 TOE Overview**

### 225 **1.4.1 Introduction**

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

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

234 **1.4.2 Overview of the Gateway in a Smart Metering System**  
 235 The following figure provides an overview of the TOE as part of a complete Smart Me-  
 236 tering System from a purely functional perspective as used in this ST.<sup>5</sup>



237  
 238 **Figure 1: The TOE and its direct environment**

239  
 240 As can be seen in Figure 1, a system for smart metering comprises different functional  
 241 units in the context of the descriptions in this ST:

- 242 • The **Gateway** (as defined in this ST) serves as the communication component  
 243 between the components in the local area network (LAN) of the consumer and  
 244 the outside world. It can be seen as a special kind of firewall dedicated to the  
 245 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.

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

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

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

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

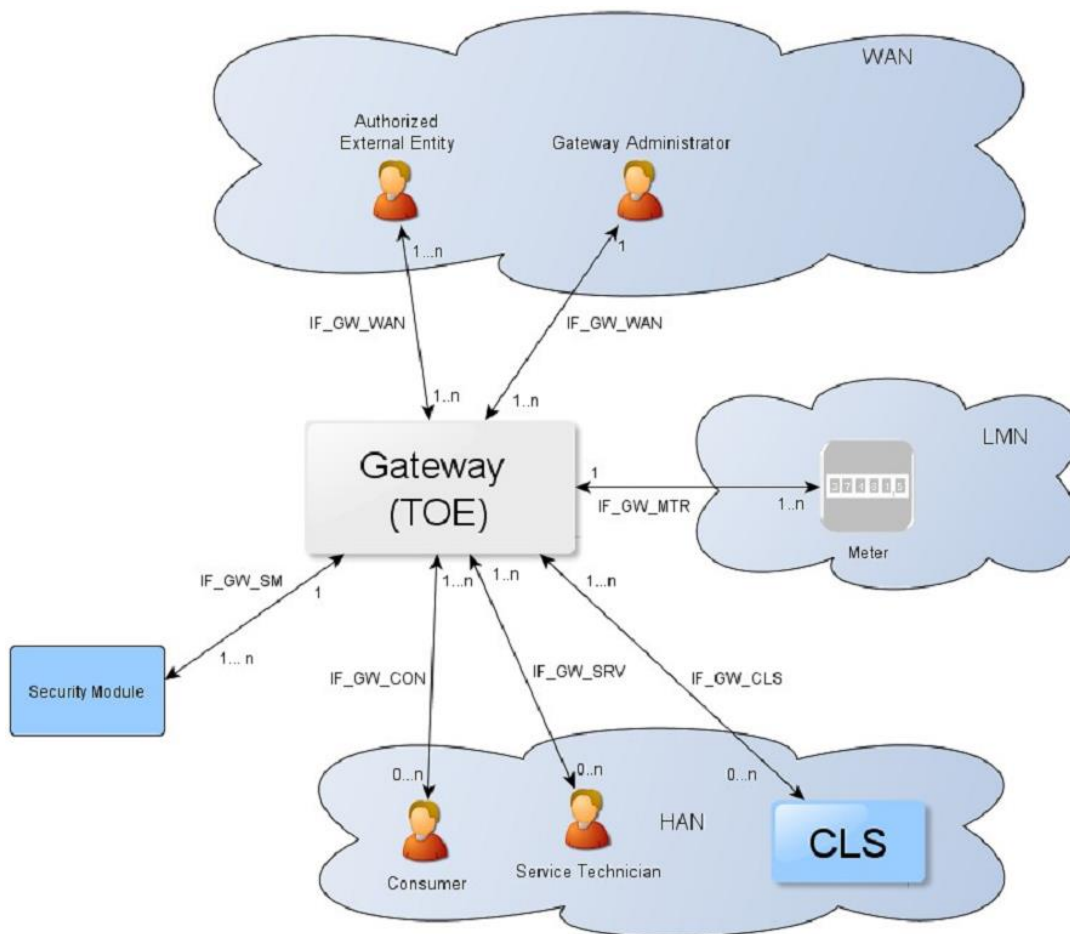
---

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.

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



274  
 275 **Figure 2: The logical interfaces of the TOE**

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

- 279 • The Gateway is the central communication unit in the Smart Metering System.  
 280 It is the only unit directly connected to the WAN, to be the first line of defence  
 281 an attacker located in the WAN would have to conquer.
- 282 • The Gateway is the central component that collects, processes and stores Me-  
 283 ter Data. It therewith is the primary point for user interaction in the context of  
 284 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.

- 285
- 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.
- 286
- 287
- 288
- 289
- 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.
- 290
- 291
- 292
- 293

294 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.

295

296

297

### 298 **1.4.3 TOE description**

299 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.

300

301

302

303

304 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).

305

306

307

308

309 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>.

310

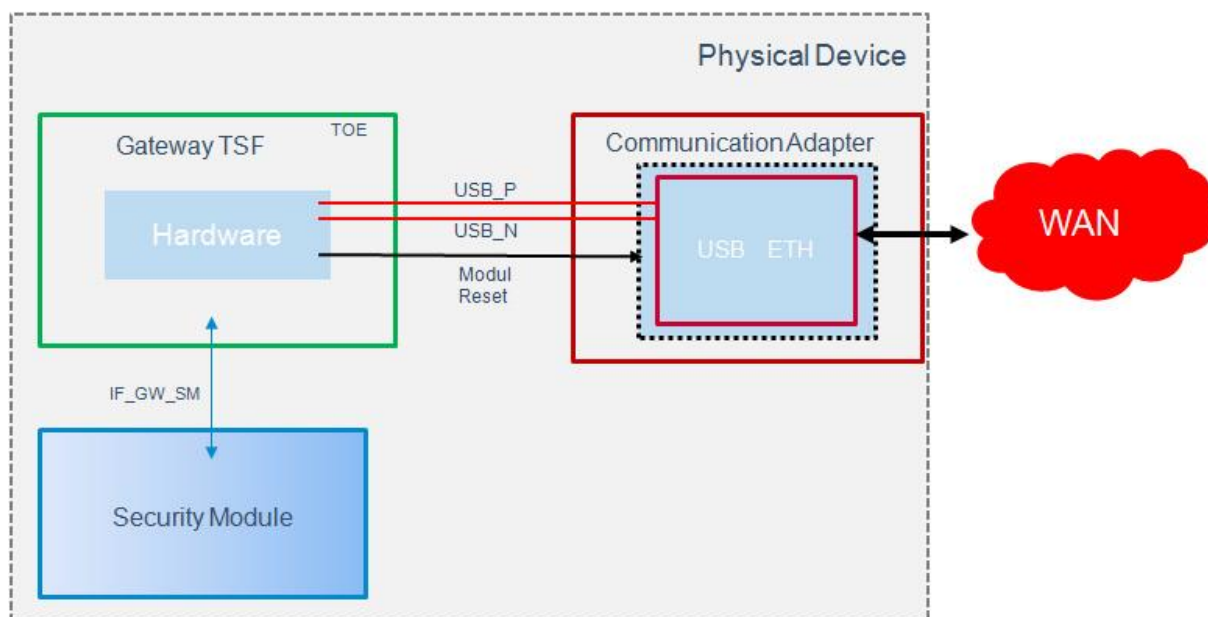
311

---

<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.

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



313  
314 **Figure 3: The product with its TOE and non-TOE parts**

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

#### 319 **1.4.4 TOE Type definition**

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

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

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

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

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

340 The TOE-design includes the following components:

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

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

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

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

350 The TOE supports the following communication protocols:

- 351 • OBIS according to [IEC-62056-6-1] and [EN 13757-1],
- 352 • DLMS/COSEM according to [IEC-62056-6-2],
- 353 • SML according to [IEC-62056-5-3-8],
- 354 • unidirectional and bidirectional wireless M-Bus according to [EN 13757-3],  
355 [EN 13757-4], and [IEC-62056-21].

356

---

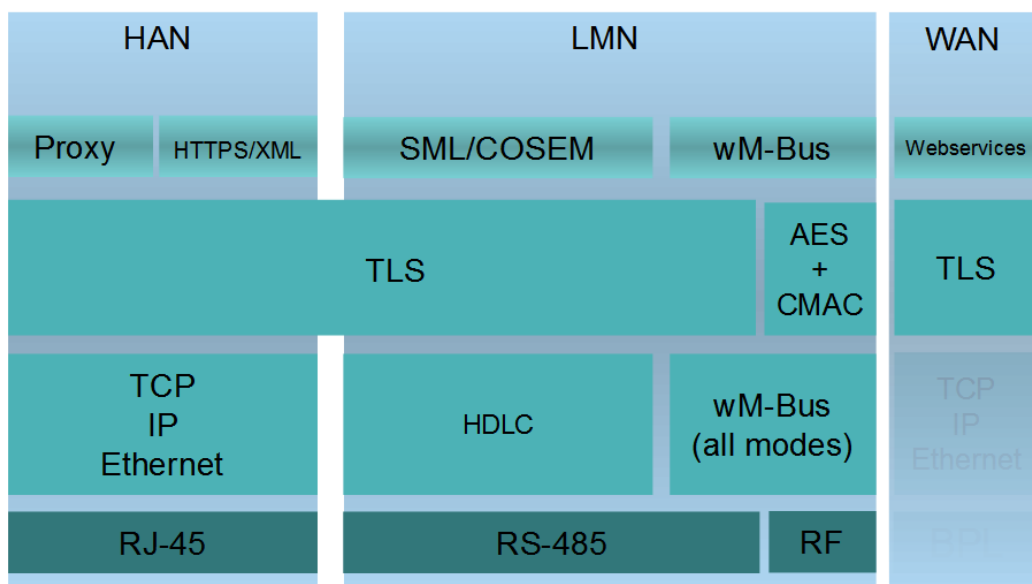
<sup>12</sup> Please note that the Security Module is physically integrated into the Gateway even though it is not part of the TOE.

357 The TOE provides the following physical interfaces for communication

- 358 • Wireless M-Bus (LMN) according to [EN 13757-3],
- 359 • RS-485 (LMN) according to [EIA RS-485],
- 360 • Ethernet (HAN) according to [IEEE 802.3], and
- 361 • USB (WAN) according to [USB].

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

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



366

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

368 The TOE provides the following functionality:

- 369 • Protected handling of Meter Data compliant to [PP\_GW, chapter 1.4.6.1 and  
 370 1.4.6.2]
- 371 • Integrity and authenticity protection e. g. of Meter Data compliant to [PP\_GW,  
 372 chapter 1.6.4.3]
- 373 • Protection of LAN devices against access from the WAN compliant to [PP\_GW,  
 374 chapter 1.4.6.4]
- 375 • Wake-Up Service compliant to [PP\_GW, chapter 1.4.6.5]
- 376 • Privacy protection compliant to [PP\_GW, chapter 1.4.6.6]
- 377 • Management of Security Functions compliant to [PP\_GW, chapter 1.4.6.7]

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

#### 380       **1.4.5 TOE logical boundary**

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

- 382           • *Handling of Meter Data*, collection and processing of Meter Data, submission  
383           to authorised external entities (e.g. one of the service providers involved) where  
384           necessary protected by a digital signature
- 385           • *Protection of authenticity, integrity and confidentiality* of data temporarily or per-  
386           sistently stored in the Gateway, transferred locally within the LAN and trans-  
387           ferred in the WAN (between Gateway and authorised external entities)
- 388           • *Firewalling* of information flows to the WAN and information flow control among  
389           Meters, Controllable Local Systems and the WAN
- 390           • *A Wake-Up-Service* that allows to contact the TOE from the WAN side
- 391           • *Privacy preservation*
- 392           • *Management of Security Functionality*
- 393           • *Identification and Authentication* of TOE users

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

##### 395       1.4.5.1 Handling of Meter Data<sup>13</sup>

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

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

- 400           • how Meter Data must be processed,
- 401           • which processed Meter Data must be sent in which intervals,
- 402           • to which component or external entity,
- 403           • signed using which key material,
- 404           • encrypted using which key material,
- 405           • whether processed Meter Data shall be pseudonymised or not, and
- 406           • 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.

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

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

- 411 • consumers must be identified and authenticated first before access to any data  
412 may be granted,
- 413 • the Gateway accepts Meter Data from authorised Meters only,
- 414 • the Gateway sends processed Meter Data to correspondingly authorised external  
415 entities only.

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

421 These functionalities:

- 422 • prevent that the Gateway accepts data from or sends data to unauthorised en-  
423 tities,
- 424 • ensure that only the minimum amount of data leaves the scope of control of the  
425 consumer,
- 426 • preserve the integrity of billing processes and as such serve in the interests of  
427 the consumer as well as in the interests of the supplier. Both parties are inter-  
428 ested in an billing process that ensures that the value of the consumed amount  
429 of a certain commodity (and only the used amount) is transmitted,
- 430 • preserve the integrity of the system components and their configurations.

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

439 1.4.5.2 Confidentiality protection

440 The TOE protects data from unauthorised disclosure

- 441 • while received from a Meter via the LMN,
- 442 • while received from the administrator via the WAN,
- 443 • while temporarily stored in the volatile memory of the Gateway,
- 444 • while transmitted to the corresponding external entity via the WAN or HAN.

445 Furthermore, all data, which no longer have to be stored in the Gateway, are securely  
446 erased to prevent any form of access to residual data via external interfaces of the TOE.

447 These functionalities protect the privacy of the consumer and prevent that an unauthor-  
448 ised party is able to disclose any of the data transferred in and from the Smart Metering  
449 System (e.g. Meter Data, configuration settings).

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

451 1.4.5.3 Integrity and Authenticity protection

452 The Gateway provides the following authenticity and integrity protection:

- 453 • Verification of authenticity and integrity when receiving Meter Data from a Meter  
454 via the LMN, to verify that the Meter Data have been sent from an authentic  
455 Meter and have not been altered during transmission. The TOE utilises the ser-  
456 vices of its Security Module for aspects of this functionality.
- 457 • Application of authenticity and integrity protection measures when sending pro-  
458 cessed Meter Data to an external entity, to enable the external entity to verify  
459 that the processed Meter Data have been sent from an authentic Gateway and  
460 have not been changed during transmission. The TOE utilises the services of  
461 its Security Module for aspects of this functionality.
- 462 • Verification of authenticity and integrity when receiving data from an external  
463 entity (e.g. configuration settings or firmware updates) to verify that the data  
464 have been sent from an authentic and authorised external entity and have not  
465 been changed during transmission. The TOE utilises the services of its Security  
466 Module for aspects of this functionality.

467 These functionalities

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

- 471           • facilitate the integrity of billing processes and serve for the interests of the con-  
472           sumer as well as for the interest of the supplier. Both parties are interested in  
473           the transmission of correct processed Meter Data to be used for billing,  
474           • protect the Smart Metering System and a corresponding large scale Smart Grid  
475           infrastructure by preventing that data (e.g. Meter Data, configuration settings,  
476           or firmware updates) from forged components (with the aim to cause damage  
477           to the Smart Grid) will be accepted in the system.

#### 478           1.4.5.4 Information flow control and firewall

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

- 482           • only the Gateway may establish a connection to an external entity in the WAN<sup>14</sup>;  
483           specifically connection establishment by an external entity in the WAN or a Me-  
484           ter in the LMN to the WAN is not possible,  
485           • the Gateway can establish connections to devices in the LMN or in the HAN,  
486           • Meters in the LMN are only allowed to establish a connection to the Gateway,  
487           • the Gateway shall offer a wake-up service that allows external entities in the  
488           WAN to trigger a connection establishment by the Gateway,  
489           • connections are allowed to pre-configured addresses only,  
490           • only cryptographically-protected (i.e. encrypted, integrity protected and mutu-  
491           ally authenticated) connections are possible.<sup>15</sup>

492           These functionalities

- 493           • prevent that the Gateway itself or the components behind the Gateway (i.e.  
494           Meters or Controllable Local Systems) can be conquered by a WAN attacker  
495           (as defined in section 3.4), that processed data are transmitted to the wrong  
496           external entity, and that processed data are transmitted without being confi-  
497           dentiality/authenticity/integrity-protected,  
498           • protect the Smart Metering System and a corresponding large scale infrastruc-  
499           ture in two ways: by preventing that conquered components will send forged

---

14           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.

15           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.

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

505 The communication flows that are enforced by the Gateway between parties in the HAN,  
 506 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)

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

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

- 509 1. Communications within the **WAN** are not restricted. However, the Gateway is  
 510 not involved in this communication,
- 511 2. No communications between devices in the **LMN** are assumed. Devices in the  
 512 LMN may only communicate to the Gateway and shall not be connected to any  
 513 other network,
- 514 3. Devices in the **HAN** may communicate with each other. However, the Gateway  
 515 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.

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

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

- 522 • the Gateway accepts the submission of Meter Data from the LMN,
- 523 • the Gateway offers a wake-up service at the WAN side as described in chapter  
524 1.4.6.5 of [PP\_GW],
- 525 • the Gateway offers a user interface to the HAN that allows CLS or consumers  
526 to connect to the Gateway in order to read relevant information.

#### 527 1.4.5.5 Wake-Up-Service

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

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

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

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

- 541 1. The Gateway verifies the wake-up packet. This comprises
  - 542 i. a check if the header identification is correct,
  - 543 ii. the recipient is the Gateway,
  - 544 iii. the wake-up packet has been sent/received within an acceptable period  
545 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.

- 546                   iv. the wake-up message has not been received before,  
547                   2. If the wake-up message could not be verified as described in step #1, the  
548                   message will be dropped/ignored. No further operations will be initiated and no  
549                   feedback is provided.  
550                   3. If the message could be verified as described in step #1, the signature of the  
551                   wake-up message will be verified. The Gateway uses the services of its Security  
552                   Module for signature verification.  
553                   4. If the signature of the wake-up message cannot be verified as described in step  
554                   #3 the message will be dropped/ignored. No feedback is given to the sending  
555                   external entity and the wake-up sequence terminates.  
556                   5. If the signature of the wake-up message could be verified successfully , the  
557                   Gateway initiates a connection to a pre-configured external entity; however no  
558                   feedback is given to the sending external entity.

559                   More details on the exact implementation of this mechanism can be found in [TR-03109-  
560                   1, „Wake-Up Service“].

#### 561                   1.4.5.6 Privacy Preservation

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

564                   This contains two aspects:

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

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

## 579 **Monitoring of Data Transfers**

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

## 583 **Configuration Reporting**

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

## 589 **Audit Log and Monitoring**

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

### 594 1.4.5.7 Management of Security Functions

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

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

## 601 **System Status**

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

### 605 1.4.5.8 Identification and Authentication

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

610 Gateway as well as the identification and authentication of CLS located in HAN and  
 611 Meters located in LMN.

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

616 **1.4.6 The logical interfaces of the TOE**

617 The TOE offers its functionality as outlined before via a set of external interfaces. Figure  
 618 2 also indicates the cardinality of the interfaces. The following table provides an overview  
 619 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.
--	---

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

621 **1.4.7 The cryptography of the TOE and its Security Module**

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

629 The following table provides a more detailed overview on how the cryptographic  
 630 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>

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

632

633 1.4.7.1 Content data encryption vs. an encrypted channel

634 The TOE utilises concepts of the encryption of data on the content level as well as the  
 635 establishment of a trusted channel to external entities.

636 As a general rule, all processed Meter Data that is prepared to be submitted to ex-  
 637 ternal entities is encrypted and integrity protected on a content level using CMS (ac-  
 638 cording to [TR-03109-1-I]).

639 Further, all communication with external entities is enforced to happen via encrypted,  
 640 integrity protected and mutually authenticated channels.

641 This concept of encryption on two layers facilitates use cases in which the external  
 642 party that the TOE communicates with is not the final recipient of the Meter Data. In

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

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

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

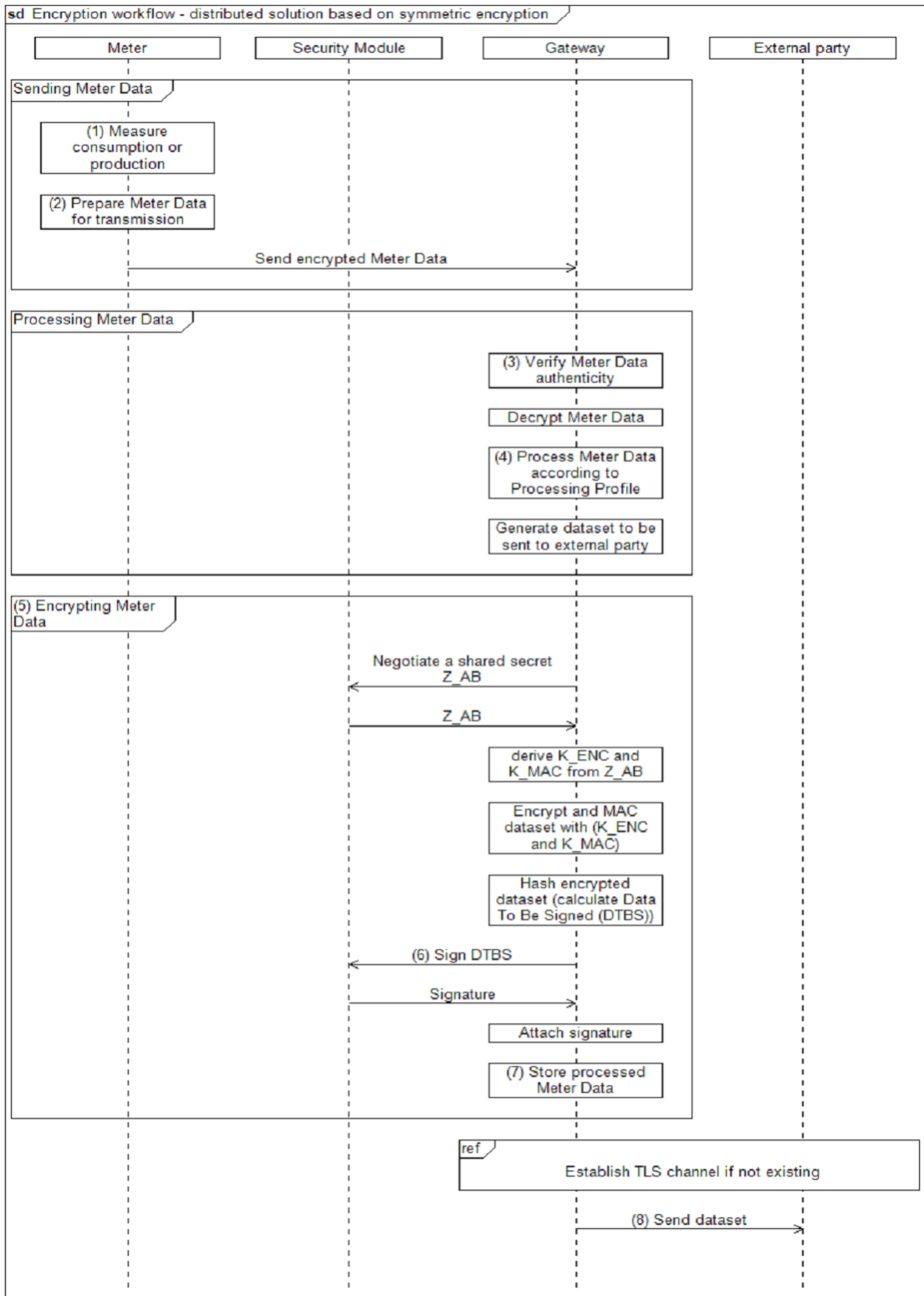
650 The basic information flow for Meter Data is as follows and shown in Figure 5:

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

---

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

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



675  
 676 **Figure 5: Cryptographic information flow for distributed Meters and Gateway**

677

678 **TOE life-cycle**

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

- 680 1. Development
- 681 2. Production
- 682 3. Pre-personalization at the developer's premises (without Security Module)
- 683 4. Pre-personalization and integration of Security Module
- 684 5. Delivery to the MPO
- 685 6. Delivery by the MPO to the installation and operational environment
- 686 7. Installation and start of operation
- 687 8. Personalization
- 688 9. Normal operation

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

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

## 695 2 Conformance Claims

### 696 2.1 CC Conformance Claim

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

702

### 703 2.2 PP Claim / Conformance Statement

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

705 In comparison to the PP, the assumption A.Delivery and the security objective for the  
706 environment OE.Delivery have been added and a refinement on the assurance compo-  
707 nent ALC\_DEL.1 has been made in order to reduce the certified scope of the TOE de-  
708 livery to the MPO.

