



1 **Technische Richtlinie BSI TR-03109-1**

2 **Anlage VI: Betriebsprozesse**

3

4 Version 1.0, Datum 18.03.2013

5

6

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel.: +49 22899 9582-100

E-Mail: smartmeter@bsi.bund.de

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2013

8	Inhaltsverzeichnis	
9	Inhaltsverzeichnis.....	3
10	Tabellenverzeichnis	6
11	1 Einleitung	7
12	2 Inbetriebnahme des Smart Meter Gateways	9
13	2.1 Smart Meter Gateway exkl. Sicherheitsmodul (A).....	10
14	2.1.1 Entwicklung.....	10
15	2.1.2 Produktion	10
16	2.1.3 Vor-Personalisierung beim Hersteller.....	10
17	2.2 Sicherheitsmodul (B)	10
18	2.2.1 Entwicklung.....	10
19	2.2.2 Produktion	10
20	2.2.3 Initialisierung.....	11
21	2.3 Smart Meter Gateway inkl. Sicherheitsmodul (C).....	11
22	2.3.1 Vor-Personalisierung und Integration	12
23	2.3.1.1 Vor-Personalisierung 1	13
24	2.3.1.2 Integration.....	14
25	2.3.1.3 Vor-Personalisierung 2	15
26	2.3.2 Installation und Vor-Ort-Inbetriebnahme des SMGW	18
27	2.3.3 Personalisierung	18
28	2.3.4 Normalbetrieb.....	21
29	2.4 Besondere (Sicherheits-)Anforderungen.....	22
30	3 Messung	23
31	3.1 Verortung im Gesamtkontext.....	23
32	3.2 Beteiligte, Rollen und Funktionen	23
33	3.3 Beschreibung und Zweck.....	23
34	3.4 Zeitpunkt	24
35	3.5 Verarbeitete Daten	24
36	3.6 Ort, Art und Weise der Verarbeitung	25
37	3.7 Schnittstellen.....	25
38	3.8 Besondere (Sicherheits-)Anforderungen.....	25
39	3.9 Prozessschritte im Überblick	26
40	4 Datenübertragung	28
41	4.1 Verortung im Gesamtkontext.....	28
42	4.2 Beteiligte, Rollen und Funktionen	28

4 Betriebsprozesse

43	4.3	Beschreibung und Zweck.....	28
44	4.4	Zeitpunkt.....	29
45	4.5	Verarbeitete Daten.....	29
46	4.6	Ort, Art und Weise der Verarbeitung.....	30
47	4.7	Schnittstellen.....	30
48	4.8	Besondere (Sicherheits-)Anforderungen.....	31
49	4.9	Prozessschritte im Überblick.....	31
50	5	Administration.....	34
51	5.1	Verortung im Gesamtkontext.....	34
52	5.2	Beteiligte, Rollen und Funktionen.....	34
53	5.3	Beschreibung und Zweck.....	35
54	5.4	Zeitpunkt.....	36
55	5.5	Verarbeitete Daten.....	36
56	5.6	Ort, Art und Weise der Verarbeitung.....	36
57	5.7	Schnittstellen.....	37
58	5.8	Besondere (Sicherheits-)Anforderungen.....	37
59	5.9	Prozessschritte im Überblick.....	38
60	6	Störungserkennung/Diagnose.....	40
61	6.1	Verortung im Gesamtkontext.....	40
62	6.2	Beteiligte, Rollen und Funktionen.....	40
63	6.3	Beschreibung und Zweck.....	40
64	6.4	Zeitpunkt.....	41
65	6.5	Verarbeitete Daten.....	41
66	6.6	Ort, Art und Weise der Verarbeitung.....	42
67	6.7	Schnittstellen.....	42
68	6.8	Besondere (Sicherheits-)Anforderungen.....	42
69	6.9	Prozessschritte im Überblick.....	43
70	7	Wechsel des Smart Meter Gateway Administrators.....	44
71	7.1	Verortung im Gesamtkontext.....	44
72	7.2	Beteiligte, Rollen und Funktionen.....	44
73	7.3	Beschreibung und Zweck.....	44
74	7.4	Zeitpunkt.....	47
75	7.5	Verarbeitete Daten.....	47
76	7.6	Ort, Art und Weise der Verarbeitung.....	48

5 Betriebsprozesse

77	7.7	Schnittstellen.....	48
78	7.8	Besondere (Sicherheits-)Anforderungen.....	48
79	7.9	Prozessschritte im Überblick	49
81			
80			

82 **Tabellenverzeichnis**

83	Tabelle 1: Prozessschritte Messung	27
84	Tabelle 2: Prozessschritte Datenübertragung.....	33
85	Tabelle 3: Prozessschritte Administration	39
86	Tabelle 4: Prozessschritte Störungserkennung/Diagnose	43
87	Tabelle 5: Prozessschritte Wechsel Smart Meter SMGW-Admin.....	50
88		

89 1 Einleitung

90 Diese Anlage beschreibt wesentliche Betriebsprozesse in Verbindung mit dem Smart Meter Gate-
91 way (SMGW), die im Energiewirtschaftsgesetz (EnWG) und in auf dessen Grundlage erlassenen
92 Rechtsverordnungen sowie in den Schutzprofilen zum Gateway und zum Sicherheitsmodul angelegt
93 sind.