709

### 710 2.3 Package Claim

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

713

### 714 2.4 Conformance Claim Rationale

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

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

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

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

723            This Security Target is consistent to the security requirements stated in [PP\_GW], no  
724            security requirement of the PP is removed, nor added to this Security Target.  
725

## 726 3 Security Problem Definition

### 727 3.1 External entities

728 The following external entities interact with the system consisting of Meter and Gateway.  
 729 Those roles have been defined for the use in this Security Target. It is possible that a  
 730 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.

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

732

### 733 3.2 Assets

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

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

738

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>

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

740 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>

741

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

742

### 743 3.3 Assumptions

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

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

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

754 **A.PhysicalProtection** It is assumed that the TOE is installed in a non-public en-  
755 vironment within the premises of the Consumer which pro-  
756 vides a basic level of physical protection. This protection  
757 covers the TOE, the Meter(s) that the TOE communicates  
758 with and the communication channel between the TOE and  
759 its Security Module.

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

762 **A.Update** It is assumed that firmware updates for the Gateway that  
763 can be provided by an authorised external entity have un-  
764 dergone a certification process according to this Security  
765 Target before they are issued and can therefore be as-  
766 sumed to be correctly implemented. It is further assumed  
767 that the external entity that is authorised to provide the up-  
768 date is trustworthy and will not introduce any malware into  
769 a firmware update.

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

- 771 • a WAN network connection with a sufficient reliabil-  
772 ity and bandwidth for the individual situation is  
773 available,
- 774 • one or more trustworthy sources for an update of  
775 the system time are available in the WAN,

- 776
- 777
- 778
- 779
- 780
- 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.

781 **A.Keygen**

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

785 **A.Delivery**

786 After the reception of the TOE by the MPO, the MPO is  
787 responsible for the secure delivery of the TOE to the instal-  
788 lation and operational environment. It is assumed that the  
789 MPO is trustworthy in context of this delivery and well  
790 trained and takes appropriate security measures to ensure  
791 protection against undetected manipulation or undetected  
792 replacement of the TOE during such a delivery to ensure  
integrity and authenticity of the TOE.

793 Note that adhering to [MSB-LK] is sufficient for MPOs to  
794 fulfill this assumption.

795 **Application Note 1:**

796 This ST acknowledges that the Gateway cannot be com-  
797 pletely protected against unauthorised physical access by  
798 its environment. However, it is important for the overall se-  
799 curity of the TOE that it is not installed within a public envi-  
ronment.

800 The level of physical protection that is expected to be pro-  
801 vided by the environment is the same level of protection  
802 that is expected for classical meters that operate according  
803 to the regulations of the national calibration authority [TR-  
804 03109-1].

---

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.

805           **Application Note 2:**           The Processing Profiles that are used for information flow  
806 control as referred to by A.ProcessProfile are an essential  
807 factor for the preservation of the privacy of the Consumer.  
808 The Processing Profiles are used to determine which data  
809 shall be sent to which entity at which frequency and how  
810 data are processed, e.g. whether the data needs to be re-  
811 lated to the Consumer (because it is used for billing pur-  
812 poses) or whether the data shall be pseudonymised.

813           The Processing Profiles shall be visible for the Consumer  
814 to allow a transparent communication.

815           It is essential that Processing Profiles correctly define the  
816 amount of information that must be sent to an external en-  
817 tity. Exact regulations regarding the Processing Profiles  
818 and the Gateway Administrator are beyond the scope of  
819 this Security Target.

820

## 821           **3.4 Threats**

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

- 827           • Attackers having physical access to Meter, Gateway, a connection between  
828 these components or local logical access to any of the interfaces (local at-  
829 tacker), trying to disclose or alter assets while stored in the Gateway or while  
830 transmitted between Meters in the LMN and the Gateway. Please note that the  
831 following threat model assumes that the local attacker has less motivation than  
832 the WAN attacker as a successful attack of a local attacker will always only  
833 impact one Gateway. Please further note that the local attacker includes au-  
834 thorised individuals like consumers.
- 835           • An attacker located in the WAN (WAN attacker) trying to compromise the con-  
836 fidentiality and/or integrity of the processed Meter Data and or configuration  
837 data transmitted via the WAN, or attacker trying to conquer a component of the

838 infrastructure (i.e. Meter, Gateway or Controllable Local System) via the WAN  
839 to cause damage to a component itself or to the corresponding grid (e.g. by  
840 sending forged Meter Data to an external entity).

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

846

847 **T.DataModificationLocal** A local attacker may try to modify (i.e. alter, delete, insert,  
848 replay or redirect) Meter Data when transmitted between  
849 Meter and Gateway, Gateway and Consumer, or Gateway  
850 and external entities. The objective of the attacker may be  
851 to alter billing-relevant information or grid status infor-  
852 mation. The attacker may perform the attack via any inter-  
853 face (LMN, HAN, or WAN).

854 In order to achieve the modification, the attacker may also  
855 try to modify secondary assets like the firmware or config-  
856 uration parameters of the Gateway.

857 **T.DataModificationWAN** A WAN attacker may try to modify (i.e. alter, delete, insert,  
858 replay or redirect) Meter Data, Gateway config data, Meter  
859 config data, CLS config data or a firmware update when  
860 transmitted between the Gateway and an external entity in  
861 the WAN.

862 When trying to modify Meter Data, it is the objective of the  
863 WAN attacker to modify billing-relevant information or grid  
864 status data.

865 When trying to modify config data or a firmware update, the  
866 WAN attacker tries to circumvent security mechanisms of  
867 the TOE or tries to get control over the TOE or a device in  
868 the LAN that is protected by the TOE.

869 **T.TimeModification** A local attacker or WAN attacker may try to alter the Gate-  
870 way time. The motivation of the attacker could be e.g. to

871		change the relation between date/time and measured consumption or production values in the Meter Data records
872		(e.g. to influence the balance of the next invoice).
873		
874	<b>T.DisclosureWAN</b>	A WAN attacker may try to violate the privacy of the Consumer by disclosing Meter Data or configuration data (Meter config, Gateway config or CLS config) or parts of it
875		when transmitted between Gateway and external entities
876		in the WAN.
877		
878		
879	<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
880		Meters of more than one Consumer are served by one
881		Gateway.
882		
883		
884	<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
885		or the grids used for commodity distribution (e.g. by sending wrong data to an external entity).
886		
887		
888		
889		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.
890		
891	<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).
892		
893		
894		
895		
896	<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.
897		
898		
899		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.
900		
901		
902	<b>T.Privacy</b>	A WAN attacker may try to obtain more detailed information from the Gateway than actually required to fulfil the
903		

904 tasks defined by its role or the contract with the Consumer.  
905 This includes scenarios in which an external entity that is  
906 primarily authorised to obtain information from the TOE  
907 tries to obtain more information than the information that  
908 has been authorised as well as scenarios in which an at-  
909 tacker who is not authorised at all tries to obtain infor-  
910 mation.  
911

## 912 3.5 Organizational Security Policies

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

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

- 917 • verification of digital signatures,
- 918 • generation of digital signatures,
- 919 • key agreement,
- 920 • key transport,
- 921 • key storage,
- 922 • Random Number Generation,

923 The Security Module shall be certified according to  
924 [SecModPP] and shall be used in accordance with its rele-  
925 vant guidance documentation.

926 **OSP.Log** The TOE shall maintain a set of log files as defined in [TR-  
927 03109-1] as follows:

- 928 1. A system log of relevant events in order to allow an  
929 authorised Gateway Administrator to analyse the  
930 status of the TOE. The TOE shall also analyse the  
931 system log automatically for a cumulation of secu-  
932 rity relevant events.
- 933 2. A consumer log that contains information about the  
934 information flows that have been initiated to the  
935 WAN and information about the Processing Profiles  
936 causing this information flow as well as the billing-  
937 relevant information.
- 938 3. A calibration log (as defined in chapter 6.2.1) that  
939 provides the Gateway Administrator with a possibil-  
940 ity to review calibration relevant events.

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

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

945 Administrator via the IF\_GW\_WAN interface of the  
946 TOE and an authorised Service Technician via the  
947 IF\_GW\_SRV interface of the TOE.

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

951 3. Access to the information in the consumer log shall  
952 only be allowed for an authorised Consumer via the  
953 IF\_GW\_CON interface of the TOE. The Consumer  
954 shall only have access to their own information.

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

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

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

## 963 4 Security Objectives

### 964 4.1 Security Objectives for the TOE

#### 965 O.Firewall

966 The TOE shall serve as the connection point for the con-  
967 nected devices within the LAN to external entities within  
968 the WAN and shall provide firewall functionality in order to  
969 protect the devices of the LMN and HAN (as long as they  
970 use the Gateway) and itself against threats from the WAN  
side.

971 The firewall:

- 972 • shall allow only connections established from HAN
- 973 or the TOE itself to the WAN (i.e. from devices in
- 974 the HAN to external entities in the WAN or from the
- 975 TOE itself to external entities in the WAN),
- 976 • shall provide a wake-up service on the WAN side
- 977 interface,
- 978 • shall not allow connections from the LMN to the
- 979 WAN,
- 980 • shall not allow any other services being offered on
- 981 the WAN side interface,
- 982 • shall not allow connections from the WAN to the
- 983 LAN or to the TOE itself,
- 984 • shall enforce communication flows by allowing traf-
- 985 fic from CLS in the HAN to the WAN only if confi-
- 986 dentiality-protected and integrity-protected and if
- 987 endpoints are authenticated.

#### 988 O.SeparateIF

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

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

995	<b>O.Conceal</b>	To protect the privacy of its Consumers, the TOE shall conceal the communication with external entities in the WAN
996		in order to ensure that no privacy-relevant information may
997		be obtained by analysing the frequency, load, size or the
998		absence of external communication. <sup>24</sup>
999		
1000	<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.
1001		
1002		
1003		
1004		This includes that:
1005		<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>
1006		<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>
1007		<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>
1008		<ul style="list-style-type: none"><li>• the TOE shall process the data according to the definition in the corresponding Processing Profile,</li></ul>
1009		<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>
1010		<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>
1011		<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>
1012		
1013		
1014		
1015		
1016		
1017		
1018		
1019		
1020		
1021		
1022		

---

<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.

1023 the data until a configurable number of unsuccessful  
 1024 retrials has been reached,  
 1025 • the TOE shall pseudonymize the data for parties  
 1026 that do not need the relation between the processed  
 1027 Meter Data and the identity of the Consumer.  
 1028

1029 **O.Crypt**

1030 The TOE shall provide cryptographic functionality as follows:  
 1031 • authentication, integrity protection and encryption  
 1032 of the communication and data to external entities  
 1033 in the WAN,  
 1034 • authentication, integrity protection and encryption  
 1035 of the communication to the Meter,  
 1036 • authentication, integrity protection and encryption  
 1037 of the communication to the Consumer,  
 1038 • replay detection for all communications with external  
 1039 entities,  
 1040 • encryption of the persistently stored TSF and user  
 1041 data of the TOE<sup>26</sup>.

1042 In addition, the TOE shall generate the required keys utilizing  
 1043 the services of its Security Module<sup>27</sup>, ensure that the  
 1044 keys are only used for an acceptable amount of time and  
 1045 destroy ephemeral<sup>28</sup> keys if no longer needed.<sup>29</sup>

1046 **O.Time**

1047 The TOE shall provide reliable time stamps and update  
 1048 its internal clock in regular intervals by retrieving reliable  
 1049 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.

1050	<b>O.Protect</b>	The TOE shall implement functionality to protect its security functions against malfunctions and tampering.
1051		
1052		Specifically, the TOE shall
1053		<ul style="list-style-type: none"> <li>• encrypt its TSF and user data as long as it is not in use,</li> </ul>
1054		
1055		<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>
1056		
1057		
1058		<ul style="list-style-type: none"> <li>• monitor user data and the TOE firmware for integrity errors,</li> </ul>
1059		
1060		<ul style="list-style-type: none"> <li>• contain a test that detects whether the interfaces for WAN and LAN are separate,</li> </ul>
1061		
1062		<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>
1063		
1064		<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>
1065		
1066		
1067		
1068	<b>O.Management</b>	The TOE shall only provide authorised Gateway Administrators with functions for the management of the security features.
1069		
1070		
1071		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.
1072		
1073		
1074		
1075		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
1076		
1077		

---

<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.

1078		and that only authentic and integrity protected updates are
1079		applied.
1080	<b>O.Log</b>	The TOE shall maintain a set of log files as defined in [TR-
1081		03109-1] as follows:
1082		1. A system log of relevant events in order to allow an
1083		authorised Gateway Administrator or an authorised
1084		Service Technician to analyse the status of the
1085		TOE. The TOE shall also analyse the system log
1086		automatically for a cumulation of security relevant
1087		events.
1088		2. A consumer log that contains information about the
1089		information flows that have been initiated to the
1090		WAN and information about the Processing Profiles
1091		causing this information flow as well as the billing-
1092		relevant information and information about the sys-
1093		tem status (including relevant error messages).
1094		3. A calibration log that provides the Gateway Admin-
1095		istrator with a possibility to review calibration rele-
1096		vant events.
1097		The TOE shall further limit access to the information in the
1098		different log files as follows:
1099		1. Access to the information in the system log shall
1100		only be allowed for an authorised Gateway Admin-
1101		istrator via IF_GW_WAN or for an authorised Ser-
1102		vice Technician via IF_GW_SRV.
1103		2. Access to the information in the consumer log shall
1104		only be allowed for an authorised Consumer via the
1105		IF_GW_CON interface of the TOE and via a se-
1106		cured (i.e. confidentiality and integrity protected)
1107		connection. The Consumer shall only have access
1108		to their own information.
1109		3. Read-only access to the information in the calibra-
1110		tion log shall only be allowed for an authorised

1111 Gateway Administrator via the WAN interface of the  
1112 TOE.

1113 The system log may overwrite the oldest events in case  
1114 that the audit trail gets full.

1115 For the consumer log, the TOE shall ensure that a suffi-  
1116 cient amount of events is available (in order to allow a Con-  
1117 sumer to verify an invoice) but may overwrite older events  
1118 in case that the audit trail gets full.

1119 For the calibration log however, the TOE shall ensure the  
1120 availability of all events over the lifetime of the TOE.

1121 **O.Access** The TOE shall control the access of external entities in  
1122 WAN, HAN or LMN to any information that is sent to, from  
1123 or via the TOE via its external interfaces<sup>32</sup>. Access control  
1124 shall depend on the destination interface that is used to  
1125 send that information.

1126

## 1127 **4.2 Security Objectives for the Operational Environment**

1128 **OE.ExternalPrivacy** Authorised and authenticated external entities receiving  
1129 any kind of private or billing-relevant data shall be trustwor-  
1130 thy and shall not perform unauthorised analyses of these  
1131 data with respect to the corresponding consumer(s).

1132 **OE.TrustedAdmins** The Gateway Administrator and the Service Technician  
1133 shall be trustworthy and well-trained.

1134 **OE.PhysicalProtection** The TOE shall be installed in a non-public environment  
1135 within the premises of the Consumer that provides a basic  
1136 level of physical protection. This protection shall cover the  
1137 TOE, the Meters that the TOE communicates with and the  
1138 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.

1139		Module. Only authorised individuals may physically access
1140		the TOE.
1141	<b>OE.Profile</b>	The Processing Profiles that are used when handling data
1142		shall be obtained from a trustworthy and reliable source
1143		only.
1144	<b>OE.SM</b>	The environment shall provide the services of a certified
1145		Security Module for
1146		<ul style="list-style-type: none"><li>• verification of digital signatures,</li></ul>
1147		<ul style="list-style-type: none"><li>• generation of digital signatures,</li></ul>
1148		<ul style="list-style-type: none"><li>• key agreement,</li></ul>
1149		<ul style="list-style-type: none"><li>• key transport,</li></ul>
1150		<ul style="list-style-type: none"><li>• key storage,</li></ul>
1151		<ul style="list-style-type: none"><li>• Random Number Generation.</li></ul>
1152		The Security Module used shall be certified according to
1153		[SecModPP] and shall be used in accordance with its rele-
1154		vant guidance documentation.
1155	<b>OE.Update</b>	The firmware updates for the Gateway that can be pro-
1156		vided by an authorised external entity shall undergo a cer-
1157		tification process according to this Security Target before
1158		they are issued to show that the update is implemented
1159		correctly. The external entity that is authorised to provide
1160		the update shall be trustworthy and ensure that no mal-
1161		ware is introduced via a firmware update.
1162	<b>OE.Network</b>	It shall be ensured that
1163		<ul style="list-style-type: none"><li>• a WAN network connection with a sufficient reliabil-</li></ul>
1164		ity and bandwidth for the individual situation is
1165		available,
1166		<ul style="list-style-type: none"><li>• one or more trustworthy sources for an update of</li></ul>
1167		the system time are available in the WAN,
1168		<ul style="list-style-type: none"><li>• the Gateway is the only communication gateway for</li></ul>
1169		Meters in the LMN,



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	
A.Delivery																			X

**Table 8: Rationale for Security Objectives**

1193

1194

1195 **4.3.2 Countering the threats**

1196 The following sections provide more detailed information on how the threats are coun-  
1197 tered by the security objectives for the TOE and its operational environment.

1198

1199 4.3.2.1 General objectives

1200 The security objectives **O.Protect**, **O.Management** and **OE.TrustedAdmins** contribute  
1201 to counter each threat and contribute to each OSP.

1202 **O.Management** is indispensable as it defines the requirements around the management  
1203 of the Security Functions. Without a secure management no TOE can be secure. Also  
1204 **OE.TrustedAdmins** contributes to this aspect as it provides the requirements on the  
1205 availability of a trustworthy Gateway Administrator and Service Technician. **O.Protect** is  
1206 present to ensure that all security functions are working as specified.

1207 Those general objectives will not be addressed in detail in the following paragraphs.

1208 4.3.2.2 T.DataModificationLocal

1209 The threat **T.DataModificationLocal** is countered by a combination of the security ob-  
1210 jectives **O.Meter**, **O.Crypt**, **O.Log** and **OE.PhysicalProtection**.

1211 **O.Meter** defines that the TOE will enforce the encryption of communication when receiv-  
1212 ing Meter Data from the Meter. **O.Crypt** defines the required cryptographic functionality.  
1213 The objectives together ensure that the communication between the Meter and the TOE  
1214 cannot be modified or released.

1215 **OE.PhysicalProtection** is of relevance as it ensures that access to the TOE is limited.

1216 4.3.2.3 T.DataModificationWAN

1217 The threat **T.DataModificationWAN** is countered by a combination of the security ob-  
1218 jectives **O.Firewall** and **O.Crypt**.

1219 **O.Firewall** defines the connections for the devices within the LAN to external entities  
1220 within the WAN and shall provide firewall functionality in order to protect the devices of  
1221 the LMN and HAN (as long as they use the Gateway) and itself against threats from the  
1222 WAN side. **O.Crypt** defines the required cryptographic functionality. Both objectives to-  
1223 gether ensure that the data transmitted between the TOE and the WAN cannot be mod-  
1224 ified by a WAN attacker.

1225 4.3.2.4 T.TimeModification

1226 The threat **T.TimeModification** is countered by a combination of the security objectives  
1227 **O.Time, O.Crypt** and **OE.PhysicalProtection**.

1228 **O.Time** defines that the TOE needs a reliable time stamp mechanism that is also up-  
1229 dated from reliable sources regularly in the WAN. **O.Crypt** defines the required crypto-  
1230 graphic functionality for the communication to external entities in the WAN. Therewith,  
1231 O.Time and O.Crypt are the core objective to counter the threat T.TimeModification.

1232 **OE.PhysicalProtection** is of relevance as it ensures that access to the TOE is limited.

1233 4.3.2.5 T.DisclosureWAN

1234 The threat **T.DisclosureWAN** is countered by a combination of the security objectives  
1235 **O.Firewall, O.Conceal** and **O.Crypt**.

1236 **O.Firewall** defines the connections for the devices within the LAN to external entities  
1237 within the WAN and shall provide firewall functionality in order to protect the devices of  
1238 the LMN and HAN (as long as they use the Gateway) and itself against threats from the  
1239 WAN side. **O.Crypt** defines the required cryptographic functionality. Both objectives to-  
1240 gether ensure that the communication between the Meter and the TOE cannot be dis-  
1241 closed.

1242 **O.Conceal** ensures that no information can be disclosed based on additional character-  
1243 istics of the communication like frequency, load or the absence of a communication.

1244 4.3.2.6 T.DisclosureLocal

1245 The threat **T.DisclosureLocal** is countered by a combination of the security objectives  
1246 **O.Meter, O.Crypt** and **OE.PhysicalProtection**.

1247 **O.Meter** defines that the TOE will enforce the encryption and integrity protection of com-  
1248 munication when polling or receiving Meter Data from the Meter. **O.Crypt** defines the  
1249 required cryptographic functionality. Both objectives together ensure that the communi-  
1250 cation between the Meter and the TOE cannot be disclosed.

1251 **OE.PhysicalProtection** is of relevance as it ensures that access to the TOE is limited.

1252 4.3.2.7 T.Infrastructure

1253 The threat **T.Infrastructure** is countered by a combination of the security objectives  
1254 **O.Firewall, O.SeparateIF, O.Meter** and **O.Crypt**.

1255 **O.Firewall** is the core objective that counters this threat. It ensures that all communica-  
1256 tion flows to the WAN are initiated by the TOE. The fact that the TOE does not offer any  
1257 services to the WAN side and will not react to any requests (except the wake-up call)  
1258 from the WAN is a significant aspect in countering this threat. Further the TOE will only  
1259 communicate using encrypted channels to authenticated and trustworthy parties which  
1260 mitigates the possibility that an attacker could try to hijack a communication.

1261 **O.Meter** defines that the TOE will enforce the encryption and integrity protection for the  
1262 communication with the Meter.

1263 **O.SeparateIF** facilitates the disjunction of the WAN from the LMN.

1264 **O.Crypt** supports the mitigation of this threat by providing the required cryptographic  
1265 primitives.

#### 1266 4.3.2.8 T.ResidualData

1267 The threat **T.ResidualData** is mitigated by the security objective **O.Protect** as this se-  
1268 curity objective defines that the TOE shall delete information as soon as it is no longer  
1269 used. Assuming that a TOE follows this requirement, an attacker cannot read out any  
1270 residual information as it does simply not exist.

#### 1271 4.3.2.9 T.ResidentData

1272 The threat **T.ResidentData** is countered by a combination of the security objectives  
1273 **O.Access**, **O.Firewall**, **O.Protect** and **O.Crypt**. Further, the environment (**OE.Physi-**  
1274 **calProtection** and **OE.TrustedAdmins**) contributes to this.

1275 **O.Access** defines that the TOE shall control the access of users to information via the  
1276 external interfaces.

1277 The aspect of a local attacker with physical access to the TOE is covered by a combi-  
1278 nation of **O.Protect** (defining the detection of physical manipulation) and **O.Crypt** (re-  
1279 quiring the encryption of persistently stored TSF and user data of the TOE). In addition,  
1280 the physical protection provided by the environment (**OE.PhysicalProtection**) and the  
1281 Gateway Administrator (**OE.TrustedAdmins**) who could realise a physical manipulation  
1282 contribute to counter this threat.

1283 The aspect of a WAN attacker is covered by **O.Firewall** as this objective ensures that  
1284 an adequate level of protection is realised against attacks from the WAN side.

1285 4.3.2.10 T.Privacy

1286 The threat **T.Privacy** is primarily addressed by the security objectives **O.Meter**, **O.Crypt**  
1287 and **O.Firewall** as these objective ensures that the TOE will only distribute Meter Data  
1288 to external parties in the WAN as defined in the corresponding Processing Profiles and  
1289 that the data will be protected for the transfer. **OE.Profile** is present to ensure that the  
1290 Processing Profiles are obtained from a trustworthy and reliable source only.

1291 Finally, **O.Conceal** ensures that an attacker cannot obtain the relevant information for  
1292 this threat by observing external characteristics of the information flow.

### 1293 **4.3.3 Coverage of organisational security policies**

1294 The following sections provide more detailed information about how the security objec-  
1295 tives for the environment and the TOE cover the organizational security policies.

#### 1296 4.3.3.1 OSP.SM

1297 The Organizational Security Policy **OSP.SM** that mandates that the TOE utilises the ser-  
1298 vices of a certified Security Module is directly addressed by the security objectives  
1299 **OE.SM** and **O.Crypt**. The objective **OE.SM** addresses the functions that the Security  
1300 Module shall be utilised for as defined in **OSP.SM** and also requires a certified Security  
1301 Module. **O.Crypt** defines the cryptographic functionalities for the TOE itself. In this con-  
1302 text, it has to be ensured that the Security Module is operated in accordance with its  
1303 guidance documentation.

#### 1304 4.3.3.2 OSP.Log

1305 The Organizational Security Policy **OSP.Log** that mandates that the TOE maintains an  
1306 audit log is directly addressed by the security objective for the TOE **O.Log**.

1307 **O.Access** contributes to the implementation of the OSP as it defines that also Gateway  
1308 Administrators are not allowed to read/modify all data. This is of specific importance to  
1309 ensure the confidentiality and integrity of the log data as is required by the **OSP.Log**.

### 1310 **4.3.4 Coverage of assumptions**

1311 The following sections provide more detailed information about how the security objec-  
1312 tives for the environment cover the assumptions.

#### 1313 4.3.4.1 A.ExternalPrivacy

1314 The assumption **A.ExternalPrivacy** is directly and completely covered by the security  
1315 objective **OE.ExternalPrivacy**. The assumption and the objective for the environment  
1316 are drafted in a way that the correspondence is obvious.

1317 4.3.4.2 A.TrustedAdmins

1318 The assumption **A.TrustedAdmins** is directly and completely covered by the security  
1319 objective **OE.TrustedAdmins**. The assumption and the objective for the environment  
1320 are drafted in a way that the correspondence is obvious.

1321 4.3.4.3 A.PhysicalProtection

1322 The assumption **A.PhysicalProtection** is directly and completely covered by the secu-  
1323 rity objective **OE.PhysicalProtection**. The assumption and the objective for the envi-  
1324 ronment are drafted in a way that the correspondence is obvious.

1325 4.3.4.4 A.ProcessProfile

1326 The assumption **A.ProcessProfile** is directly and completely covered by the security  
1327 objective **OE.Profile**. The assumption and the objective for the environment are drafted  
1328 in a way that the correspondence is obvious.

1329 4.3.4.5 A.Update

1330 The assumption **A.Update** is directly and completely covered by the security objective  
1331 **OE.Update**. The assumption and the objective for the environment are drafted in a way  
1332 that the correspondence is obvious.

1333 4.3.4.6 A.Network

1334 The assumption **A.Network** is directly and completely covered by the security objective  
1335 **OE.Network**. The assumption and the objective for the environment are drafted in a way  
1336 that the correspondence is obvious.

1337 4.3.4.7 A.Keygen

1338 The assumption **A.Keygen** is directly and completely covered by the security objective  
1339 **OE.Keygen**. The assumption and the objective for the environment are drafted in a way  
1340 that the correspondence is obvious.

1341 4.3.4.8 A.Delivery

1342 The assumption **A.Delivery** is directly and completely covered by the security objective  
1343 **OE.Delivery**. The assumption and the objective for the environment are drafted in a way  
1344 that the correspondence is obvious.

1345

1346 **5 Extended Component definition**

1347 **5.1 Communication concealing (FPR\_CON)**

1348 The additional family Communication concealing (FPR\_CON) of the Class FPR (Pri-  
1349 vacy) is defined here to describe the specific IT security functional requirements of the  
1350 TOE. The TOE shall prevent attacks against Personally Identifiable Information (PII) of  
1351 the Consumer that may be obtained by an attacker by observing the encrypted commu-  
1352 nication of the TOE with remote entities.

1353

1354 **5.2 Family behaviour**

1355 This family defines requirements to mitigate attacks against communication channels in  
1356 which an attacker tries to obtain privacy relevant information based on characteristics of  
1357 an encrypted communication channel. Examples include but are not limited to an analy-  
1358 sis of the frequency of communication or the transmitted workload.

1359

1360 **5.3 Component levelling**

1361 FPR\_CON: Communication concealing -----1

1362

1363 **5.4 Management**

1364 The following actions could be considered for the management functions in FMT:

- 1365 a. Definition of the interval in FPR\_CON.1.2 if definable within the operational  
1366 phase of the TOE.

1367

1368 **5.5 Audit**

1369 There are no auditable events foreseen.

1370

1371 **5.6 Communication concealing (FPR\_CON.1)**

1372 Hierarchical to: No other components.

1373 Dependencies: No dependencies.

1374 FPR\_CON.1.1 The TSF shall enforce the [assignment: *information*  
1375 *flow policy*] in order to ensure that no personally iden-  
1376 tifiable information (PII) can be obtained by an analysis  
1377 of [assignment: *characteristics of the information flow*  
1378 *that need to be concealed*].

1379 FPR\_CON.1.2 The TSF shall connect to [assignment: *list of external*  
1380 *entities*] in intervals as follows [selection: *weekly,*  
1381 *daily, hourly, [assignment: other interval]*] to conceal  
1382 the data flow.

## 1383 6 Security Requirements

### 1384 6.1 Overview

1385 This chapter describes the security functional and the assurance requirements which  
 1386 have to be fulfilled by the TOE. Those requirements comprise functional components  
 1387 from part 2 of [CC] and the assurance components as defined for the Evaluation Assur-  
 1388 ance Level 4 from part 3 of [CC].

1389 The following notations are used:

- 1390 • **Refinement** operation (denoted by **bold text**): is used to add details to a re-  
 1391 quirement, and thus further restricts a requirement. In case that a word has  
 1392 been deleted from the original text this refinement is indicated by crossed out  
 1393 ~~bold text~~.
- 1394 • **Selection** operation (denoted by underlined text): is used to select one or more  
 1395 options provided by the [CC] in stating a requirement.
- 1396 • **Assignment** operation (denoted by *italicised text*): is used to assign a specific  
 1397 value to an unspecified parameter, such as the length of a password.
- 1398 • **Iteration** operation: are identified with a suffix in the name of the SFR (e.g.  
 1399 FDP\_IFC.2/FW).

1400 It should be noted that the requirements in the following chapters are not necessarily be  
 1401 ordered alphabetically. Where useful the requirements have been grouped.

1402 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

1403

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

1404 **6.2 Class FAU: Security Audit**

1405 **6.2.1 Introduction**

1406 The TOE compliant to this Security Target shall implement three different audit logs as  
 1407 defined in **OSP.Log** and **O.Log**. The following table provides an overview over the three  
 1408 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>

1409

**Table 10: Overview over audit processes**

1410	<b>6.2.2 Security Requirements for the System Log</b>	
1411	6.2.2.1 Security audit automatic response (FAU_ARP)	
1412	<b>6.2.2.1.1 FAU_ARP.1/SYS: Security Alarms for system log</b>	
1413	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>
1414		upon detection of a potential security violation.
1415		
1416	Hierarchical to:	No other components
1417	Dependencies:	FAU_SAA.1 Potential violation analysis
1418		
1419	6.2.2.2 Security audit data generation (FAU_GEN)	
1420	<b>6.2.2.2.1 FAU_GEN.1/SYS: Audit data generation for system log</b>	
1421	FAU_GEN.1.1/SYS	The TSF shall be able to generate an audit record of the
1422		following auditable events:
1423		a) Start-up and shutdown of the audit functions;
1424		b) All auditable events for the <u>basic</u> <sup>34</sup> level of audit; and
1425		c) <i>other non privacy relevant auditable events: none</i> <sup>35</sup> .
1426	FAU_GEN.1.2/SYS	The TSF shall record within each audit record at least the
1427		following information:
1428		a) Date and time of the event, type of event, subject identity
1429		(if applicable), and the outcome (success or failure) of the
1430		event; and
1431		b) For each audit event type, based on the auditable event
1432		definitions of the functional components included in the
1433		<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*]

1434	Hierarchical to:	No other components
1435	Dependencies:	FPT_STM.1
1436	6.2.2.3 Security audit analysis (FAU_SAA)	
1437	<b>6.2.2.3.1 FAU_SAA.1/SYS: Potential violation analysis for system</b>	
1438	<b>log</b>	
1439	FAU_SAA.1.1./SYS	The TSF shall be able to apply a set of rules in monitoring
1440		the audited events and based upon these rules indicate a
1441		potential violation of the enforcement of the SFRs.
1442	FAU_SAA.1.2/SYS	The TSF shall enforce the following rules for monitoring
1443		audited events:
1444		a) Accumulation or combination of
1445		<ul style="list-style-type: none"> <li>• <i>Start-up and shutdown of the audit functions</i></li> </ul>
1446		<ul style="list-style-type: none"> <li>• <i>all auditable events for the basic level of audit</i></li> </ul>
1447		<ul style="list-style-type: none"> <li>• <i>all types of failures in the TSF as listed in</i></li> </ul>
1448		<i>FPT_FLS.1</i> <sup>38</sup>
1449		known to indicate a potential security violation.
1450		b) <i>any other rules: none</i> <sup>39</sup> .
1451	Hierarchical to:	No other components
1452	Dependencies:	FAU_GEN.1
1453	6.2.2.4 Security audit review (FAU_SAR)	
1454	<b>6.2.2.4.1 FAU_SAR.1/SYS: Audit Review for system log</b>	
1455	FAU_SAR.1.1/SYS	The TSF shall provide <i>only authorised Gateway</i>
1456		<i>Administrators via the IF_GW_WAN interface and</i>
1457		<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*]

1458		<i>interface</i> <sup>40</sup> with the capability to read all information <sup>41</sup>
1459		from the <b>system</b> audit records <sup>42</sup> .
1460	FAU_SAR.1.2/SYS	The TSF shall provide the audit records in a manner
1461		suitable for the user to interpret the information.
1462	Hierarchical to:	No other components
1463	Dependencies:	FAU_GEN.1
1464	6.2.2.5 Security audit event storage (FAU_STG)	
1465	<b>6.2.2.5.1 FAU_STG.4/SYS: Prevention of audit data loss for</b>	
1466	<b>systemlog</b>	
1467	FAU_STG.4.1/SYS	The TSF shall <u>overwrite the oldest stored audit records</u> <sup>43</sup>
1468		and other actions to be taken in case of audit storage
1469		failure: none <sup>44</sup> if the <b>system</b> audit trail <sup>45</sup> is full.
1470	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1471	Dependencies:	FAU_STG.1 Protected audit trail storage
1472	<b>Application Note 4:</b>	The size of the audit trail that is available before the oldest
1473		events get overwritten is configurable for the Gateway
1474		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*]

1475	<b>6.2.3 Security Requirements for the Consumer Log</b>	
1476	6.2.3.1 Security audit data generation (FAU_GEN)	
1477	<b>6.2.3.1.1 FAU_GEN.1/CON: Audit data generation for consumer log</b>	
1478	FAU_GEN.1.1/CON	The TSF shall be able to generate an audit record of the
1479		following auditable events:
1480		a) Start-up and shutdown of the audit functions;
1481		b) All auditable events for the <u>not specified</u> <sup>46</sup> level of audit;
1482		and
1483		c) <i>all audit events as listed in Table 11 and additional</i>
1484		<i>events: none</i> <sup>47</sup> .
1485	FAU_GEN.1.2/CON	The TSF shall record within each audit record at least the
1486		following information:
1487		a) Date and time of the event, type of event, subject identity
1488		(if applicable), and the outcome (success or failure) of the
1489		event; and
1490		b) For each audit event type, based on the auditable event
1491		definitions of the functional components included in the
1492		<b>PP/ST</b> <sup>48</sup> , <i>additional information as listed in Table 11 and</i>
1493		<i>additional events: none</i> <sup>49</sup> .
1494	Hierarchical to:	No other components
1495	Dependencies:	FPT_STM.1
1496		

---

<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	-

1497 **Table 11: Events for consumer log**

1498

1499 6.2.3.2 Security audit review (FAU\_SAR)

1500 **6.2.3.2.1 FAU\_SAR.1/CON: Audit Review for consumer log**

1501 FAU\_SAR.1.1/CON The TSF shall provide *only authorised Consumer via the*  
1502 *IF\_GW\_CON interface*<sup>50</sup> with the capability to read *all*

---

50 [assignment: *authorised users*]

1503		<i>information that are related to them</i> <sup>51</sup> from the <b>consumer</b>
1504		audit records <sup>52</sup> .
1505	FAU_SAR.1.2/CON	The TSF shall provide the audit records in a manner
1506		suitable for the user to interpret the information.
1507	Hierarchical to:	No other components
1508	Dependencies:	FAU_GEN.1
1509	<b>Application Note 5:</b>	FAU_SAR.1.2/CON shall ensure that the Consumer is
1510		able to interpret the information that is provided to him in a
1511		way that allows him to verify the invoice.
1512	6.2.3.3 Security audit event storage (FAU_STG)	
1513	<b>6.2.3.3.1 FAU_STG.4/CON: Prevention of audit data loss for the</b>	
1514	<b>consumer log</b>	
1515	FAU_STG.4.1/CON	The TSF shall <u>overwrite the oldest stored audit records</u> and
1516		<i>interrupt metrological operation in case that the oldest</i>
1517		<i>audit record must still be kept for billing verification</i> <sup>53</sup> if the
1518		<b>consumer</b> audit trail is full.
1519	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1520	Dependencies:	FAU_STG.1 Protected audit trail storage
1521	<b>Application Note 6:</b>	The size of the audit trail that is available before the oldest
1522		events get overwritten is configurable for the Gateway
1523		Administrator.

---

51 [assignment: *list of audit information*]

52 [refinement: *audit records*]

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

1524	<b>6.2.4 Security Requirements for the Calibration Log</b>	
1525	6.2.4.1 Security audit data generation (FAU_GEN)	
1526	<b>6.2.4.1.1 FAU_GEN.1/CAL: Audit data generation for calibration log</b>	
1527	FAU_GEN.1.1/CAL	The TSF shall be able to generate an audit record of the
1528		following auditable events:
1529		a) Start-up and shutdown of the audit functions;
1530		b) All auditable events for the <u>not specified</u> <sup>54</sup> level of audit;
1531		and
1532		c) <i>all calibration-relevant information according to Table</i>
1533		<i>12</i> <sup>55</sup> .
1534	FAU_GEN.1.2/CAL	The TSF shall record within each audit record at least the
1535		following information:
1536		a) Date and time of the event, type of event, subject identity
1537		(if applicable), and the outcome (success or failure) of the
1538		event; and
1539		b) For each audit event type, based on the auditable event
1540		definitions of the functional components included in the
1541		<b>PP/ST</b> <sup>56</sup> , <i>other audit relevant information: none</i> <sup>57</sup> .
1542	Hierarchical to:	No other components
1543	Dependencies:	FPT_STM.1
1544	<b>Application Note 7:</b>	The calibration log serves to fulfil national requirements in
1545		the context of the calibration of the TOE.
1546		

---

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>

<p>Change of meter profiles</p>	<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>
<p>Software update</p>	<p>Every update of the code which touches calibration regulations (serialized COSEM-objects, rules) MUST be logged in calibration log.</p>
<p>Firmware update</p>	<p>Every firmware update (incl. operating system update if applicable) MUST be logged in calibration log.</p>
<p>Error messages of a meter</p>	<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>

1547

**Table 12: Content of calibration log**

1548

1549	6.2.4.2 Security audit review (FAU_SAR)	
1550	<b>6.2.4.2.1 FAU_SAR.1/CAL: Audit Review for the calibration log</b>	
1551	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> .
1552		
1553		
1554		
1555	FAU_SAR.1.2/CAL	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
1556		
1557	Hierarchical to:	No other components
1558	Dependencies:	FAU_GEN.1
1559	6.2.4.3 Security audit event storage (FAU_STG)	
1560	<b>6.2.4.3.1 FAU_STG.4/CAL: Prevention of audit data loss for calibration log</b>	
1561		
1562	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.
1563		
1564		
1565	Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
1566	Dependencies:	FAU_STG.1 Protected audit trail storage
1567	<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.
1568		
1569		

---

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*]

1570	<b>6.2.5 Security Requirements that apply to all logs</b>	
1571	6.2.5.1 Security audit data generation (FAU_GEN)	
1572	<b>6.2.5.1.1 FAU_GEN.2: User identity association</b>	
1573	FAU_GEN.2.1	For audit events resulting from actions of identified users,
1574		the TSF shall be able to associate each auditable event
1575		with the identity of the user that caused the event.
1576	Hierarchical to:	No other components
1577	Dependencies:	FAU_GEN.1
1578		FIA_UID.1
1579	<b>Application Note 9:</b>	Please note that FAU_GEN.2 applies to all audit logs, the
1580		system log, the calibration log, and the consumer log.

1581	6.2.5.2 Security audit event storage (FAU_STG)	
1582	<b>6.2.5.2.1 FAU_STG.2: Guarantees of audit data availability</b>	
1583	FAU_STG.2.1	The TSF shall protect the stored audit records in <b>the all</b>
1584		audit trails <sup>64</sup> from unauthorised deletion.
1585	FAU_STG.2.2	The TSF shall be able to <u>prevent</u> <sup>65</sup> unauthorised
1586		modifications to the stored audit records in <b>the all</b> audit
1587		trails <sup>66</sup> .
1588	FAU_STG.2.3	The TSF shall ensure that <i>all</i> <sup>67</sup> stored audit records will be
1589		maintained when the following conditions occur: <u>audit</u>
1590		<u>storage exhaustion or failure</u> <sup>68</sup> .
1591	Hierarchical to:	FAU_STG.1 Protected audit trail storage
1592	Dependencies:	FAU_GEN.1
1593	<b>Application Note 10:</b>	Please note that FAU_STG.2 applies to all audit logs, the
1594		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*]

## 1595 6.3 Class FCO: Communication

### 1596 6.3.1 Non-repudiation of origin (FCO\_NRO)

#### 1597 6.3.1.1 FCO\_NRO.2: Enforced proof of origin

1598 FCO\_NRO.2.1 The TSF shall enforce the generation of evidence of origin  
1599 for transmitted *Meter Data*<sup>69</sup> at all times.

1600 FCO\_NRO.2.2 The TSF shall be able to relate the *key material used for*  
1601 *signature*<sup>70, 71</sup> of the originator of the information, and the  
1602 *signature*<sup>72</sup> of the information to which the evidence  
1603 applies.

1604 FCO\_NRO.2.3 The TSF shall provide a capability to verify the evidence of  
1605 origin of information to recipient, Consumer<sup>73</sup> given  
1606 *limitations of the digital signature according to TR-03109-*  
1607 *1*<sup>74</sup>.

1608 Hierarchical to: FCO\_NRO.1 Selective proof of origin

1609 Dependencies: FIA\_UID.1 Timing of identification

1610 **Application Note 11:** FCO\_NRO.2 requires that the TOE calculates a signature  
1611 over Meter Data that is submitted to external entities.