94 Die Betriebsprozesse skizzieren technische Abläufe und mit diesen verbundene organisatorische
95 Aspekte, nicht aber die vertraglichen und daraus abgeleiteten organisatorischen Aspekte im Sinne
96 der Geschäfts- oder Marktprozesse, wie sie in den Geschäftsprozessen zur Kundenbelieferung mit
97 Elektrizität (GPKE) und Wechselprozessen im Messwesen (WiM) dargelegt sind. Die Geschäfts-
98 prozesse sind den hier dargestellten Betriebsprozessen übergeordnet oder laufen parallel zu ihnen.
99 Wo die Geschäfts- bzw. Marktprozesse oder vertragsrechtliche Prozessschritte (z.B. die vertragliche
100 Vereinbarung einer Tarifänderung) Auslöser, Bedingungen/Voraussetzungen oder nachfolgende
101 Ereignisse sind, wird auf sie hingewiesen. Ebenso werden datenschutzrechtliche Anforderungen
102 nicht näher beschrieben, denen der Gesetzgeber allerdings im Rahmen des Smart Metering eine
103 wesentliche Rolle zukommen lässt.¹

104 Ausgangspunkt der hier beschriebenen Prozesse und der damit verbundenen Datenströme ist das
105 SMGW mit seinen Datenerhebungen und -verarbeitungen. Der Fokus liegt auf dem SMGW und auf
106 den Aktivitäten, die der SMGW-Admin im Hinblick auf das SMGW durchführt. Zudem werden die
107 an den einzelnen Prozessen beteiligten Parteien (Stellen/Personen) genannt.

108 Werden im Rahmen der Beschreibung der einzelnen Prozesse bestimmte Beteiligte bzw. Rollen
109 genannt, so gelten die für diese gemachten Angaben auch für von ihnen rechtmäßig eingesetzte au-
110 torisierte Dienstleister.

111 Die in dieser Anlage behandelten Prozesse beschreiben Ausschnitte aus dem Lebenszyklus des
112 SMGW von der Inbetriebnahme bis zur Außerbetriebnahme. Für Prozesse und Arbeitsschritte, die
113 zeitlich vor den energiewirtschaftlichen oder energierechtlichen Prozessen bzw. Aktivitäten² erfol-
114 gen, wozu die Entwicklung, Produktion, Eichung, Beschaffung der SMGW zählen, werden keine
115 Prozessbeschreibungen vorgenommen.

116 Soweit zu den Prozessen bereits wesentliche Aspekte bzw. grundlegende Anforderungen in der BSI
117 TR-03109-1 dargestellt sind, wird auf die entsprechenden Kapitel dieser TR verwiesen.

118 In dieser Anlage werden einige kritische Prozesse beschrieben. Bisher beschrieben sind die folgen-
119 den Prozesse:

- 120 • Inbetriebnahme des Smart Meter Gateways
- 121 • Messung

¹ Wesentliche Anforderungen des Datenschutzes ergeben sich aus § 21g EnWG, vorbehaltlich weiterer Ergänzungen durch Rechtsverordnungen nach § 21i EnWG.

² Beispielsweise der Beginn der Belieferung mit Strom.

- 122 • Datenübertragung
- 123 • Administration
- 124 • Störungserkennung/Diagnose
- 125 • Wechsel des Smart Meter Gateway Administrators
- 126 Die Anlage kann sukzessive um die Beschreibung weiterer Prozesse erweitert werden, wie z.B.
- 127 • Austausch, Hinzufügen oder Entfernen von Zählern
- 128 • Wechsel des Lieferanten
- 129 • Außerbetriebnahme des Smart Meter Gateways
- 130 Die Beschreibungen zu den Prozessen in dieser Anlage sind grundsätzlich nur informativ. Ausnah-
- 131 men können sich dort ergeben, wo es auf die genaue Einhaltung einzelner Schritte ankommt. Diese
- 132 Prozesse bzw. Schritte sind entsprechend gekennzeichnet. Hinsichtlich der Definitionen der in die-
- 133 ser Anlage verwendeten Begriffe wird auf die BSI TR-03109-1 verwiesen.
- 134 Die Darstellung bezieht sich in der vorliegenden Version dieser Anlage vornehmlich auf den Be-
- 135 reich der Elektroenergie.

136

2 Inbetriebnahme des Smart Meter Gateways

137

Dieses Kapitel beschreibt aus technischer Sicht die einzelnen Phasen des Lebenszyklus, die sowohl das Smart Meter Gateway (SMGW) als auch das Sicherheitsmodul nach ihrer Herstellung durchlaufen müssen. Nach der Phase „Integration des Sicherheitsmoduls in das SMGW“ werden die Phasen für das SMGW inkl. Sicherheitsmodul betrachtet. Somit gliedert sich der Lebenszyklus des SMGW in drei Teile:

138

139

140

141

142

- (A) SMGW exklusive Sicherheitsmodul

143

- (B) Sicherheitsmodul

144

- (C) SMGW inklusive Sicherheitsmodul

145

Wenn im Folgenden von Smart Meter Gateway (kurz SMGW) ohne Erwähnung des Sicherheitsmoduls gesprochen wird, so ist hier ein SMGW inkl. Sicherheitsmodul gemeint.