1612 Therefore, the TOE has to create a hash value over the  
1613 Data To Be Signed (DTBS) as defined in  
1614 FCS\_COP.1/HASH. The creation of the actual signature  
1615 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*]

## 1616 6.4 Class FCS: Cryptographic Support

### 1617 6.4.1 Cryptographic support for TLS

#### 1618 6.4.1.1 Cryptographic key management (FCS\_CKM)

##### 1619 **6.4.1.1.1 FCS\_CKM.1/TLS: Cryptographic key generation for TLS**

1620 FCS\_CKM.1.1/TLS The TSF shall generate cryptographic keys in accordance  
 1621 with a specified cryptographic key generation algorithm  
 1622 *TLS-PRF with SHA-256 or SHA-384*<sup>75</sup> and specified  
 1623 cryptographic key sizes *128 bit, 256 bit or 384 bit*<sup>76</sup> that  
 1624 meet the following: *[RFC 5246] in combination with*  
 1625 *[FIPS Pub. 180-4] and [RFC 2104]*<sup>77</sup>.

1626 Hierarchical to: No other components.

1627 Dependencies: [FCS\_CKM.2 Cryptographic key distribution, or  
 1628 FCS\_COP.1 Cryptographic operation], fulfilled by  
 1629 FCS\_COP.1/TLS

1630 FCS\_CKM.4 Cryptographic key destruction

1631 **Application Note 12:** The Security Module is used for the generation of random  
 1632 numbers and for all cryptographic operations with the pri-  
 1633 vate key of a TLS certificate.

1634 **Application Note 13:** The TOE uses only cryptographic specifications and  
 1635 algorithms as described in [TR-03109-3].

#### 1636 6.4.1.2 Cryptographic operation (FCS\_COP)

##### 1637 **6.4.1.2.1 FCS\_COP.1/TLS: Cryptographic operation for TLS**

1638 FCS\_COP.1.1/TLS The TSF shall perform *TLS encryption, decryption, and*  
 1639 *integrity protection*<sup>78</sup> in accordance with a specified  
 1640 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*]

1641 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,  
 1642 TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,  
 1643 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,  
 1644 and  
 1645 TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384  
 1646 <sup>79</sup> using elliptic curves BrainpoolP256r1, BrainpoolP384r1,  
 1647 BrainpoolP512r1 (according to [RFC 5639]), NIST P-256,  
 1648 and NIST P-384 (according to [RFC 5114]) and  
 1649 cryptographic key sizes 128 bit or 256 bit <sup>80</sup> that meet the  
 1650 following: [RFC 2104], [RFC 5114], [RFC 5246],  
 1651 [RFC 5289], [RFC 5639], [NIST 800-38A], and [NIST 800-  
 1652 38D]<sup>81</sup>.

1653 Hierarchical to: No other components.  
 1654 Dependencies: [FDP\_ITC.1 Import of user data without security attributes,  
 1655 or  
 1656 FDP\_ITC.2 Import of user data with security attributes, or  
 1657 FCS\_CKM.1 Cryptographic key generation], fulfilled by  
 1658 FCS\_CKM.1/TLS  
 1659 FCS\_CKM.4 Cryptographic key destruction

1660 **Application Note 14:** The TOE uses only cryptographic specifications and  
 1661 algorithms as described in [TR-03109-3].

## 1662 6.4.2 Cryptographic support for CMS

1663 6.4.2.1 Cryptographic key management (FCS\_CKM)

### 1664 6.4.2.1.1 FCS\_CKM.1/CMS: Cryptographic key generation for CMS

1665 FCS\_CKM.1.1/CMS The TSF shall generate cryptographic keys in accordance  
 1666 with a specified cryptographic key generation algorithm  
 1667 ECKA-EG<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*]

1668		<i>bit</i> <sup>83</sup> that meet the following: [X9.63] in combination with
1669		[RFC 3565] <sup>84</sup> .
1670	Hierarchical to:	No other components.
1671	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or
1672		FCS_COP.1 Cryptographic operation], fulfilled by
1673		FCS_COP.1/CMS
1674		FCS_CKM.4 Cryptographic key destruction
1675	<b>Application Note 15:</b>	The TOE utilises the services of its Security Module for the
1676		generation of random numbers and for all cryptographic
1677		operations with the private asymmetric key of a CMS cer-
1678		tificate.
1679	<b>Application Note 16:</b>	The TOE uses only cryptographic specifications and
1680		algorithms as described in [TR-03109-3].
1681		6.4.2.2 Cryptographic operation (FCS_COP)
1682		<b>6.4.2.2.1 FCS_COP.1/CMS: Cryptographic operation for CMS</b>
1683	FCS_COP.1.1/CMS	The TSF shall perform
1684		<i>symmetric encryption, decryption and integrity protection</i>
1685		in accordance with a specified cryptographic algorithm
1686		<i>AES-CBC-CMAC or AES-GCM</i> <sup>85</sup> and cryptographic key
1687		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*]

1688		<i>[NIST 800-38D], [RFC 4493], [RFC 5084], and [RFC 5652]</i>
1689		<i>in combination with [NIST 800-38A]<sup>87</sup>.</i>
1690	Hierarchical to:	No other components.
1691	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1692		or
1693		FDP_ITC.2 Import of user data with security attributes, or
1694		FCS_CKM.1 Cryptographic key generation], fulfilled by
1695		FCS_CKM.1/CMS
1696		FCS_CKM.4 Cryptographic key destruction
1697	<b>Application Note 17:</b>	The TOE uses only cryptographic specifications and
1698		algorithms as described in [TR-03109-3].
1699	<b>6.4.3 Cryptographic support for Meter communication encryption</b>	
1700	6.4.3.1 Cryptographic key management (FCS_CKM)	
1701	<b>6.4.3.1.1 FCS_CKM.1/MTR: Cryptographic key generation for Meter</b>	
1702	<b>communication (symmetric encryption)</b>	
1703	FCS_CKM.1.1/MTR	The TSF shall generate cryptographic keys in accordance
1704		with a specified cryptographic key generation algorithm
1705		<i>AES-CMAC<sup>88</sup> and specified cryptographic key sizes 128</i>
1706		<i>bit<sup>89</sup> that meet the following: [FIPS Pub. 197], and</i>
1707		<i>[RFC 4493]<sup>90</sup>.</i>
1708	Hierarchical to:	No other components.
1709	Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or
1710		FCS_COP.1 Cryptographic operation], fulfilled by
1711		FCS_COP.1/MTR
1712		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*]

1713	<b>Application Note 18:</b>	The TOE uses only cryptographic specifications and
1714		algorithms as described in [TR-03109-3].
1715		6.4.3.2 Cryptographic operation (FCS_COP)
1716	<b>6.4.3.2.1 FCS_COP.1/MTR: Cryptographic operation for Meter</b>	
1717	<b>communication encryption</b>	
1718	FCS_COP.1.1/MTR	The TSF shall perform symmetric encryption, decryption,
1719		integrity protection <sup>91</sup> in accordance with a specified
1720		cryptographic algorithm AES-CBC-CMAC <sup>92</sup> and
1721		cryptographic key sizes 128 bit <sup>93</sup> that meet the following:
1722		[FIPS Pub. 197] and [RFC 4493] in combination with
1723		[ISO 10116] <sup>94</sup> .
1724	Hierarchical to:	No other components.
1725	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1726		or
1727		FDP_ITC.2 Import of user data with security attributes, or
1728		FCS_CKM.1 Cryptographic key generation], fulfilled by
1729		FCS_CKM.1/MTR
1730		FCS_CKM.4 Cryptographic key destruction
1731	<b>Application Note 19:</b>	The ST allows different scenarios of key generation for
1732		Meter communication encryption. Those are:
1733		1. If a TLS encryption is being used, the key
1734		generation/negotiation is as defined by
1735		FCS_CKM.1/TLS.
1736		2. If AES encryption is being used, the key has been
1737		brought into the Gateway via a management
1738		function during the pairing process for the Meter

---

91 [assignment: *list of cryptographic operations*]

92 [assignment: *cryptographic algorithm*]

93 [assignment: *cryptographic key sizes*]

94 [assignment: *list of standards*]

1739 (see FMT\_SMF.1) as defined by  
1740 FCS\_COP.1/MTR.

1741 **Application Note 20:** If the connection between the Meter and TOE is  
1742 unidirectional, the communication between the Meter and  
1743 the TOE is secured by the use of a symmetric AES  
1744 encryption. If a bidirectional connection between the Meter  
1745 and the TOE is established, the communication is secured  
1746 by a TLS channel as described in chapter 6.4.1. As the  
1747 TOE shall be interoperable with all kind of Meters, both  
1748 kinds of encryption are implemented.

1749 **Application Note 21:** The TOE uses only cryptographic specifications and  
1750 algorithms as described in [TR-03109-3].

## 1751 6.4.4 General Cryptographic support

### 1752 6.4.4.1 Cryptographic key management (FCS\_CKM)

#### 1753 6.4.4.1.1 FCS\_CKM.4: Cryptographic key destruction

1754 FCS\_CKM.4.1 The TSF shall destroy cryptographic keys in accordance  
1755 with a specified cryptographic key destruction method  
1756 *Zeroisation*<sup>95</sup> that meets the following: *none*<sup>96</sup>.

1757 Hierarchical to: No other components.

1758 Dependencies: [FDP\_ITC.1 Import of user data without security attributes,  
1759 or

1760 FDP\_ITC.2 Import of user data with security attributes, or

1761 FCS\_CKM.1 Cryptographic key generation], fulfilled by  
1762 FCS\_CKM.1/TLS and

1763 FCS\_CKM.1/CMS and FCS\_CKM.1/MTR

1764 **Application Note 22:** Please note that as against the requirement FDP\_RIP.2,  
1765 the mechanisms implementing the requirement from  
1766 FCS\_CKM.4 shall be suitable to avoid attackers with

---

95 [assignment: *cryptographic key destruction method*]

96 [assignment: *list of standards*]

1767		physical access to the TOE from accessing the keys after
1768		they are no longer used.
1769	6.4.4.2 Cryptographic operation (FCS_COP)	
1770	<b>6.4.4.2.1 FCS_COP.1/HASH: Cryptographic operation, hashing for</b>	
1771	<b>signatures</b>	
1772	FCS_COP.1.1/HASH	The TSF shall perform <i>hashing for signature creation and</i>
1773		<i>verification</i> <sup>97</sup> in accordance with a specified cryptographic
1774		algorithm <i>SHA-256, SHA-384 and SHA-512</i> <sup>98</sup> and
1775		cryptographic key sizes <i>none</i> <sup>99</sup> that meet the following:
1776		<i>[FIPS Pub. 180-4]</i> <sup>100</sup> .
1777	Hierarchical to:	No other components.
1778	Dependencies:	[FDP_ITC.1 Import of user data without security attributes,
1779		or
1780		FDP_ITC.2 Import of user data with security attributes, or
1781		FCS_CKM.1 Cryptographic key generation <sup>101</sup> ]
1782		FCS_CKM.4 Cryptographic key destruction
1783	<b>Application Note 23:</b>	The TOE is only responsible for hashing of data in the
1784		context of digital signatures. The actual signature
1785		operation and the handling (i.e. protection) of the
1786		cryptographic keys in this context is performed by the
1787		Security Module.
1788	<b>Application Note 24:</b>	The TOE uses only cryptographic specifications and
1789		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.



## 1813 6.5 Class FDP: User Data Protection

### 1814 6.5.1 Introduction to the Security Functional Policies

1815 The security functional requirements that are used in the following chapters implicitly  
1816 define a set of Security Functional Policies (SFP). These policies are introduced in the  
1817 following paragraphs in more detail to facilitate the understanding of the SFRs:

- 1818 • The **Gateway access SFP** is an access control policy to control the access to  
1819 objects under the control of the TOE. The details of this access control policy  
1820 highly depend on the concrete application of the TOE. The access control policy  
1821 is described in more detail in [TR-03109-1].
- 1822 • The **Firewall SFP** implements an information flow policy to fulfil the objective  
1823 O.Firewall. All requirements around the communication control that the TOE  
1824 poses on communications between the different networks are defined in this  
1825 policy.
- 1826 • The **Meter SFP** implements an information flow policy to fulfil the objective  
1827 O.Meter. It defines all requirements concerning how the TOE shall handle Meter  
1828 Data.

### 1829 6.5.2 Gateway Access SFP

#### 1830 6.5.2.1 Access control policy (FDP\_ACC)

##### 1831 6.5.2.1.1 FDP\_ACC.2: Complete access control

1832 FDP\_ACC.2.1 The TSF shall enforce the *Gateway access SFP*<sup>106</sup> on  
1833 *subjects: external entities in WAN, HAN and LMN*  
1834 *objects: any information that is sent to, from or via*  
1835 *the TOE and any information that is stored in the*  
1836 *TOE*<sup>107</sup> and all operations among subjects and  
1837 objects covered by the SFP.

1838 FDP\_ACC.2.2 The TSF shall ensure that all operations between any  
1839 subject controlled by the TSF and any object controlled by  
1840 the TSF are covered by an access control SFP.

---

106 [assignment: *access control SFP*]

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

1841	Hierarchical to:	FDP_ACC.1 Subset access control
1842	Dependencies:	FDP_ACF.1 Security attribute based access control
1843	<b>6.5.2.1.2 FDP_ACF.1: Security attribute based access control</b>	
1844	FDP_ACF.1.1	The TSF shall enforce the <i>Gateway access SFP</i> <sup>108</sup> to
1845		objects based on the following:
1846		<i>subjects: external entities on the WAN, HAN or</i>
1847		<i>LMN side</i>
1848		<i>objects: any information that is sent to, from or via</i>
1849		<i>the TOE</i>
1850		<i>attributes: destination interface</i> <sup>109</sup> .
1851	FDP_ACF.1.2	The TSF shall enforce the following rules to determine if
1852		an operation among controlled subjects and controlled
1853		objects is allowed:
1854		• <i>an authorised Consumer is only allowed to have</i>
1855		<i>read access to his own User Data via the interface</i>
1856		<i>IF_GW_CON,</i>
1857		• <i>an authorised Service Technician is only allowed to</i>
1858		<i>have read access to the system log via the interface</i>
1859		<i>IF_GW_SRV, the Service Technician must not be</i>
1860		<i>allowed to read, modify or delete any other TSF</i>
1861		<i>data,</i>
1862		• <i>an authorised Gateway Administrator is allowed to</i>
1863		<i>interact with the TOE only via IF_GW_WAN,</i>
1864		• <i>only authorised Gateway Administrators are</i>
1865		<i>allowed to establish a wake-up call,</i>
1866		• <i>additional rules governing access among controlled</i>
1867		<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*]

1868		<i>operations on controlled objects or none:</i>
1869		<i>none</i> <sup>110, 111</sup>
1870	FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to
1871		objects based on the following additional rules: <i>none</i> <sup>112</sup> .
1872	FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects
1873		based on the following additional rules:
1874		<ul style="list-style-type: none"> <li>• <i>the Gateway Administrator is not allowed to read</i></li> </ul>
1875		<i>consumption data or the Consumer Log,</i>
1876		<ul style="list-style-type: none"> <li>• <i>nobody must be allowed to read the symmetric</i></li> </ul>
1877		<i>keys used for encryption</i> <sup>113</sup> .
1878	Hierarchical to:	No other components
1879	Dependencies:	FDP_ACC.1 Subset access control
1880		FMT_MSA.3 Static attribute initialisation
1881	<b>6.5.3 Firewall SFP</b>	
1882	6.5.3.1 Information flow control policy (FDP_IFC)	
1883	<b>6.5.3.1.1 FDP_IFC.2/FW: Complete information flow control for</b>	
1884	<b><i>firewall</i></b>	
1885	FDP_IFC.2.1/FW	The TSF shall enforce the <i>Firewall SFP</i> <sup>114</sup> on <i>the TOE,</i>
1886		<i>external entities on the WAN side, external entities on the</i>
1887		<i>LAN side and all information flowing between them</i> <sup>115</sup> and
1888		all operations that cause that information to flow to and
1889		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*]

1890 FDP\_IFC.2.2/FW The TSF shall ensure that all operations that cause any  
 1891 information in the TOE to flow to and from any subject in  
 1892 the TOE are covered by an information flow control SFP.

1893 Hierarchical to: FDP\_IFC.1 Subset information flow control

1894 Dependencies: FDP\_IFF.1 Simple security attributes

1895 6.5.3.2 Information flow control functions (FDP\_IFF)

### 1896 **6.5.3.2.1 FDP\_IFF.1/FW: Simple security attributes for Firewall**

1897 FDP\_IFF.1.1/FW The TSF shall enforce the *Firewall SFP*<sup>116</sup> based on the  
 1898 following types of subject and information security  
 1899 attributes:

1900 *subjects: The TOE and external entities on the*  
 1901 *WAN, HAN or LMN side*

1902 *information: any information that is sent to, from or*  
 1903 *via the TOE*

1904 *attributes: destination\_interface (TOE, LMN, HAN*  
 1905 *or WAN), source\_interface (TOE, LMN, HAN or*  
 1906 *WAN), destination\_authenticated,*  
 1907 *source\_authenticated*<sup>117</sup>.

1908 FDP\_IFF.1.2/FW The TSF shall permit an information flow between a  
 1909 controlled subject and controlled information via a  
 1910 controlled operation if the following rules hold:

1911 *(if source\_interface=HAN or*  
 1912 *source\_interface=TOE) and*

1913 *destination\_interface=WAN and*

1914 *destination\_authenticated = true*

1915 *Connection establishment is allowed*

1916

---

116 [assignment: *information flow control SFP*]

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

1917 *if source\_interface=LMN and*  
 1918 *destination\_interface= TOE and*  
 1919 *source\_authenticated = true*  
 1920 *Connection establishment is allowed*  
 1921  
 1922 *if source\_interface=TOE and*  
 1923 *destination\_interface= LMN and*  
 1924 *destination\_authenticated = true*  
 1925 *Connection establishment is allowed*  
 1926  
 1927 *if source\_interface=HAN and*  
 1928 *destination\_interface= TOE and*  
 1929 *source\_authenticated = true*  
 1930 *Connection establishment is allowed*  
 1931  
 1932 *if source\_interface=TOE and*  
 1933 *destination\_interface= HAN and*  
 1934 *destination\_authenticated = true*  
 1935 *Connection establishment is allowed*  
 1936 *else*  
 1937 *Connection establishment is denied*<sup>118</sup>.  
 1938 FDP\_IFF.1.3/FW The TSF shall enforce the *establishment of a connection*  
 1939 *to a configured external entity in the WAN after having*  
 1940 *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*]

1941	FDP_IFF.1.4/FW	The TSF shall explicitly authorise an information flow
1942		based on the following rules: <i>none</i> <sup>120</sup> .
1943	FDP_IFF.1.5/FW	The TSF shall explicitly deny an information flow based on
1944		the following rules: <i>none</i> <sup>121</sup> .
1945	Hierarchical to:	No other components
1946	Dependencies:	FDP_IFC.1 Subset information flow control
1947		FMT_MSA.3 Static attribute initialisation
1948	<b>Application Note 27:</b>	It should be noted that the FDP_IFF.1.1/FW facilitates
1949		different interfaces of the origin and the destination of an
1950		information flow implicitly requires the TOE to implement
1951		physically separate ports for WAN, LMN and HAN.
1952	<b>6.5.4 Meter SFP</b>	
1953	6.5.4.1 Information flow control policy (FDP_IFC)	
1954	<b>6.5.4.1.1 FDP_IFC.2/MTR: Complete information flow control for</b>	
1955	<b>Meter information flow</b>	
1956	FDP_IFC.2.1/MTR	The TSF shall enforce the <i>Meter SFP</i> <sup>122</sup> on <i>the TOE,</i>
1957		<i>attached Meters, authorized External Entities in the WAN</i>
1958		<i>and all information flowing between them</i> <sup>123</sup> and all
1959		operations that cause that information to flow to and from
1960		subjects covered by the SFP.
1961	FDP_IFC.2.2/MTR	The TSF shall ensure that all operations that cause any
1962		information in the TOE to flow to and from any subject in
1963		the TOE are covered by an information flow control SFP.
1964	Hierarchical to:	FDP_IFC.1 Subset information flow control
1965	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*]

1966	6.5.4.2 Information flow control functions (FDP_IFF)	
1967	<b>6.5.4.2.1 FDP_IFF.1/MTR: Simple security attributes for Meter</b>	
1968	<b>information</b>	
1969	FDP_IFF.1.1/MTR	The TSF shall enforce the <i>Meter SFP</i> <sup>124</sup> based on the
1970		following types of subject and information security
1971		attributes:
1972		<ul style="list-style-type: none"> <li>• <i>subjects: TOE, external entities in WAN, Meters located in LMN</i></li> </ul>
1973		
1974		<ul style="list-style-type: none"> <li>• <i>information: any information that is sent via the TOE</i></li> </ul>
1975		
1976		<ul style="list-style-type: none"> <li>• <i>attributes: destination interface, source interface (LMN or WAN), Processing Profile</i><sup>125</sup>.</li> </ul>
1977		
1978	FDP_IFF.1.2/MTR	The TSF shall permit an information flow between a
1979		controlled subject and controlled information via a
1980		controlled operation if the following rules hold:
1981		<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>
1982		
1983	FDP_IFF.1.3/MTR	The TSF shall enforce the following rules:
1984		<ul style="list-style-type: none"> <li>• Data received from Meters shall be processed as defined in the corresponding Processing Profiles,</li> </ul>
1985		
1986		<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>
1987		
1988		
1989		<ul style="list-style-type: none"> <li>• The internal system time shall be synchronised as follows:</li> </ul>
1990		

---

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*]

1991			○ <i>The TOE shall compare the system time to a</i>
1992			<i>reliable external time source every 24</i>
1993			<i>hours</i> <sup>127</sup> .
1994			○ <i>If the deviation between the local time and the</i>
1995			<i>remote time is acceptable</i> <sup>128</sup> , <i>the local system</i>
1996			<i>time shall be updated according to the remote</i>
1997			<i>time.</i>
1998			○ <i>If the deviation is not acceptable the TOE</i>
1999			<i>shall ensure that any following Meter Data is</i>
2000			<i>not used, stop operation</i> <sup>129</sup> <i>and</i>
2001			<i>inform a Gateway Administrator</i> <sup>130</sup> .
2002	FDP_IFF.1.4/MTR		The TSF shall explicitly authorise an information flow
2003			based on the following rules: <i>none</i> <sup>131</sup> .
2004	FDP_IFF.1.5/MTR		The TSF shall explicitly deny an information flow based on
2005			the following rules: <i>The TOE shall deny any acceptance of</i>
2006			<i>information by external entities in the LMN unless the</i>
2007			<i>authenticity, integrity and confidentiality of the Meter Data</i>
2008			<i>could be verified</i> <sup>132</sup> .
2009	Hierarchical to:		No other components
2010	Dependencies:		FDP_IFC.1 Subset information flow control
2011			FMT_MSA.3 Static attribute initialisation
2012	<b>Application Note 28:</b>		FDP_IFF.1.3 defines that the TOE shall update the local
2013			system time regularly with reliable external time sources if
2014			the deviation is acceptable. In the context of this
2015			functionality two aspects should be mentioned:

---

127 [assignment: *synchronization interval between 1 minute and 24 hours*]

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

129 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.

130 [assignment: *additional information flow control SFP rules*]

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

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

2016		<b>Reliability of external source</b>
2017		<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>
2018		
2019		
2020		
2021		
2022		
2023		
2024		
2025		
2026		
2027		<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>
2028		
2029		
2030		
2031		
2032		
2033		
2034		
2035		
2036		
2037		<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>
2038		
2039		
2040		
2041		
2042		
2043		
2044		
2045		

---

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

2046 received from the Meter. The TOE has two options to do  
2047 so:

- 2048 1. To implement a channel between the Meter and the  
2049 TOE using the functionality as described in  
2050 FCS\_COP.1/TLS.  
2051 2. To accept, decrypt and verify data that has been  
2052 encrypted by the Meter as required in  
2053 FCS\_COP.1/MTR if a wireless connection to the  
2054 meters is established.

2055 The latter possibility can be used only if a wireless  
2056 connection between the Meter and the TOE is established.

## 2057 **6.5.5 General Requirements on user data protection**

### 2058 6.5.5.1 Residual information protection (FDP\_RIP)

#### 2059 **6.5.5.1.1 FDP\_RIP.2: Full residual information protection**

2060 FDP\_RIP.2.1 The TSF shall ensure that any previous information  
2061 content of a resource is made unavailable upon the  
2062 deallocation of the resource from <sup>134</sup> all objects.

2063 Hierarchical to: FDP\_RIP.1 Subset residual information protection

2064 Dependencies: No dependencies.

2065 **Application Note 30:** Please refer to chapter F.9 of part 2 of [CC] for more  
2066 detailed information about what kind of information this  
2067 requirement applies to.

2068 Please further note that this SFR has been used in order  
2069 to ensure that information that is no longer used is made  
2070 unavailable from a logical perspective. Specifically, it has  
2071 to be ensured that this information is no longer available  
2072 via an external interface (even if an access control or  
2073 information flow policy would fail). However, this does not  
2074 necessarily mean that the information is overwritten in a

---

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

2075 way that makes it impossible for an attacker to get access  
 2076 to is assuming a physical access to the memory of the  
 2077 TOE.

2078 6.5.5.2 Stored data integrity (FDP\_SDI)

#### 2079 **6.5.5.2.1 FDP\_SDI.2: Stored data integrity monitoring and action**

2080 FDP\_SDI.2.1 The TSF shall monitor user data stored in containers  
 2081 controlled by the TSF for *integrity errors*<sup>135</sup> on all objects,  
 2082 based on the following attributes: *cryptographical check*  
 2083 *sum*<sup>136</sup>.

2084 FDP\_SDI.2.2 Upon detection of a data integrity error, the TSF shall  
 2085 *create a system log entry*<sup>137</sup>.

2086 Hierarchical to: FDP\_SDI.1 Stored data integrity monitoring

2087 Dependencies: No dependencies.

## 2088 **6.6 Class FIA: Identification and Authentication**

### 2089 **6.6.1 User Attribute Definition (FIA\_ATD)**

2090 6.6.1.1 FIA\_ATD.1: User attribute definition

2091 FIA\_ATD.1.1 The TSF shall maintain the following list of security  
 2092 attributes belonging to individual users:

- 2093 • *User Identity*
- 2094 • *Status of Identity (Authenticated or not)*
- 2095 • *Connecting network (WAN, HAN or LMN)*
- 2096 • *Role membership*
- 2097 • *none*<sup>138</sup>.

2098 Hierarchical to: No other components.

2099 Dependencies: No dependencies.

---

135 [assignment: *integrity errors*]

136 [assignment: *user data attributes*]

137 [assignment: *action to be taken*]

138 [assignment: *list of security attributes*]

2100	<b>6.6.2 Authentication Failures (FIA_AFL)</b>	
2101	6.6.2.1 FIA_AFL.1: Authentication failure handling	
2102	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> .
2103		
2104		
2105	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> .
2106		
2107		
2108	Hierarchical to:	No other components
2109	Dependencies:	FIA_UAU.1 Timing of authentication
2110	<b>6.6.3 User Authentication (FIA_UAU)</b>	
2111	6.6.3.1 FIA_UAU.2: User authentication before any action	
2112	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.
2113		
2114		
2115	Hierarchical to:	FIA_UAU.1
2116	Dependencies:	FIA_UID.1 Timing of identification
2117	<b>Application Note 31:</b>	Please refer to [TR-03109-1] for a more detailed overview on the authentication of TOE users.
2118		
2119	6.6.3.2 FIA_UAU.5: Multiple authentication mechanisms	
2120	FIA_UAU.5.1	The TSF shall provide
2121		<ul style="list-style-type: none"> <li>• <i>authentication via certificates at the IF_GW_MTR interface</i></li> </ul>
2122		
2123		<ul style="list-style-type: none"> <li>• <i>TLS-authentication via certificates at the IF_GW_WAN interface</i></li> </ul>
2124		

---

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]

- 2125 • *TLS-authentication via HAN-certificates at the*  
 2126 *IF\_GW\_CON interface*
- 2127 • *authentication via password at the IF\_GW\_CON*  
 2128 *interface*
- 2129 • *TLS-authentication via HAN-certificates at the*  
 2130 *IF\_GW\_SRV interface*
- 2131 • *authentication at the IF\_GW\_CLS interface*  
 2132 • *verification via a commands' signature*<sup>143</sup>
- 2133 to support user authentication.
- 2134 FIA\_UAU.5.2 The TSF shall authenticate any user's claimed identity  
 2135 according to the
- 2136 • *meters shall be authenticated via certificates at the*  
 2137 *IF\_GW\_MTR interface only*
- 2138 • *Gateway Administrators shall be authenticated via*  
 2139 *TLS-certificates at the IF\_GW\_WAN interface only*
- 2140 • *Consumers shall be authenticated via TLS-*  
 2141 *certificates or via password at the IF\_GW\_CON*  
 2142 *interface only*
- 2143 • *Service Technicians shall be authenticated via*  
 2144 *TLS-certificates at the IF\_GW\_SRV interface only*
- 2145 • *CLS shall be authenticated at the IF\_GW\_CLS only*  
 2146 • *each command of an Gateway Administrator shall*  
 2147 *be authenticated by verification of the commands'*  
 2148 *signature,*
- 2149 • *other external entities shall be authenticated via*  
 2150 *TLS-certificates at the IF\_GW\_WAN interface*  
 2151 *only*<sup>144</sup>.

---

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

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

2152	Hierarchical to:	No other components.
2153	Dependencies:	No dependencies.
2154	<b>Application Note 32:</b>	Please refer to [TR-03109-1] for a more detailed overview
2155		on the authentication of TOE users.
2156	6.6.3.3 FIA_UAU.6: Re-authenticating	
2157	FIA_UAU.6.1	The TSF shall re-authenticate <b>an external entity</b> <sup>145</sup> under
2158		the conditions
2159		<ul style="list-style-type: none"> <li>• <i>TLS channel to the WAN shall be disconnected</i></li> </ul>
2160		<i>after 48 hours,</i>
2161		<ul style="list-style-type: none"> <li>• <i>TLS channel to the LMN shall be disconnected after</i></li> </ul>
2162		<i>5 MB of transmitted information,</i>
2163		<ul style="list-style-type: none"> <li>• <i>other local users shall be re-authenticated after at</i></li> </ul>
2164		<i>least 10 minutes</i> <sup>146</sup> <i>of inactivity</i> <sup>147</sup> .
2165	Hierarchical to:	No other components.
2166	Dependencies:	No dependencies.
2167	<b>Application Note 33:</b>	This requirement on re-authentication for external entities
2168		in the WAN and LMN is addressed by disconnecting the
2169		TLS channel even though a re-authentication is - strictly
2170		speaking - only achieved if the TLS channel is build up
2171		again.
2172	<b>6.6.4 User identification (FIA_UID)</b>	
2173	6.6.4.1 FIA_UID.2: User identification before any action	
2174	FIA_UID.2.1	The TSF shall require each user to be successfully
2175		identified before allowing any other TSF-mediated actions
2176		on behalf of that user.
2177	Hierarchical to:	FIA_UID.1
2178	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*]

2179	<b>6.6.5 User-subject binding (FIA_USB)</b>	
2180	6.6.5.1 FIA_USB.1: User-subject binding	
2181	FIA_USB.1.1	The TSF shall associate the following user security
2182		attributes with subjects acting on the behalf of that user:
2183		<i>attributes as defined in FIA_ATD.1 <sup>148</sup>.</i>
2184	FIA_USB.1.2	The TSF shall enforce the following rules on the initial
2185		association of user security attributes with subjects acting
2186		on the behalf of users:
2187		<ul style="list-style-type: none"><li>• <i>The initial value of the security attribute ‘connecting</i></li></ul>
2188		<i>network’ is set to the corresponding physical</i>
2189		<i>interface of the TOE (HAN, WAN, or LMN).</i>
2190		<ul style="list-style-type: none"><li>• <i>The initial value of the security attribute ‘role</i></li></ul>
2191		<i>membership’ is set to the user role claimed on basis</i>
2192		<i>of the credentials used for authentication at the</i>
2193		<i>connecting network as defined in FIA_UAU.5.2. For</i>
2194		<i>role membership ‘Gateway Administrators’,</i>
2195		<i>additionally the remote network endpoint <sup>149</sup>used</i>
2196		<i>and configured in the TSF data must be identical.</i>
2197		<ul style="list-style-type: none"><li>• <i>The initial value of the security attribute ‘user</i></li></ul>
2198		<i>identity’ is set to the identification attribute of the</i>
2199		<i>credentials used by the subject. The security</i>
2200		<i>attribute ‘user identity’ is set to the subject key ID of</i>
2201		<i>the certificate in case of a certificate-based</i>
2202		<i>authentication, the meter-ID for wired Meters and</i>
2203		<i>the user name owner in case of a password-based</i>
2204		<i>authentication at interface IF_GW_CON.</i>
2205		<ul style="list-style-type: none"><li>• <i>The initial value of the security attribute ‘status of</i></li></ul>
2206		<i>identity’ is set to the authentication status of the</i>
2207		<i>claimed identity. If the authentication is successful</i>
2208		<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.

2209 *identity is 'authenticated', otherwise it is*  
 2210 *'not authenticated'* <sup>150</sup>.

2211 FIA\_USB.1.3 The TSF shall enforce the following rules governing  
 2212 changes to the user security attributes associated with  
 2213 subjects acting on the behalf of users:

- 2214 • *security attribute 'connecting network' is not*  
 2215 *changeable.*
- 2216 • *security attribute 'role membership' is not*  
 2217 *changeable.*
- 2218 • *security attribute 'user identity' is not changeable.*
- 2219 • *security attribute 'status of identity' is not*  
 2220 *changeable*<sup>151</sup>.

2221 Hierarchical to: No other components.

2222 Dependencies: FIA\_ATD.1 User attribute definition

## 2223 **6.7 Class FMT: Security Management**

### 2224 **6.7.1 Management of the TSF**

#### 2225 6.7.1.1 Management of functions in TSF (FMT\_MOF)

##### 2226 **6.7.1.1.1 FMT\_MOF.1: Management of security functions** 2227 ***behaviour***

2228 FMT\_MOF.1.1 The TSF shall restrict the ability to modify the behaviour  
 2229 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*]

- 2230 *FMT\_SMF.1* <sup>153</sup> to roles and criteria as defined in Table
- 2231 13 <sup>154</sup>.
- 2232 Hierarchical to: No other components.
- 2233 Dependencies: *FMT\_SMR.1* Security roles
- 2234 *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.

2235 **Table 13: Restrictions on Management Functions**

<sup>153</sup> [assignment: *list of functions*]

<sup>154</sup> [assignment: *the authorised identified roles*]

<sup>155</sup> 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.

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

2236 6.7.1.2 Specification of Management Functions (FMT\_SMF)

2237 **6.7.1.2.1 FMT\_SMF.1: Specification of Management Functions**

2238 FMT\_SMF.1.1 The TSF shall be capable of performing the following  
 2239 management functions: *list of management functions as*  
 2240 *defined in Table 14 and Table 15 and additional*  
 2241 *functionalities: none*<sup>157</sup>.

2242 Hierarchical to: No other components.

2243 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>

<sup>163</sup> 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.

<sup>164</sup> 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.

<sup>165</sup> 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.

<sup>166</sup> 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.

<sup>167</sup> 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

2244

**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.

2245

<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>

2246

**Table 15: Gateway specific Management Functionalities**

2247

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

2248

6.7.2.1 FMT\_SMR.1: Security roles

2249

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>.

2250

2251

2252

2253

FMT\_SMR.1.2

The TSF shall be able to associate users with roles.

2254

Hierarchical to:

No other components.

2255

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*]

2256	<b>6.7.3 Management of security attributes for Gateway access SFP</b>	
2257	6.7.3.1 Management of security attributes (FMT_MSA)	
2258	<b>6.7.3.1.1 FMT_MSA.1/AC: Management of security attributes for</b>	
2259	<b>Gateway access SFP</b>	
2260	FMT_MSA.1.1/AC	The TSF shall enforce the <i>Gateway access SFP</i> <sup>175</sup> to
2261		restrict the ability to <u>query, modify, delete, other</u>
2262		<u>operations: none</u> <sup>176</sup> the security attributes <i>all relevant</i>
2263		<i>security attributes</i> <sup>177</sup> to <i>authorised Gateway</i>
2264		<i>Administrators</i> <sup>178</sup> .
2265	Hierarchical to:	No other components.
2266	Dependencies:	[FDP_ACC.1 Subset access control, or
2267		FDP_IFC.1 Subset information flow control], fulfilled by
2268		FDP_ACC.2
2269		FMT_SMR.1 Security roles
2270		FMT_SMF.1 Specification of Management Functions
2271	<b>6.7.3.1.2 FMT_MSA.3/AC: Static attribute initialisation for Gateway</b>	
2272	<b>access SFP</b>	
2273	FMT_MSA.3.1/AC	The TSF shall enforce the <i>Gateway access SFP</i> <sup>179</sup> to
2274		provide <u>restrictive</u> <sup>180</sup> default values for security attributes
2275		that are used to enforce the SFP.
2276	FMT_MSA.3.2/AC	The TSF shall allow the <i>no role</i> <sup>181</sup> to specify alternative
2277		initial values to override the default values when an object
2278		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*]

2279	Hierarchical to:	No other components.
2280	Dependencies:	FMT_MSA.1 Management of security attributes
2281		FMT_SMR.1 Security roles
2282	<b>6.7.4 Management of security attributes for Firewall SFP</b>	
2283	6.7.4.1 Management of security attributes (FMT_MSA)	
2284	<b>6.7.4.1.1 FMT_MSA.1/FW: Management of security attributes for</b>	
2285	<b>firewall policy</b>	
2286	FMT_MSA.1.1/FW	The TSF shall enforce the <i>Firewall SFP</i> <sup>182</sup> to restrict the
2287		ability to <u>query, modify, delete, other operations: none</u> <sup>183</sup>
2288		the security attributes <i>all relevant security attributes</i> <sup>184</sup> to
2289		<i>authorised Gateway Administrators</i> <sup>185</sup> .
2290	Hierarchical to:	No other components.
2291	Dependencies:	[FDP_ACC.1 Subset access control, or
2292		FDP_IFC.1 Subset information flow control], fulfilled by
2293		FDP_IFC.2/FW
2294		FMT_SMR.1 Security roles
2295		FMT_SMF.1 Specification of Management Functions
2296	<b>6.7.4.1.2 FMT_MSA.3/FW: Static attribute initialisation for Firewall</b>	
2297	<b>policy</b>	
2298	FMT_MSA.3.1/FW	The TSF shall enforce the <i>Firewall SFP</i> <sup>186</sup> to provide
2299		<u>restrictive</u> <sup>187</sup> default values for security attributes that are
2300		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]*]

2301	FMT_MSA.3.2/FW	The TSF shall allow the <i>no role</i> <sup>188</sup> to specify alternative
2302		initial values to override the default values when an object
2303		or information is created.
2304	Hierarchical to:	No other components.
2305	Dependencies:	FMT_MSA.1 Management of security attributes
2306		FMT_SMR.1 Security roles
2307	<b>Application Note 34:</b>	The definition of restrictive default rules for the firewall
2308		information flow policy refers to the rules as defined in
2309		FDP_IFF.1.2/FW and FDP_IFF.1.5/FW. Those rules apply
2310		to all information flows and must not be overwritable by
2311		anybody.
2312	<b>6.7.5 Management of security attributes for Meter SFP</b>	
2313	6.7.5.1 Management of security attributes (FMT_MSA)	
2314	<b>6.7.5.1.1 FMT_MSA.1/MTR: Management of security attributes for</b>	
2315	<b>Meter policy</b>	
2316	FMT_MSA.1.1/MTR	The TSF shall enforce the <i>Meter SFP</i> <sup>189</sup> to restrict the
2317		ability to <u>change default, query, modify, delete, other</u>
2318		<u>operations: none</u> <sup>190</sup> the security attributes <i>all relevant</i>
2319		<i>security attributes</i> <sup>191</sup> to <i>authorised Gateway</i>
2320		<i>Administrators</i> <sup>192</sup> .
2321	Hierarchical to:	No other components.
2322	Dependencies:	[FDP_ACC.1 Subset access control, or
2323		FDP_IFC.1 Subset information flow control], fulfilled by
2324		FDP_IFC.2/FW
2325		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*]

2326		FMT_SMF.1 Specification of Management Functions
2327	<b>6.7.5.1.2</b>	<b><i>FMT_MSA.3/MTR: Static attribute initialisation for Meter</i></b>
2328		<b><i>policy</i></b>
2329	FMT_MSA.3.1/MTR	The TSF shall enforce the <i>Meter SFP</i> <sup>193</sup> to provide
2330		<u>restrictive</u> <sup>194</sup> default values for security attributes that are
2331		used to enforce the SFP.
2332	FMT_MSA.3.2/MTR	The TSF shall allow the <i>no role</i> <sup>195</sup> to specify alternative
2333		initial values to override the default values when an object
2334		or information is created.
2335	Hierarchical to:	No other components.
2336	Dependencies:	FMT_MSA.1 Management of security attributes
2337		FMT_SMR.1 Security roles
2338		
2339	<b>6.8 Class FPR: Privacy</b>	
2340	<b>6.8.1 Communication Concealing (FPR_CON)</b>	
2341	6.8.1.1 FPR_CON.1: Communication Concealing	
2342	FPR_CON.1.1	The TSF shall enforce the <i>Firewall SFP</i> <sup>196</sup> in order to
2343		ensure that no personally identifiable information (PII) can
2344		be obtained by an analysis of <i>frequency, load, size or the</i>
2345		<i>absence of external communication</i> <sup>197</sup> .
2346	FPR_CON.1.2	The TSF shall connect to <i>the Gateway Administrator,</i>
2347		<i>authorized External Entity in the WAN</i> <sup>198</sup> in intervals as

---

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

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

195 [assignment: *the authorised identified roles*]

196 [assignment: *information flow policy*]

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

198 [assignment: *list of external entities*]

2348		follows <u>daily, other interval: none</u> <sup>199</sup> to conceal the data
2349		flow <sup>200</sup> .
2350	Hierarchical to:	No other components.
2351	Dependencies:	No dependencies.
2352	<b>6.8.2 Pseudonymity (FPR_PSE)</b>	
2353	6.8.2.1 FPR_PSE.1 Pseudonymity	
2354	FPR_PSE.1.1	The TSF shall ensure that <i>external entities in the WAN</i> <sup>201</sup>
2355		are unable to determine the real user name bound to
2356		<i>information neither relevant for billing nor for a secure</i>
2357		<i>operation of the Grid sent to parties in the WAN</i> <sup>202</sup> .
2358	FPR_PSE.1.2	The TSF shall be able to provide <i>aliases as defined by the</i>
2359		<i>Processing Profiles</i> <sup>203</sup> <del>of the real user name for the</del>
2360		<b>Meter and Gateway identity</b> <sup>204</sup> to <i>external entities in the</i>
2361		<i>WAN</i> <sup>205</sup> .
2362	FPR_PSE.1.3	The TSF shall <u>determine an alias for a user</u> <sup>206</sup> and verify
2363		that it conforms to the <i>alias given by the Gateway</i>
2364		<i>Administrator in the Processing Profile</i> <sup>207</sup> .
2365	Hierarchical to:	No other components.
2366	Dependencies:	No dependencies.
2367	<b>Application Note 35:</b>	When the TOE submits information about the consumption
2368		or production of a certain commodity that is not relevant for
2369		the billing process nor for a secure operation of the Grid,
2370		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*]

2371 link to the identity of the consumer. In those cases, the  
 2372 TOE shall replace the identity of the Consumer by a  
 2373 pseudonymous identifier. Please note that the identity of  
 2374 the Consumer may not be their name but could also be a  
 2375 number (e.g. consumer ID) used for billing purposes.

2376 A Gateway may use more than one pseudonymous  
 2377 identifier.

2378 A complete anonymisation would be beneficial in terms of  
 2379 the privacy of the consumer. However, a complete  
 2380 anonymous set of information would not allow the external  
 2381 entity to ensure that the data comes from a trustworthy  
 2382 source.

2383 Please note that an information flow shall only be initiated  
 2384 if allowed by a corresponding Processing Profile.

2385

## 2386 **6.9 Class FPT: Protection of the TSF**

### 2387 **6.9.1 Fail secure (FPT\_FLS)**

2388 6.9.1.1 FPT\_FLS.1: Failure with preservation of secure state

2389 FPT\_FLS.1.1 The TSF shall preserve a secure state when the following  
 2390 types of failures occur:

- 2391 • *the deviation between local system time of the TOE*
- 2392 *and the reliable external time source is too large,*
- 2393 • *TOE hardware / firmware integrity violation or*
- 2394 • *TOE software application integrity violation* <sup>208</sup>.

2395 Hierarchical to: No other components.

2396 Dependencies: No dependencies.

2397 **Application Note 36:** The local clock shall be as exact as required by normative  
 2398 or legislative regulations. If no regulation exists, a

---

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

2399 maximum deviation of 3% of the measuring period is  
 2400 allowed to be in conformance with [PP\_GW].

## 2401 **6.9.2 Replay Detection (FPT\_RPL)**

### 2402 6.9.2.1 FPT\_RPL.1: Replay detection

2403 FPT\_RPL.1.1 The TSF shall detect replay for the following entities: *all*  
 2404 *external entities* <sup>209</sup>.

2405 FPT\_RPL.1.2 The TSF shall perform *ignore replayed data* <sup>210</sup> when  
 2406 replay is detected.

2407 Hierarchical to: No other components.

2408 Dependencies: No dependencies.

## 2409 **6.9.3 Time stamps (FPT\_STM)**

### 2410 6.9.3.1 FPT\_STM.1: Reliable time stamps

2411 FPT\_STM.1.1 The TSF shall be able to provide reliable time stamps.

2412 Hierarchical to: No other components.

2413 Dependencies: No dependencies.

2414

## 2415 **6.9.4 TSF self test (FPT\_TST)**

### 2416 6.9.4.1 FPT\_TST.1: TSF testing

2417 FPT\_TST.1.1 The TSF shall run a suite of self tests during initial startup,  
 2418 at the request of a user and periodically during normal  
 2419 operation <sup>211</sup> to demonstrate the correct operation of the  
 2420 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*]

2421	FPT_TST.1.2	The TSF shall provide authorised users with the capability
2422		to verify the integrity of <u>TSF data</u> <sup>213</sup> .
2423	FPT_TST.1.3	The TSF shall provide authorised users with the capability
2424		to verify the integrity of <u>TSF</u> <sup>214</sup> .
2425	Hierarchical to:	No other components.
2426	Dependencies:	No dependencies.

## 2427 **6.9.5 TSF physical protection (FPT\_PHP)**

### 2428 6.9.5.1 FPT\_PHP.1: Passive detection of physical attack

2429	FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical
2430		tampering that might compromise the TSF.
2431	FPT_PHP.1.2	The TSF shall provide the capability to determine whether
2432		physical tampering with the TSF's devices or TSF
2433		elements has occurred.
2434	Hierarchical to:	No other components.
2435	Dependencies:	No dependencies.

2436

## 2437 **6.10 Class FTP: Trusted path/channels**

### 2438 **6.10.1 Inter-TSF trusted channel (FTP\_ITC)**

#### 2439 6.10.1.1 FTP\_ITC.1/WAN: Inter-TSF trusted channel for WAN

2440	FTP_ITC.1.1/WAN	The TSF shall provide a communication channel between
2441		itself and another trusted IT product that is logically distinct
2442		from other communication channels and provides assured
2443		identification of its end points and protection of the channel
2444		data from modification or disclosure.

---

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

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

2445	FTP_ITC.1.2/WAN	The TSF shall permit <u>the TSF</u> <sup>215</sup> to initiate communication
2446		via the trusted channel.
2447	FTP_ITC.1.3/WAN	The TSF shall initiate communication via the trusted
2448		channel for <i>all communications to external entities in the</i>
2449		<i>WAN</i> <sup>216</sup> .
2450	Hierarchical to:	No other components
2451	Dependencies:	No dependencies.
2452	6.10.1.2      FTP_ITC.1/MTR:	Inter-TSF trusted channel for Meter
2453	FTP_ITC.1.1/MTR	The TSF shall provide a communication channel between
2454		itself and another trusted IT product that is logically distinct
2455		from other communication channels and provides assured
2456		identification of its end points and protection of the channel
2457		data from modification or disclosure.
2458	FTP_ITC.1.2/MTR	The TSF shall permit <b>the Meter and the TOE</b> <sup>217</sup> to initiate
2459		communication via the trusted channel.
2460	FTP_ITC.1.3/MTR	The TSF shall initiate communication via the trusted
2461		channel for <i>any communication between a Meter and the</i>
2462		<i>TOE</i> <sup>218</sup> .
2463	Hierarchical to:	No other components.
2464	Dependencies:	No dependencies.
2465	<b>Application Note 37:</b>	The corresponding cryptographic primitives are defined by
2466		FCS_COP.1/MTR.
2467	6.10.1.3      FTP_ITC.1/USR:	Inter-TSF trusted channel for User
2468	FTP_ITC.1.1/USR	The TSF shall provide a communication channel between
2469		itself and another trusted IT product that is logically distinct
2470		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*]

2471 identification of its end points and protection of the channel  
 2472 data from modification or disclosure.

2473 FTP\_ITC.1.2/USR The TSF shall permit **the Consumer, the Service**  
 2474 **Technician** <sup>219</sup> to initiate communication via the trusted  
 2475 channel.

2476 FTP\_ITC.1.3/USR The TSF shall initiate communication via the trusted  
 2477 channel for *any communication between a Consumer and*  
 2478 *the TOE and the Service Technician and the TOE* <sup>220</sup>.

2479 Hierarchical to: No other components.

2480 Dependencies: No dependencies.

2481

2482 **6.11 Security Assurance Requirements for the TOE**

2483 The minimum Evaluation Assurance Level for this Security Target is **EAL 4 augmented**  
 2484 **by AVA\_VAN.5 and ALC\_FLR.2**. The following table lists the assurance components  
 2485 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>

2487 **6.11.1 Refinement for ALC\_DEL.1 for the following assurance elements**

2488 ALC\_DEL.1.1D: The developer shall document and provide procedures for delivery of

2489 the TOE or parts of it to the **consumer MPO**.

2490 ALC\_DEL.1.1C: The delivery documentation shall describe all procedures that are nec-

2491 essary to maintain security when distributing versions of the TOE to the **consumer MPO**.

2492 Application Note: "MPO" as the recipient of the TOE delivery is to be understood to also

2493 include service technicians or any other agent who act as a contractor on behalf of the

2494 MPO.

2495

2496 **6.12 Security Requirements rationale**

2497 **6.12.1 Security Functional Requirements rationale**

2498 6.12.1.1 Fulfilment of the Security Objectives

2499 This chapter proves that the set of security requirements (TOE) is suited to fulfil the

2500 security objectives described in chapter 4 and that each SFR can be traced back to the

2501 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	

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
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						
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								

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
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		
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		

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
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			
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	

2502 **Table 17: Fulfilment of Security Objectives**

2503 The following paragraphs contain more details on this mapping.

2504 **6.12.1.1.1 O.Firewall**

2505 O.Firewall is met by a combination of the following SFRs:

- 2506 • **FDP\_IFC.2/FW** defines that the TOE shall implement an information flow policy
- 2507 for its firewall functionality.
- 2508 • **FDP\_IFF.1/FW** defines the concrete rules for the firewall information flow policy.

- 2509           • **FTP\_ITC.1/WAN** defines the policy around the trusted channel to parties in the  
2510           WAN.

#### 2511           **6.12.1.1.2 O.SeparateIF**

2512           O.SeparateIF is met by a combination of the following SFRs:

- 2513           • **FDP\_IFC.2/FW** and **FDP\_IFF.1/FW** implicitly require the TOE to implement  
2514           physically separate ports for WAN and LMN.  
2515           • **FPT\_TST.1** implements a self test that also detects whether the ports for WAN  
2516           and LAN have been interchanged.

#### 2517           **6.12.1.1.3 O.Conceal**

2518           O.Conceal is completely met by **FPR\_CON.1** as directly follows.

#### 2519           **6.12.1.1.4 O.Meter**

2520           O.Meter is met by a combination of the following SFRs:

- 2521           • **FDP\_IFC.2/MTR** and **FDP\_IFF.1/MTR** define an information flow policy to  
2522           introduce how the Gateway shall handle Meter Data.  
2523           • **FCO\_NRO.2** ensure that all Meter Data will be signed by the Gateway (invoking  
2524           the services of its Security Module) before being submitted to external entities.  
2525           • **FPR\_PSE.1** defines requirements around the pseudonymization of Meter  
2526           identities for Status data.  
2527           • **FTP\_ITC.1/MTR** defines the requirements around the Trusted Channel that  
2528           shall be implemented by the Gateway in order to protect information submitted  
2529           via the Gateway and external entities in the WAN or the Gateway and a  
2530           distributed Meter.

2531

2532 **6.12.1.1.5 O.Crypt**

2533 O.Crypt is met by a combination of the following SFRs:

- 2534 • **FCS\_CKM.4** defines the requirements around the secure deletion of ephemeral  
2535 cryptographic keys.
- 2536 • **FCS\_CKM.1/TLS** defines the requirements on key negotiation for the TLS  
2537 protocol.
- 2538 • **FCS\_CKM.1/CMS** defines the requirements on key generation for symmetric  
2539 encryption within CMS.
- 2540 • **FCS\_COP.1/TLS** defines the requirements around the encryption and  
2541 decryption capabilities of the Gateway for communications with external parties  
2542 and to Meters.
- 2543 • **FCS\_COP.1/CMS** defines the requirements around the encryption and  
2544 decryption of content and administration data.
- 2545 • **FCS\_CKM.1/MTR** defines the requirements on key negotiation for meter com-  
2546 munication encryption.
- 2547 • **FCS\_COP.1/MTR** defines the cryptographic primitives for meter  
2548 communication encryption.
- 2549 • **FCS\_COP.1/HASH** defines the requirements on hashing that are needed in the  
2550 context of digital signatures (which are created and verified by the Security  
2551 Module).
- 2552 • **FCS\_COP.1/MEM** defines the requirements around the encryption of TSF data.
- 2553 • **FPT\_RPL.1** ensures that a replay attack for communications with external  
2554 entities is detected.

2555 **6.12.1.1.6 O.Time**

2556 O.Time is met by a combination of the following SFRs:

- 2557 • **FDP\_IFC.2/MTR** and **FDP\_IFF.1/MTR** define the required update functionality  
2558 for the local time as part of the information flow control policy for handling Meter  
2559 Data.
- 2560 • **FPT\_STM.1** defines that the TOE shall be able to provide reliable time stamps.

2561

2562 **6.12.1.1.7 O.Protect**

2563 O.Protect is met by a combination of the following SFRs:

- 2564 • **FCS\_COP.1/MEM** defines that the TOE shall encrypt its TSF and user data as  
2565 long as it is not in use.
- 2566 • **FDP\_RIP.2** defines that the TOE shall make information unavailable as soon  
2567 as it is no longer needed.
- 2568 • **FDP\_SDI.2** defines requirements around the integrity protection for stored data.
- 2569 • **FPT\_FLS.1** defines requirements that the TOE falls back to a safe state for  
2570 specific error cases.
- 2571 • **FPT\_TST.1** defines the self testing functionality to detect whether the interfaces  
2572 for WAN and LAN are separate.
- 2573 • **FPT\_PHP.1** defines the exact requirements around the physical protection that  
2574 the TOE has to provide.

2575 **6.12.1.1.8 O.Management**

2576 O.Management is met by a combination of the following SFRs:

- 2577 • **FIA\_ATD.1** defines the attributes for users.
- 2578 • **FIA\_AFL.1** defines the requirements if the authentication of users fails multiple  
2579 times.
- 2580 • **FIA\_UAU.2** defines requirements around the authentication of users.
- 2581 • **FIA\_UID.2** defines requirements around the identification of users.
- 2582 • **FIA\_USB.1** defines that the TOE must be able to associate users with subjects  
2583 acting on behalf of them.
- 2584 • **FMT\_MOF.1** defines requirements around the limitations for management of  
2585 security functions.
- 2586 • **FMT\_MSA.1/AC** defines requirements around the limitations for management  
2587 of attributes used for the Gateway access SFP.
- 2588 • **FMT\_MSA.1/FW** defines requirements around the limitations for management  
2589 of attributes used for the Firewall SFP.
- 2590 • **FMT\_MSA.1/MTR** defines requirements around the limitations for management  
2591 of attributes used for the Meter SFP.
- 2592 • **FMT\_MSA.3/AC** defines the default values for the Gateway access SFP.
- 2593 • **FMT\_MSA.3/FW** defines the default values for the Firewall SFP.
- 2594 • **FMT\_MSA.3/MTR** defines the default values for the Meter SFP.

- 2595
- **FMT\_SMF.1** defines the management functionalities that the TOE must offer.
- 2596
- **FMT\_SMR.1** defines the role concept for the TOE.

2597

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

2598 O.Log defines that the TOE shall implement three different audit processes that are  
2599 covered by the Security Functional Requirements as follows:

2600

##### **System Log**

2601 The implementation of the system log itself is covered by the use of **FAU\_GEN.1/SYS**.  
2602 **FAU\_ARP.1/SYS** and **FAU\_SAA.1/SYS** allow to define a set of criteria for automated  
2603 analysis of the audit and a corresponding response. **FAU\_SAR.1/SYS** defines the  
2604 requirements around the audit review functions and that access to them shall be limited  
2605 to authorised Gateway Administrators via the IF\_GW\_WAN interface and to authorised  
2606 Service Technicians via the IF\_GW\_SRV interface. Finally, **FAU\_STG.4/SYS** defines  
2607 the requirements on what should happen if the audit log is full.

2608

##### **Consumer Log**

2609 The implementation of the consumer log itself is covered by the use of  
2610 **FAU\_GEN.1/CON**. **FAU\_STG.4/CON** defines the requirements on what should happen  
2611 if the audit log is full. **FAU\_SAR.1/CON** defines the requirements around the audit review  
2612 functions for the consumer log and that access to them shall be limited to authorised  
2613 Consumer via the IF\_GW\_CON interface. **FTP\_ITC.1/USR** defines the requirements on  
2614 the protection of the communication of the Consumer with the TOE.

2615

##### **Calibration Log**

2616 The implementation of the calibration log itself is covered by the use of  
2617 **FAU\_GEN.1/CAL**. **FAU\_STG.4/CAL** defines the requirements on what should happen  
2618 if the audit log is full. **FAU\_SAR.1/CAL** defines the requirements around the audit review  
2619 functions for the calibration log and that access to them shall be limited to authorised  
2620 Gateway Administrators via the IF\_GW\_WAN interface.

2621 **FAU\_GEN.2**, **FAU\_STG.2** and **FPT\_STM.1** apply to all three audit processes.

2622

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

2623 **FDP\_ACC.2** and **FDP\_ACF.1** define the access control policy as required to address  
2624 O.Access. **FIA\_UAU.5** ensures that entities that would like to communicate with the TOE  
2625 are authenticated before any action whereby **FIA\_UAU.6** ensures that external entities

2626 in the WAN are re-authenticated after the session key has been used for a certain  
 2627 amount of time.

2628 6.12.1.2 Fulfilment of the dependencies

2629 The following table summarises all TOE functional requirements dependencies of this  
 2630 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	-	-

2631 **Table 18: SFR Dependencies**

2632 6.12.1.3 Justification for missing dependencies

2633 Dependency FCS\_CKM.1 for FCS\_COP.1/MEM ist not fulfilled. For the key generation  
 2634 process an external security module (“D-HSM”) is used so that the key is imported from  
 2635 an HSM during TOE production.

2636 The hash algorithm as defined in FCS\_COP.1/HASH does not need any key material.  
 2637 As such the dependency to an import or generation of key material is omitted for this  
 2638 SFR.

2639 **6.12.2 Security Assurance Requirements rationale**

2640 The decision on the assurance level has been mainly driven by the assumed attack  
 2641 potential. As outlined in the previous chapters of this Security Target it is assumed that  
 2642 – at least from the WAN side – a high attack potential is posed against the security  
 2643 functions of the TOE. This leads to the use of AVA\_VAN.5 (Resistance against high  
 2644 attack potential).

2645 In order to keep evaluations according to this Security Target commercially feasible EAL  
 2646 4 has been chosen as assurance level as this is the lowest level that provides the  
 2647 prerequisites for the use of AVA\_VAN.5.

2648 Eventually, the augmentation by ALC\_FLR.2 has been chosen to emphasize the  
 2649 importance of a structured process for flaw remediation at the developer’s side,  
 2650 specifically for such a new technology.

2651 6.12.2.1 Dependencies of assurance components

2652 The dependencies of the assurance requirements taken from EAL 4 are fulfilled  
 2653 automatically. The augmentation by AVA\_VAN.5 and ALC\_FLR.2 does not introduce  
 2654 additional assurance components that are not contained in EAL 4.

## 2655 7 TOE Summary Specification

2656 The following paragraph provides a TOE summary specification describing how the TOE  
2657 meets each SFR.

2658

### 2659 7.1 SF.1: Authentication of Communication and Role Assignment 2660 for external entities

2661 The TOE contains a software module that authenticates all communication channels  
2662 with WAN, HAN and LMN networks. The authentication is based on the TLS 1.2 protocol  
2663 compliant to [RFC 5246]. According to [TR-03109], this TLS authentication mechanism  
2664 is used for all TLS secured communications channels with external entities. The TOE  
2665 does always implement the bidirectional authentication as required by [TR-03109-1] with  
2666 one exception: if the Consumer requests a password-based authentication from the  
2667 GWA according to [TR-03109-1], and the GWA activates this authentication method for  
2668 this Consumer, the TOE uses a unidirectional TLS authentication. Thus, although the  
2669 client has not sent a valid certificate, the TOE continues the TLS authentication process  
2670 with the password authentication process for this client (see [RFC 5246, chap. 7.4.6.]).  
2671 The password policy to be fulfilled hereby is that the password must be at least 10 char-  
2672 acters long containing at least one character of each of the following character groups:  
2673 capital letters, small letters, digits, and special characters (!"§\$%&/()=?+\*~#',;:-\_). Fur-  
2674 ther characters could also be used.

2675 [TR-03109-1] requires the TOE to use elliptical curves conforming to [RFC 5289]  
2676 whereas the following cipher suites are supported:

- 2677 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,
- 2678 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,
- 2679 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, and
- 2680 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384.

2681 The following elliptical curves are supported by the TOE

- 2682 • BrainpoolP256r1 (according to [RFC 5639]),
- 2683 • BrainpoolP384r1 (according to [RFC 5639]),
- 2684 • BrainpoolP512r1 (according to [RFC 5639]),
- 2685 • NIST P-256 (according to [RFC 5114]), and
- 2686 • NIST P-384 (according to [RFC 5114]).

2687           Alongside, the TOE supports the case of unidirectional communication with wireless me-  
2688           ter (via the wM-Bus protocol), where the external entity is authenticated via AES with  
2689           CMAC authentication. In this case, the AES algorithm is operating in CBC mode with  
2690           128-bit symmetric keys. The authentication is successful in case that the CMAC has  
2691           been successfully verified by the use of a cryptographic key  $K_{\text{mac}}$ . The cryptographic key  
2692           for CMAC authentication ( $K_{\text{mac}}$ ) is derived from the meter individual key MK conformant  
2693           to [TR-03116-3, chap. 7.2]. The meter individual key MK (brought into the TOE by the  
2694           GWA) is selected by the TOE through the MAC-protected but unencrypted meter-id sub-  
2695           mitted by the meter.

2696           The generation of the cryptographic key material for TLS secured communication chan-  
2697           nels utilizes a Security Module. This Security Module is compliant to [TR-03109-2] and  
2698           evaluated according to [SecModPP].

2699           The destruction of cryptographic key material used by the TOE is performed through  
2700           “zeroisation”. The TOE stores all ephemeral keys used for TLS secured communication  
2701           or other cryptographic operations in the RAM only. For instance, whenever a TLS se-  
2702           cured communication is terminated, the TOE wipes the RAM area used for the crypto-  
2703           graphic key material with 0-bytes directly after finishing the usage of that material.

2704           The TOE receives the authentication certificate of the external entity during the hand-  
2705           shake phase of the TLS protocol. For the establishment of the TLS secured communi-  
2706           cation channel, the TOE verifies the correctness of the signed data transmitted during  
2707           the TLS protocol handshake phase. While importing an authentication certificate the  
2708           TOE verifies the certificate chain of the certificate for all certificates of the SM-PKI ac-  
2709           cording to [TR-03109-4]. Note, that the certificate used for the TLS-based authentication  
2710           of wired meters is self-signed and not part of the SM-PKI. Additionally, the TOE checks  
2711           whether the certificate is configured by the Gateway Administrator for the used interface,  
2712           and whether the remote IP address used and configured in the TSF data are identical  
2713           (**FIA\_USB.1**). The TOE does not check the certificate’s revocation status. In order to  
2714           authenticate the external entity, the key material of the TOE’s communication partner  
2715           must be known and trusted.

2716           The following communication types are known to the TOE <sup>222</sup>:

2717           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.

- 2718                   b) LMN communication via IF\_GW\_MTR (wireless or wired Meter)
- 2719                   c) HAN communication via IF\_GW\_CON, IF\_GW\_CLS or IF\_GW\_SRV
- 2720                   Except the communication with wireless meters at IF\_GW\_MTR, all communication
- 2721                   types are TLS-based. In order to accept a TLS communication connection as being au-
- 2722                   thenticated, the following conditions must be fulfilled:
- 2723                   a) The TLS channel must have been established successfully with the required
- 2724                   cryptographic mechanisms.
- 2725                   b) The certificate of the external entity must be known and trusted through config-
- 2726                   uration by the Gateway Administrator, and associated with the according com-
- 2727                   munication type<sup>223</sup>.
- 2728                   For the successfully authenticated external entity, the TOE performs an internal assign-
- 2729                   ment of the communication type based on the certificate received at the external inter-
- 2730                   face if applicable. The user identity is associated with the name of the certificate owner
- 2731                   in case of a certificate-based authentication or with the user name in case of a password-
- 2732                   based authentication at interface IF\_GW\_CON.
- 2733                   For the LMN communication of the TOE with wireless (a.k.a. wM-Bus-based) meters,
- 2734                   the external entity is authenticated by the use of the AES-CMAC algorithm and the me-
- 2735                   ter-ID for wired Meters is used for association to the user identity (**FIA\_USB.1**). This
- 2736                   communication is only allowed for meters not supporting TLS-based communication
- 2737                   scenarios.
- 2738                   **FCS\_CKM.1/TLS** is fulfilled by the TOE through the implementation of the pseudoran-
- 2739                   dom function of the TLS protocol compliant to [RFC 5246] while the Security Module is
- 2740                   used by the TOE for the generation of the cryptographic key material. The use of TLS
- 2741                   according to [RFC 5246] and the use of the postulated cipher suites according to
- 2742                   [RFC 5639] fulfill the requirement **FCS\_COP.1/TLS**. The requirements
- 2743                   **FCS\_CKM.1/MTR** and **FCS\_COP.1/MTR** are fulfilled by the use of AES-CMAC-secured
- 2744                   communication for wireless meters. The requirement **FCS\_CKM.4** is fulfilled by the de-
- 2745                   scribed method of “zeroisation” when destroying cryptographic key material. The imple-
- 2746                   mentation of the described mechanisms (especially the use of TLS and AES-CBC with
- 2747                   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.

2748 **FTP\_ITC.1/USR. FPT\_RPL.1** is fulfilled by the use of the TLS protocol respectively the  
2749 integration of transmission counters according to [TR-03116-3, chap. 7.3].

2750 A successfully established connection will be automatically disconnected by the TOE if  
2751 a TLS channel to the WAN is established more than 48 hours, if a TLS channel to the  
2752 LMN has transmitted more than 5 MB of information or if a channel to a local user is  
2753 inactive for a time configurable by the authorised Gateway Administrator of up to 10  
2754 minutes, and a new connection establishment will require a new full authentication pro-  
2755 cedure (**FIA\_UAU.6**). In any case – whether the connection has been successfully es-  
2756 tablished or not – all associated resources related with the connection or connection  
2757 attempt are freed. The implementation of this requirement is done by means of the TOE's  
2758 operation system monitoring and limiting the resources of each process. This means  
2759 that with each connection (or connection attempt) an internal session is created that is  
2760 associated with resources monitored and limited by the TOE. All resources are freed  
2761 even before finishing a session if the respective resource is no longer needed so that no  
2762 previous information content of a resource is made available. Especially, the associated  
2763 cryptographic key material is wiped as soon it is no longer needed. As such, the TOE  
2764 ensures that during the phase of connection termination the internal session is also ter-  
2765 minated and by this, all internal data (associated cryptographic key material and volatile  
2766 data) is wiped by the zeroisation procedure described. Allocated physical resources are  
2767 also freed. In case non-volatile data is no longer needed, the associated resources data  
2768 are freed, too. The TOE doesn't reuse any objects after deallocation of the resource  
2769 (**FDP\_RIP.2**).

2770 If the external entity can be successfully authenticated on basis of the received certificate  
2771 (or the password in case of a consumer using password authentication) and the ac-  
2772 claimed identity could be approved for the used external interface, the TOE associates  
2773 the user identity, the authentication status and the connecting network to the role ac-  
2774 cording to the internal role model (**FIA\_ATD.1**). In order to implement this, the TOE uti-  
2775 lizes an internal data model which supplies the allowed communication network and  
2776 other restricting properties linked with the submitted security attribute on the basis of the  
2777 submitted authentication data providing the multiple mechanisms for authentication of  
2778 any user's claimed identity according to the necessary rules according to [TR-03109-1]  
2779 (**FIA\_UAU.5**).

2780 In case of wireless meter communication (via the wM-Bus protocol), the security attribute  
2781 of the Meter is the meter-id authenticated by the CMAC, where the meter-id is the identity  
2782 providing criterion that is used by the TOE. The identity of the Meter is associated to the

2783 successfully authenticated external entity by the TOE and linked to the respective role  
2784 according to Table 5 and its active session. In this case, the identity providing criterion  
2785 is also the meter-id.

2786 The TOE enforces an explicit and complete security policy protecting the data flow for  
2787 all external entities (**FDP\_IFC.2/FW**, **FDP\_IFF.1/FW**, **FDP\_IFC.2/MTR**,  
2788 **FDP\_IFF.1/MTR**). The security policy defines the accessibility of data for each external  
2789 entity and additionally the permitted actions for these data. Moreover, the external enti-  
2790 ties do also underlie restrictions for the operations which can be executed with the TOE  
2791 (**FDP\_ACF.1**). In case that it is not possible to authenticate an external entity success-  
2792 fully (e.g. caused by unknown authentication credentials), no other action is allowed on  
2793 behalf of this user and the concerning connection is terminated (**FIA\_UAU.2**). Any com-  
2794 munication is only possible after successful authentication and identification of the ex-  
2795 ternal entity (**FIA\_UID.2**, **FIA\_USB.1**).

2796 The reception of the wake-up service data package is a special case that requests the  
2797 TOE to establish a TLS authenticated and protected connection to the Gateway Admin-  
2798 istrator. The TOE validates the data package due to its compliance to the structure de-  
2799 scribed in [TR-03109-1] and verifies the ECDSA signature with the public key of the  
2800 Gateway Administrator's certificate which must be known and trusted to the TOE. The  
2801 TOE does not perform a revocation check or any validity check compliant to the shell  
2802 model. The TOE verifies the electronic signature successfully when the certificate is  
2803 known, trusted and associated to the Gateway Administrator. The TOE establishes the  
2804 connection to the Gateway Administrator when the package has been validated due to  
2805 its structural conformity, the signature has been verified and the integrated timestamp  
2806 fulfills the requirements of [TR-03109-1]. Receiving the data package and the successful  
2807 validation of the wake-up package does not mean that the Gateway Administrator has  
2808 successfully been authenticated.

2809 If the Gateway Administrator could be successfully authenticated based on the certificate  
2810 submitted during the TLS handshake phase, the role will be assigned by the TOE ac-  
2811 cording to now approved identity based on the internal role model and the TLS channel  
2812 will be established.

### 2813 **WAN roles**

2814 The TOE assigns the following roles in the WAN communication (**FMT\_SMR.1**):

- 2815 • authorised Gateway Administrator,
- 2816 • authorised External Entity.

2817 The role assignment is based on the X.509 certificate used by the external entity during  
2818 TLS connection establishment. The TOE has explicit knowledge of the Gateway Admin-  
2819 istrator's certificate and the assignment of the role "Gateway Administrator" requires the  
2820 successful authentication of the WAN connection.

2821 The assignment of the role "Authorized External Entity" requires the X.509 certificate  
2822 that is used during the TLS handshake to be part of an internal trust list that is under  
2823 control of the TOE.

2824 The role "Authorized External Entity" can be assigned to more than one external entity.

### 2825 **HAN roles**

2826 The TOE differentiates and assigns the following roles in the HAN communication  
2827 (**FMT\_SMR.1**):

- 2828 • authorised Consumer
- 2829 • authorised Service Technician

2830 The role assignment is based on the X.509 certificate used by the external entity for  
2831 TLS-secured communication channels or on password-based authentication at interface  
2832 IF\_GW\_CON if configured (**FIA\_USB.1**).

2833 The assignment of roles in the HAN communication requires the successful identification  
2834 of the external entity as a result of a successful authentication based on the certificate  
2835 used for the HAN connection. The certificates used to authenticate the "Consumer" or  
2836 the "Service Technician" are explicitly known to the TOE through configuration by the  
2837 Gateway Administrator.

### 2838 **Multi-client capability in the HAN**

2839 The HAN communication might use more than one, parallel and independent authenti-  
2840 cated communication channels. The TOE ensures that the certificates that are used for  
2841 the authentication are different from each other.

2842 The role "Consumer" can be assigned to multiple, parallel sessions. The TOE ensures  
2843 that these parallel sessions are logically distinct from each other by the use of different  
2844 authentication information. This ensures that only the Meter Data associated with the  
2845 authorized user are provided and Meter Data of other users are not accessible.

### 2846 **LMN roles**

2847 One of the following authentication mechanisms is used for Meters:

- 2848 a) authentication by the use of TLS according to [RFC 5246] for wired Meters  
2849 a) authentication by the use of AES with CMAC authentication according to  
2850 [RFC 3394] for wireless Meters.

2851 The TOE explicitly knows the identification credentials needed for authentication (X.509  
2852 certificate when using TLS; meter-id in conjunction with CMAC and known  $K_{mac}$  when  
2853 using AES) through configuration by the Gateway Administrator. If the Meter could be  
2854 successfully authenticated and the claimed identity could thus be proved, the according  
2855 role “Authorised External Entity” is assigned by the TOE for this Meter at IF\_GW\_MTR  
2856 based on the internal role model.

### 2857 **LMN multi-client capabilities**

2858 The LMN communication can be run via parallel, logically distinct and separately au-  
2859 thenticated communication channels. The TOE ensures that the authentication creden-  
2860 tials of each separate channel are different.

2861 The TOE’s internal policy for access to data and objects under control of the TOE is  
2862 closely linked with the identity of the external entity at IF\_GW\_MTR according to the  
2863 TOE-internal role model. Based on the successfully verified authentication data, a per-  
2864 mission catalogue with security attributes is internally assigned, which defines the al-  
2865 lowed actions and access permissions within a communication channel.

2866 The encapsulation of the TOE processes run by this user is realized through the mech-  
2867 anisms offered by the TOE’s operating system and very restrictive user rights for each  
2868 process. Each role is assigned to a separate, limited user account in the TOE’s operating  
2869 system. For all of these accounts, it is only allowed to read, write or execute the files  
2870 absolutely necessary for implementing the program logic. For each identity interacting  
2871 with the TOE, a separate operating system process is started. Especially, the databases  
2872 used by the TOE and the logging service are adequately separated for enforcement of  
2873 the necessary security domain separation (**FDP\_ACF.1**). The allowed actions and ac-  
2874 cess permissions and associated objects are assigned to the successfully approved  
2875 identity of the user based on the used authentication credentials and the resulting asso-  
2876 ciated role. The current session is unambiguously associated with this user. No interac-  
2877 tion (e.g. access to Meter Data) is possible without an appropriate permission catalogue  
2878 (**FDP\_ACC.2**). The freeing of the role assignment and associated resources are ensured  
2879 through the monitoring of the current session.

## 2880 7.2SF.2: Acceptance and Deposition of Meter Data, Encryption of 2881 Meter Data for WAN transmission

2882 The TOE receives Meter Data from an LMN communication channel and deposits these  
2883 Meter Data with the associated data for tariffing in a database especially assigned to this  
2884 individual Meter residing in an encrypted file system (**FCS\_COP.1/MEM**). The time in-  
2885 terval for receiving or retrieving Meter Data can be configured individually per meter  
2886 through a successfully authenticated Gateway Administrator and are initialized by the  
2887 TOE during the setup procedure with pre-defined values.

2888 The Meter Data are cryptographically protected and their integrity is verified by the TOE  
2889 before the tariffing and deposition is performed. In case of a TLS secured communica-  
2890 tion, the integrity and confidentiality of the transmitted data is protected by the TLS pro-  
2891 tocol according to [RFC 5246]. In case of a unidirectional communication at  
2892 IF\_GW\_MTR/wireless, the integrity is verified by the verification of the CMAC check sum  
2893 whereas the protection of the confidentiality is given by the use of AES in CBC mode  
2894 with 128 bit key length in combination with the CMAC authentication (**FCS\_CKM.1/MTR**,  
2895 **FCS\_COP.1/MTR**). The AES encryption key has been brought into the TOE via a man-  
2896 agement function during the pairing process for the Meter. In the TOE's internal data  
2897 model, the used cryptographic keys  $K_{mac}$  and  $K_{enc}$  are associated with the meter-id due  
2898 to the fact of the unidirectional communication. The TOE contains a packet monitor for  
2899 Meter Data to avoid replay attacks based on the re-sending of Meter Data packages. In  
2900 case of recognized data packets which have already been received and processed by  
2901 the TOE, these data packets are blocked by the packet monitor (**FPT\_RPL.1**).

2902 Concerning the service layers, the TOE detects replay attacks that can occur during  
2903 authentication processes against the TOE or for example receiving data from one of the  
2904 involved communication networks. This is for instance achieved through the correct in-  
2905 terpretation of the strictly increasing ordering numbers for messages from the meters (in  
2906 case that a TLS-secured communication channel is not used), through the enforcement  
2907 of an appropriate time slot of execution for successfully authenticated wake-up calls, and  
2908 of course through the use of the internal means of the TLS protocol according to  
2909 [RFC 5246] (**FPT\_RPL.1**).

2910 The deposition of Meter Data is performed in a way that these Meter Data are associated  
2911 with a permission profile. This means that all of the operations and actions that can be  
2912 taken with these data as described afterwards (e.g. sending via WAN to an Authenti-  
2913 cated External Entity) depend on the permissions which are associated with the

2914 Meter Data. For metrological purposes, the Meter Data's security attribute - if applicable  
2915 - will be persisted associated with its corresponding Meter Data by the TOE. All user  
2916 associated data stored by the TOE are protected by an AES-128-CMAC value. Before  
2917 accessing these data, the TOE verifies the CMAC value that has been applied to the  
2918 user data and detects integrity errors on any data and especially on user associated  
2919 Meter Data in a reliable manner (**FDP\_SDI.2**).

2920 Closely linked with the deposition of the Meter Data is the assignment of an unambigu-  
2921 ous and reliable timestamp on these data. The reliability grounds on the regular use of  
2922 an external time source offering a sufficient exactness (**FPT\_STM.1**) which is used to  
2923 synchronize the operating system of the TOE. A maximum deviation of 3% of the meas-  
2924 uring period is allowed to be in conformance with [PP\_GW]. The data set (Meter Data  
2925 and tariff data) is associated with the timestamp in an inseparably manner because each  
2926 Meter Data entry in the database includes the corresponding time stamp and the data-  
2927 base is cryptographically protected through the encrypted file system. For details about  
2928 database encryption please see page 153).

2929 For transmission of consumption data (tariffed Meter Data) or status data into the WAN,  
2930 the TOE ensures that the data are encrypted and digitally signed (**FCO\_NRO.2**,  
2931 **FCS\_CKM.1/CMS**, **FCS\_COP.1/CMS**, **FCS\_COP.1/HASH**, **FCS\_COP.1/MEM**). In case  
2932 of a successful transmission of consumption data into the WAN, beside the transmitted  
2933 data the data's signature applied by the TOE is logged in the Consumer-Log for the  
2934 respective Consumer at IF\_GW\_CON thus providing the possibility not only for the re-  
2935 cipient to verify the evidence of origin for the transmitted data but to the Consumer at  
2936 IF\_GW\_CON, too (**FCO\_NRO.2**). The encryption is performed with the hybrid encryption  
2937 as specified in [TR-03109-1-I] in combination with [TR-03116-3]. The public key of the  
2938 external entity, the data have to be encrypted for, is known by the TOE through the  
2939 authentication data configured by the Gateway Administrator and its assigned identity.  
2940 This public key is assumed by the TOE to be valid because the TOE does not verify the  
2941 revocation status of certificates. The public key used for the encryption of the derived  
2942 symmetric key used for transmission of consumption data is different from the public key  
2943 in the TLS certificate of the external entity used for the TLS secured communication  
2944 channel. The derivation of the hybrid key used for transmission of consumption data is  
2945 done according to [TR-03116-3, chapter 8].

2946 The TOE does also foresee the case that the data is encrypted for an external entity that  
2947 is not directly assigned to the external entity holding the active communication channel.  
2948 The electronic signature is created through the utilization of the Security Module whereas

2949 the TOE is responsible for the computation of the hash value for the data to be signed.  
2950 Therefore, the TOE utilizes the SHA-256 or SHA-384 hash algorithm. The SHA-512 hash  
2951 algorithm is available in the TOE but not yet used (**FCS\_COP.1/HASH**). The data to be  
2952 sent to the external entity are prepared on basis of the tariffed meter data. The data to  
2953 be transmitted are removed through deallocation of the resources after the (successful  
2954 or unsuccessful) transmission attempt so that afterwards no previous information will be  
2955 available (**FDP\_RIP.2**). The created temporary session keys which have been used for  
2956 encryption of the data are also deleted by the already described zeroisation mechanism  
2957 as soon they are no longer needed (**FCS\_CKM.4**).

2958 The time interval for transmission of the data is set for a daily transmission, and can be  
2959 additionally configured by the Gateway Administrator. The TOE sends randomly gener-  
2960 ated messages into the WAN, so that through this the analysis of frequency, load, size  
2961 or the absence of external communication is concealed (**FPR\_CON.1**). Data that are not  
2962 relevant for accounting are aliased for transmission so that no personally identifiable  
2963 information (PII) can be obtained by an analysis of not billing-relevant information sent  
2964 to parties in the WAN. Therefore, the TOE utilizes the alias as defined by the Gateway  
2965 Administrator in the Processing Profile for the Meter identity to external parties in the  
2966 WAN. Thereby, the TOE determines the alias for a user and verifies that it conforms to  
2967 the alias given in the Processing Profile (**FPR\_PSE.1**).

2968

### 2969 **7.3SF.3: Administration, Configuration and SW Update**

2970 The TOE includes functionality that allows its administration and configuration as well as  
2971 updating the TOE's complete firmware ("firmware updates") or only the software appli-  
2972 cation including the service layer ("software updates"). This functionality is only provided  
2973 for the authenticated Gateway Administrator (**FMT\_MOF.1**, **FMT\_MSA.1/AC**,  
2974 **FMT\_MSA.1/FW**, **FMT\_MSA.1/MTR**).

2975 The following operations can be performed by the successfully authenticated Gateway  
2976 Administrator:

- 2977 a) Definition and deployment of Processing Profiles including user administration,  
2978 rights management and setting configuration parameters of the TOE
- 2979 b) Deployment of tariff information
- 2980 c) Deployment and installation of software/firmware updates

2981 A complete overview of the possible management functions is given in Table 14 and  
2982 Table 15 (**FMT\_SMF.1**). Beside the possibility for a successfully authenticated Service  
2983 Technician to view the system log via interface IF\_GW\_SRV, administrative or configu-  
2984 ration measures on the TOE can only be taken by the successfully authenticated Gate-  
2985 way Administrator.

2986 In order to perform these measures, the TOE has to establish a TLS secured channel  
2987 to the Gateway Administrator and must authenticate the Gateway Administrator suc-  
2988 cessfully. There are two possibilities:

- 2989 a) The TOE independently contacts the Gateway Administrator at a certain time  
2990 specified in advance by the Gateway Administrator.
- 2991 b) Through a message sent to the wake-up service, the TOE is requested to con-  
2992 tact the Gateway Administrator.

2993 In the second case, the wake-up data packet is received by the TOE from the WAN and  
2994 checked by the TOE for structural correctness according to [TR-03109-1]. Afterwards,  
2995 the TOE verifies the correctness of the electronic signature applied to the wake-up mes-  
2996 sage data packet using the certificate of the Gateway Administrator stored in the TSF  
2997 data. Afterwards, a TLS connection to the Gateway Administrator is established by the  
2998 TOE and the above mentioned operations can be performed.

2999 Software/firmware updates always have to be signed by the TOE manufacturer.

3000 Software/firmware updates can be of different content:

- 3001 a) The whole boot image of the TOE is changed.
- 3002 b) Only individual components of the TOE are changed. These components can  
3003 be the boot loader plus the static kernel or the SMGW application.

3004 The update packet is realized in form of an archive file enveloped into a CMS signature  
3005 container according to [RFC 5652]. The electronic signature of the update packet is cre-  
3006 ated using signature keys from the TOE manufacturer. The verification of this signature  
3007 is performed by the TOE using the TOE's Security Module using the trust anchor of the  
3008 TOE manufacturer. If the signature of the transferred data could not be successfully  
3009 verified by the TOE or if the version number of the new firmware is not higher than the  
3010 version number of the installed firmware, the received data is rejected by the TOE and  
3011 not used for further processing. Any administrator action is entered in the System Log of  
3012 the TOE. Additionally, an authorised Consumer can interact with the TOE via the

3013 interface IF\_GW\_CON to get the version number and the current time displayed  
3014 (**FMT\_MOF.1**).

3015 The signature of the update packet is immediately verified after receipt. After successful  
3016 verification of the update packet the update process is immediately performed. In each  
3017 case, the Gateway Administrator gets notified by the TOE and an entry in the TOE's  
3018 system log will be written.

3019 All parameters that can be changed by the Gateway Administrator are preset with re-  
3020 strictive values by the TOE. No role can specify alternative initial values to override these  
3021 restrictive default values (**FMT\_MSA.3/AC**, **FMT\_MSA.3/FW**, **FMT\_MSA.3/MTR**).

3022 This mechanism is supported by the TOE-internal resource monitor that internally mon-  
3023 itors existing connections, assigned roles and operations allowed at a specific time.

3024

#### 3025 **7.4 SF.4: Displaying Consumption Data**

3026 The TOE offers the possibility of displaying consumption data to authenticated Consum-  
3027 ers at interface IF\_GW\_CON. Therefore, the TOE contains a web server that implements  
3028 TLS-based communication with mutual authentication (**FTP\_ITC.1/USR**). If the Con-  
3029 sumer requests a password-based authentication from the GWA according to [TR-  
3030 03109-1] and the GWA activates this authentication method for this Consumer, the TOE  
3031 uses TLS authentication with server-side authentication and HTTP digest access au-  
3032 thentication according to [RFC 7616]. In both cases, the requirement **FCO\_NRO.2** is  
3033 fulfilled through the use of TLS-based communication and through encryption and digital  
3034 signature of the (tariffed) Meter Data to be displayed using **FCS\_COP.1/HASH**.

3035 To additionally display consumption data, a connection at interface IF\_GW\_CON must  
3036 be established and the role "(authorised) Consumer" is assigned to the user with his  
3037 used display unit by the TOE. Different Consumer can use different display units. The  
3038 amount of allowed connection attempts at IF\_GW\_CON is set to 5. In case the amount  
3039 of allowed connection attempts is reached, the TOE blocks IF\_GW\_CON (**FIA\_AFL.1**).  
3040 The display unit has to technically support the applied authentication mechanism and  
3041 the HTTP protocol version 1.1 according to [RFC 2616] as communication protocol. Data  
3042 is provided as HTML data stream and transferred to the display unit. In this case, further  
3043 processing of the transmitted data stream is carried out by the display unit.

3044 According to [TR-03109-1], the TOE exclusively transfers Consumer specific consump-  
3045 tion data to the display unit. The Consumer can be identified in a clear and unambiguous

3046 manner due to the applied authentication mechanism. Moreover, the TOE ensures that  
3047 exclusively the data actually assigned to the Consumer is provided at the display unit  
3048 via IF\_GW\_CON (**FIA\_USB.1**).

3049

## 3050 **7.5 SF.5: Audit and Logging**

3051 The TOE generates audit data for all actions assigned in the System-Log  
3052 (**FAU\_GEN.1/SYS**), the Consumer-Log (**FAU\_GEN.1/CON**), and the Calibration-Log  
3053 (**FAU\_GEN.1/CAL**) as well. On the one hand, this applies to the values measured by  
3054 the Meter (Consumer-Log) and on the other hand to system data (System-Log) used by  
3055 the Gateway Administrator of the TOE in order to check the TOE's current functional  
3056 status. In addition, metrological entries are created in the Calibration-Log. The TOE thus  
3057 distinguishes between the following log classes:

- 3058 a) System-Log
- 3059 b) Consumer-Log
- 3060 c) Calibration-Log

3061 The TOE audits and logs all security functions that are used. Thereby, the TOE compo-  
3062 nent accomplishing this security audit functionality includes the necessary rules moni-  
3063 toring these audited events and through this indicating a potential violation of the en-  
3064 forcement of the TOE security functionality (e. g. in case of an integrity violation, replay  
3065 attack or an authentication failure). If such a security breach is detected, it is shown as  
3066 such in the log entry (**FAU\_SAA.1/SYS**).

3067 The System-Log can only be read by the authorized Gateway Administrator via interface  
3068 IF\_GW\_WAN or by an authorized Service Technician via interface IF\_GW\_SRV  
3069 (**FAU\_SAR.1/SYS**). Potential security breaches are separately indicated and identified  
3070 as such in the System-Log and the GWA gets informed about this potential security  
3071 breach (**FAU\_ARP.1/SYS**, **FDP\_SDI.2**). Data of the Consumer-Log can exclusively be  
3072 viewed by authenticated Consumers via interface IF\_GW\_CON designed to display con-  
3073 sumption data (**FAU\_SAR.1/CON**). The data included in the Calibration-Log can only be  
3074 read by the authenticated Gateway Administrator via interface IF\_GW\_WAN  
3075 (**FAU\_SAR.1/CAL**).

3076 If possible, each log entry is assigned to an identity that is known to the TOE. For audit  
3077 events resulting from actions of identified users resp. roles, the TOE associates the

3078 generated log information to the identified users while generating the audit information  
3079 (**FAU\_GEN.2**).

3080 Generated audit and log data are stored in a cryptographically secured storage. For this  
3081 purpose, a file-based SQL database system is used securing its' data using an AES-  
3082 XTS-128 encrypted file system (AES in XTS mode with 128-bit keys) according to  
3083 [FIPS Pub. 197] and [NIST 800-38E]. This is achieved by using device-specific AES  
3084 keys so that the secure environment can only be accessed with the associated symmet-  
3085 ric key available. Using an appropriately limited access of this symmetric, the TOE im-  
3086 plements the necessary rules so that it can be ensured that unauthorised modification  
3087 or deletion is prohibited (**FAU\_STG.2**).

3088 Audit and log data are stored in separate locations: One location is used to store Con-  
3089 sumer-specific log data (Consumer-Log) whereas device status data and metrological  
3090 data are stored in a separate location: status data are stored in the System-Log and  
3091 metrological data are stored in the Calibration-Log. Each of these logs is located in phys-  
3092 ically separate databases secured by different cryptographic keys. In case of several  
3093 external meters, a separate database is created for each Meter to store the respective  
3094 consumption and log data (**FAU\_GEN.2**).

3095 If the audit trail of the System-Log or the Consumer-Log is full (so that no further data  
3096 can be added), the oldest entries in the audit trail are overwritten (**FAU\_STG.2**,  
3097 **FAU\_STG.4/SYS**, **FAU\_STG.4/CON**). If the Consumer-Log's oldest audit record must  
3098 be kept because the period of billing verification (of usually 15 months) has not been  
3099 reached, the TOE's metrological activity is paused until the oldest audit record gets  
3100 deletable. Thereafter, the TOE's metrological activity is started again through an internal  
3101 timer. Moreover, the mechanism for storing log entries is designed in a way that these  
3102 entries are cryptographically protected against unauthorized deletion. This is especially  
3103 achieved by assigning cryptographic keys to each of the individual databases for the  
3104 System-Log, Consumer-Log and Calibration-Log.

3105 If the Calibration-Log cannot store any further data, the operation of the TOE is stopped  
3106 through the termination of its metering services and the TOE informs the Gateway Ad-  
3107 ministrator by creating an entry in the System-Log, so that additional measures can be  
3108 taken by the Gateway Administrator. Calibration-Log entries are never overwritten by  
3109 the TOE (**FAU\_STG.2**, **FAU\_STG.4/CAL**, **FMT\_MOF.1**).

3110 The TOE anonymizes the data in a way that no conclusions about a specific person or  
3111 user can be drawn from the log or recorded not billing relevant data. Stored consumption

3112 data are exclusively intended for accounting with the energy supplier. The data stored  
3113 in the System-Log are used for analysis purposes concerning necessary technical anal-  
3114 yses and possible security-related information.

## 3115 **7.6 SF.6: TOE Integrity Protection**

3116 The TOE makes physical tampering detectable through the TOE's sealed packaging of  
3117 the device. So if an attacker opens the case, this can be physically noticed, e. g. by the  
3118 Service Technician (**FPT\_PHP.1**).

3119 The TOE provides a secure boot mechanism. Beginning from the AES-128-encrypted  
3120 bootloader protected by a digital signature applied by the TOE manufacturer, each sub-  
3121 sequent step during the boot process is based on the previous step establishing a con-  
3122 tinuous forward-concatenation of cryptographical verification procedures. Thus, it is en-  
3123 sured that each part of the firmware, that means the operating system, the service layers  
3124 and the software application in general, is tested by the TOE during initial startup.  
3125 Thereby, a test of the TSF data being part of the software application is included. During  
3126 this complete self-test, it is checked that the electronic system of the physical device,  
3127 and all firmware components of the TOE are in authentic condition. This complete self-  
3128 test can also be run at the request of the successfully authenticated Gateway Adminis-  
3129 trator via interface IF\_GW\_WAN or at the request of the successfully authenticated Ser-  
3130 vice Technician via interface IF\_GW\_SRV. At the request of the successfully authenti-  
3131 cated Consumer via interface IF\_GW\_CON, the TOE will only test the integrity of the  
3132 Smart Metering software application including the service layers (without the operating  
3133 system) and the completeness of the TSF data stored in the TOE's database. Addition-  
3134 ally, the TOE itself runs a complete self-test periodically at least once a month during  
3135 normal operation. The integrity of TSF data stored in the TOE's database is always  
3136 tested during read access of that part of TSF data (**FPT\_TST.1**). **FPT\_RPL.1** is fulfilled  
3137 by the use of the TLS protocol respectively the integration of transmission counters ac-  
3138 cording to [TR-03116-3, chap. 7.3], and through the enforcement of an appropriate time  
3139 slot of execution for successfully authenticated wake-up calls.

3140 If an integrity violation of the TOE's hardware or firmware is detected or if the deviation  
3141 between local system time of the TOE and the reliable external time source is too large,  
3142 further use of the TOE for the purpose of gathering Meter Data is not possible. Also in  
3143 this case, the TOE signals the incorrect status via a suitable signal output on the case

3144 of the device, and the further use of the TOE for the purpose of gathering Meter Data is  
 3145 not allowed (**FPT\_FLS.1**).

3146 Basically, if an integrity violation is detected, the TOE will create an entry in the System  
 3147 Log to document this status for the authorised Gateway Administrator on interface  
 3148 IF\_GW\_WAN resp. for the authorised Service Technician on interface IF\_GW\_SRV, and  
 3149 will inform the Gateway Administrator on this incident (**FAU\_ARP.1/SYS**,  
 3150 **FAU\_GEN.1/SYS**, **FAU\_SAR.1/SYS**, **FPT\_TST.1**).

3151 **7.7 TSS Rationale**

3152 The following table shows the correspondence analysis for the described TOE security  
 3153 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		

3154

**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.

## 3155 8 List of Tables

3156	TABLE 1: SMART METER GATEWAY PRODUCT CLASSIFICATIONS.....	10
3157	TABLE 2: COMMUNICATION FLOWS BETWEEN DEVICES IN DIFFERENT NETWORKS .....	24
3158	TABLE 3: MANDATORY TOE EXTERNAL INTERFACES.....	29
3159	TABLE 4: CRYPTOGRAPHIC SUPPORT OF THE TOE AND ITS SECURITY MODULE .....	30
3160	TABLE 5: ROLES USED IN THE SECURITY TARGET .....	36
3161	TABLE 6: ASSETS (USER DATA).....	38
3162	TABLE 7: ASSETS (TSF DATA) .....	39
3163	TABLE 8: RATIONALE FOR SECURITY OBJECTIVES .....	56
3164	TABLE 9: LIST OF SECURITY FUNCTIONAL REQUIREMENTS .....	67
3165	TABLE 10: OVERVIEW OVER AUDIT PROCESSES .....	69
3166	TABLE 11: EVENTS FOR CONSUMER LOG .....	74
3167	TABLE 12: CONTENT OF CALIBRATION LOG .....	79
3168	TABLE 13: RESTRICTIONS ON MANAGEMENT FUNCTIONS.....	108
3169	TABLE 14: SFR RELATED MANAGEMENT FUNCTIONALITIES .....	113
3170	TABLE 15: GATEWAY SPECIFIC MANAGEMENT FUNCTIONALITIES .....	114
3171	TABLE 16: ASSURANCE REQUIREMENTS.....	125
3172	TABLE 17: FULFILMENT OF SECURITY OBJECTIVES .....	129
3173	TABLE 18: SFR DEPENDENCIES .....	139
3174	TABLE 19: RATIONALE FOR THE SFR AND THE TOE SECURITY FUNCTIONALITIES .....	158
3175		

3176 **9 List of Figures**

3177 FIGURE 1: THE TOE AND ITS DIRECT ENVIRONMENT ..... 13  
3178 FIGURE 2: THE LOGICAL INTERFACES OF THE TOE ..... 15  
3179 FIGURE 3: THE PRODUCT WITH ITS TOE AND NON-TOE PARTS ..... 17  
3180 FIGURE 4: THE TOE'S PROTOCOL STACK..... 19  
3181 FIGURE 5: CRYPTOGRAPHIC INFORMATION FLOW FOR DISTRIBUTED METERS AND GATEWAY  
3182 ..... 32  
3183

3184 **10 Appendix**3185 **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)
------------------------	--------------------------------------

3186

3187      **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

## 3188 11 Literature

- 3189 [CC] Common Criteria for Information Technology Security  
3190 Evaluation –  
3191 Part 1: Introduction and general model, April 2017, ver-  
3192 sion 3.1, Revision 5, CCMB-2017-04-001,  
3193 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf)  
3194 [tal.org/files/ccfiles/CCPART1V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf)
- 3195 Part 2: Security functional requirements, April 2017, ver-  
3196 sion 3.1, Revision 5, CCMB-2017-04-002,  
3197 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf)  
3198 [tal.org/files/ccfiles/CCPART2V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf)
- 3199 Part 3: Security assurance requirements, April 2017, ver-  
3200 sion 3.1, Revision 5, CCMB-2017-04-003,  
3201 [https://www.commoncriteriapor-](https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf)  
3202 [tal.org/files/ccfiles/CCPART3V3.1R5.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf)
- 3203 [CEN] SMART METERS CO-ORDINATION GROUP (SM-CG)  
3204 Item 5. M/441 first phase deliverable – Communication –  
3205 Annex: Glossary (SMCG/Sec0022/DC)
- 3206 [PP\_GW] Protection Profile for the Gateway of a Smart Metering  
3207 System (Smart Meter Gateway PP), Schutzprofil für die  
3208 Kommunikationseinheit eines intelligenten Messsystems  
3209 für Stoff- und Energiemengen, SMGW-PP, v.1.3, Bundes-  
3210 amt für Sicherheit in der Informationstechnik, 31.03.2014
- 3211 [SecModPP] Protection Profile for the Security Module of a Smart Me-  
3212 ter Gateway (Security Module PP), Schutzprofil für das  
3213 Sicherheitsmodul der Kommunikationseinheit eines intelli-  
3214 genten Messsystems für Stoff- und Energiemengen,  
3215 SecMod-PP, Version 1.0.2, Bundesamt für Sicherheit in  
3216 der Informationstechnik, 18.10.2013
- 3217 [SD\_6] ISO/IEC JTC 1/SC 27 N7446, Standing Document 6  
3218 (SD6): Glossary of IT Security Terminology 2009-04-29,  
3219 available at

3220		<a href="http://www.teletrust.de/uploads/media/ISOIEC_JTC1_SC27_IT_Security_Glossary_TeleTrusT_Documentation.pdf">http://www.teletrust.de/uploads/me-</a>
3221		<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>
3222		<a href="http://www.teletrust.de/uploads/media/ISOIEC_JTC1_SC27_IT_Security_Glossary_TeleTrusT_Documentation.pdf">TrusT_Documentation.pdf</a>
3223	[TR-02102]	Technische Richtlinie BSI TR-02102, Kryptographische
3224		Verfahren: Empfehlungen und Schlüssellängen, Bundes-
3225		amt für Sicherheit in der Informationstechnik, Version
3226		2022-01
3227	[TR-03109]	Technische Richtlinie BSI TR-03109, Version 1.1, Bun-
3228		desamt für Sicherheit in der Informationstechnik,
3229		22.09.2021
3230	[TR-03109-1]	Technische Richtlinie BSI TR-03109-1, Anforderungen an
3231		die Interoperabilität der Kommunikationseinheit eines
3232		Messsystems, Version 1.1, Bundesamt für Sicherheit in
3233		der Informationstechnik, 17.09.2021
3234	[TR-03109-1-I]	Technische Richtlinie BSI TR-03109-1 Anlage I, CMS-
3235		Datenformat für die Inhaltsdatenverschlüsselung und -
3236		signatur, Version 1.0.9, Bundesamt für Sicherheit in der
3237		Informationstechnik, 18.03.2013
3238	[TR-03109-1-VI]	Technische Richtlinie BSI TR-03109-1 Anlage VI, Be-
3239		triebsprozesse, Version 1.0, Bundesamt für Sicherheit in
3240		der Informationstechnik, 18.03.2013
3241	[TR-03109-2]	Technische Richtlinie BSI TR-03109-2, Smart Meter Ga-
3242		teway – Anforderungen an die Funktionalität und In-
3243		teroperabilität des Sicherheitsmoduls, Version 1.1, Bun-
3244		desamt für Sicherheit in der Informationstechnik,
3245		15.12.2014
3246	[TR-03109-3]	Technische Richtlinie BSI TR-03109-3, Kryptographische
3247		Vorgaben für die Infrastruktur von intelligenten Messsys-
3248		temen, Version 1.1, Bundesamt für Sicherheit in der Infor-
3249		mationstechnik, 17.04.2014
3250	[TR-03109-4]	Technische Richtlinie BSI TR-03109-4, Smart Metering
3251		PKI - Public Key Infrastruktur für Smart Meter Gateways,

3252		Version 1.2.1, Bundesamt für Sicherheit in der Informationstechnik, 09.08.2017
3253		
3254	[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
3255		
3256		
3257	[TR-03111]	Technische Richtlinie BSI TR-03111, Elliptic Curve Cryptography (ECC), Version 2.1, 01.06.2018
3258		
3259	[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
3260		
3261		
3262		
3263	[AGD_Consumer]	Handbuch für Verbraucher, Smart Meter Gateway, Version 4.15, 15.08.2024, Power Plus Communications AG
3264		
3265	[AGD_Techniker]	Handbuch für Service-Techniker, Smart Meter Gateway, Version 5.13, 15.08.2024, Power Plus Communications AG
3266		
3267		
3268	[AGD_GWA]	Handbuch für Hersteller von Smart-Meter Gateway-Administrations-Software, Smart Meter Gateway, Version 4.18.1, 23.10.2025, Power Plus Communications AG
3269		
3270		
3271	[AGD_SEC]	Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung, Version 1.15, 02.12.2024, Power Plus Communications AG
3272		
3273		
3274	[SMGW_Logging]	Logmeldungen, SMGW, Version 3.5, 29.07.2024, Power Plus Communications AG
3275		
3276	[FIPS Pub. 140-2]	NIST, FIPS 140-3, Security Requirements for cryptographic modules, 2019
3277		
3278	[FIPS Pub. 180-4]	NIST, FIPS 180-4, Secure Hash Standard, 2015
3279	[FIPS Pub. 197]	NIST, FIPS 197, Advances Encryption Standard (AES), 2001
3280		
3281	[IEEE 1901]	IEEE Std 1901-2010, IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications, 2010
3282		
3283		

3284	[IEEE 802.3]	IEEE Std 802.3-2008, IEEE Standard for Information
3285		technology, Telecommunications and information ex-
3286		change between systems, Local and metropolitan area
3287		networks, Specific requirements, 2008
3288	[ISO 10116]	ISO/IEC 10116:2006, Information technology -- Security
3289		techniques -- Modes of operation for an n-bit block cipher,
3290		2006
3291	[NIST 800-38A]	NIST Special Publication 800-38A, Recommendation for
3292		Block Cipher Modes of Operation: Methods and Tech-
3293		niques, December 2001, <a href="http://nvl-pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf">http://nvl-</a>
3294		<a href="http://nvl-pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf">pubs.nist.gov/nistpubs/</a> Legacy/SP/nistspecialpublica-
3295		<a href="http://nvl-pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf">tion800-38a.pdf</a>
3296	[NIST 800-38D]	NIST Special Publication 800-38D, Recommendation for
3297		Block Cipher Modes of Operation: Galois/Counter Mode
3298		(GCM) and GMAC, M. Dworkin, November 2007,
3299		<a href="http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf">http://csrc.nist.gov/publications/nistpubs/800-38D/SP-</a>
3300		<a href="http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf">800-38D.pdf</a>
3301	[NIST 800-38E]	NIST Special Publication 800-38E, Recommendation for
3302		Block Cipher Modes of Operation: The XTS-AES Mode
3303		for Confidentiality on Storage Devices, M. Dworkin, Janu-
3304		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>
3305		<a href="http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf">38E/nist-sp-800-38E.pdf</a>
3306	[RFC 2104]	RFC 2104, HMAC: Keyed-Hashing for Message Authenti-
3307		cation, M. Bellare, R. Canetti und H. Krawczyk, February
3308		1997, <a href="http://rfc-editor.org/rfc/rfc2104.txt">http://rfc-editor.org/rfc/rfc2104.txt</a>
3309	[RFC 2616]	RFC 2616, Hypertext Transfer Protocol - HTTP/1.1, R.
3310		Fielding, J. Gettys, J. Mogul, H. Frystyk, P. Masinter, P.
3311		Leach, T. Berners-Lee, June 1999, <a href="http://rfc-editor.org/rfc/rfc2616.txt">http://rfc-edi-</a>
3312		<a href="http://rfc-editor.org/rfc/rfc2616.txt">tor.org/rfc/rfc2616.txt</a>
3313	[RFC 7616]	RFC 7616, HTTP Digest Access Authentication, R.
3314		Shekh-Yusef, D. Ahrens, S. Bremer, September 2015,
3315		<a href="http://rfc-editor.org/rfc/rfc7616.txt">http://rfc-editor.org/rfc/rfc7616.txt</a>

3316	[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>
3317		
3318		
3319	[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>
3320		
3321		
3322		
3323	[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>
3324		
3325		
3326	[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>
3327		
3328		
3329		
3330	[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>
3331		
3332		
3333		
3334	[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>
3335		
3336		
3337	[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>
3338		
3339		
3340	[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>
3341		
3342		
3343		
3344	[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>
3345		
3346		
3347		

3348	[RFC 5652]	RFC 5652, Cryptographic Message Syntax (CMS), R.
3349		Housley, Vigil Security, September 2009,
3350		<a href="http://www.ietf.org/rfc/rfc5652.txt">http://www.ietf.org/rfc/rfc5652.txt</a>
3351	[EIA RS-485]	EIA Standard RS-485, Electrical Characteristics of Gener-
3352		ators and Receivers for Use in Balanced Multipoint Sys-
3353		tems, ANSI/TIA/EIA-485-A-98, 1983/R2003
3354	[EN 13757-1]	M-Bus DIN EN 13757-1: Kommunikationssysteme für
3355		Zähler und deren Fernablesung Teil 1: Datenaustausch
3356	[EN 13757-3]	M-Bus DIN EN 13757-3, Kommunikationssysteme für
3357		Zähler und deren Fernablesung Teil 3: Spezielle Anwen-
3358		dungsschicht
3359	[EN 13757-4]	M-Bus DIN EN 13757-4, Kommunikationssysteme für
3360		Zähler und deren Fernablesung Teil 4: Zählerauslesung
3361		über Funk, Fernablesung von Zählern im SRD-Band von
3362		868 MHz bis 870 MHz
3363	[IEC-62056-5-3-8]	Electricity metering – Data exchange for meter reading,
3364		tariff and load control – Part 5-3-8: Smart Message Lan-
3365		guage SML, 2012
3366	[IEC-62056-6-1]	IEC-62056-6-1, Datenkommunikation der elektrischen
3367		Energiemessung, Teil 6-1: OBIS Object Identification Sys-
3368		tem, 2017, International Electrotechnical Commission
3369	[IEC-62056-6-2]	IEC-62056-6-2, Datenkommunikation der elektrischen
3370		Energiemessung - DLMS/COSEM, Teil 6-2: COSEM Inter-
3371		face classes, 2017, International Electrotechnical Commis-
3372		sion
3373	[IEC-62056-21]	IEC-62056-21, Direct local data exchange - Mode C, 2011,
3374		International Electrotechnical Commission
3375	[LUKS]	LUKS On-Disk Format Specification Version 1.2.1, Clem-
3376		ens Fruhwirth, October 16th, 2011
3377	[PACE]	The PACE-AA Protocol for Machine Readable Travel Doc-
3378		uments, and its Security, Jens Bender, Ozgur Dagdelen,

3379		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>
3380		
3381	[X9.63]	ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011
3382		
3383		
3384	[G865]	DVGW-Arbeitsblatt G865 Gasabrechnung, 11/2008
3385	[VDE4400]	VDE-AR-N 4400:2011-09, Messwesen Strom, VDE-Anwendungsregel, 01.09.2011
3386		
3387	[DIN 43863-5]	DIN: Herstellerübergreifende Identifikationsnummer für Messeinrichtungen, 2012
3388		
3389	[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>
3390		
3391		
3392		
3393	[ITU G.hn]	G.996x Unified high-speed wireline-based home networking transceivers, 2018
3394		
3395	[MSB-LK]	Anforderungskatalog zur MSB-Lieferkette, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik
3396		



**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