146

147

Zur Inbetriebnahme des gesamten Messsystems ist es neben der hier beschriebenen Inbetriebnahme des SMGW erforderlich, mindestens einen Zähler mit dem SMGW zu verbinden. Dieses wird durch einen weiteren Prozess in dieser Anlage beschrieben werden. Die Reihenfolge, in der diese beiden Inbetriebnahme-Prozesse durchlaufen werden, ist dabei unerheblich.

148

149

150

151

152

Grundsätzliche Anmerkungen:

153

Für die Inbetriebnahme des Messsystems besteht die zwingende Notwendigkeit, dass am Installationsort eine stabile WAN-Verbindung etabliert werden kann. Dem Gateway Administrator sind des Weiteren der Installationsplatz, der Energiekunde und der Tarif des Energiekunden bekannt.

154

155

156

Im Vorfeld der nachfolgenden Prozessschritte ist auf die umfassende Abstimmung zwischen den etablierten Marktrollen und dem SMGW-Admin hinzuweisen. Die Erfassung der Kriterien für den Einbau der SMGW bedingt einen Informationsaustausch des Lieferanten und Messstellenbetreibers mit dem Verteilnetzbetreiber über die Marktkommunikation³. Gleichmaßen müssen die Zertifikate über die Marktkommunikation rechtzeitig an den SMGW-Admin übermittelt werden.

157

158

159

160

161

Die Details der komplexen Abstimmungsprozesse als Vorbedingung für den Einbau und Betrieb von SMGW sind eingehend zwischen BNetzA und Verbänden abzustimmen. Sie bedingen ebenfalls Verpflichtungen Dritter und haben Auswirkungen auf Fristen, die vom Ordnungsgeber⁴ zu berücksichtigen sind.

162

163

164

³ Unter Marktkommunikation wird die Kommunikation zwischen dem Smart Meter Gateway Administrator und den Externen Marktteilnehmern bzw. zwischen Letzteren verstanden. Die Marktkommunikation (auch Marktprozesse oder Geschäftsprozesse genannt) wird in dieser Technischen Richtlinie nicht betrachtet, sondern wird insbesondere in Festlegungen der Bundesnetzagentur beschrieben bzw. geregelt.

⁴ Im Rahmen der nach § 21i EnWG zu erlassenden bzw. zu novellierenden Rechtsverordnungen.

165 **2.1 Smart Meter Gateway exkl. Sicherheitsmodul (A)**

166 **2.1.1 Entwicklung**

167 **Rolle:**

168 Hersteller des SMGW

169 **Beschreibung:**

170 Entwicklung des SMGW beim Hersteller.

171 **2.1.2 Produktion**

172 **Rolle:**

173 Hersteller des SMGW

174 **Beschreibung:**

175 Produktion des SMGW beim Hersteller.

176 **2.1.3 Vor-Personalisierung beim Hersteller**

177 **Rolle:**

178 Hersteller des SMGW

179 **Beschreibung:**

180 Einspielung der initialen und CC-zertifizierten Firmware gemäß zertifiziertem Produktionsprozess
181 in das SMGW.

182 Vergabe einer eindeutigen SMGW-ID gemäß der Norm DIN 43863-5:2012-04 "Herstellerübergrei-
183 fende Identifikationsnummer für Messeinrichtungen".

184 **2.2 Sicherheitsmodul (B)**

185 **2.2.1 Entwicklung**

186 **Rolle:**

187 Hersteller des Sicherheitsmoduls

188 **Beschreibung:**

189 Entwicklung des Sicherheitsmoduls beim Hersteller.

190 **2.2.2 Produktion**

191 **Rolle:**

192 Hersteller des Sicherheitsmoduls

193 **Beschreibung:**

194 Produktion des Sicherheitsmoduls und Einspielung des Betriebssystems beim Hersteller.

195 **2.2.3 Initialisierung**

196 **Rolle:**

197 Initialisierer des Sicherheitsmoduls

198 **Beschreibung:**

199 Einspielung des Dateisystems und ggf. Patches für das Betriebssystem auf dem Sicherheitsmodul.

200

201 **2.3 Smart Meter Gateway inkl. Sicherheitsmodul (C)**

202 Der weitere Lebenszyklus des SMGW gliedert sich in folgende aufeinander aufbauende Phasen:

- 203 • Vor-Personalisierung und Integration von Sicherheitsmodul und SMGW (siehe Ziffer 2.3.1)
- 204 • Installation und Vor-Ort-Inbetriebnahme des SMGW (siehe Ziffer 2.3.2)
- 205 • Personalisierung des SMGW (siehe Ziffer 2.3.3)
- 206 • Normalbetrieb des SMGW („End-Usage“ mit Administration und Smart Meter-Wirkbetrieb,
207 siehe Ziffer 2.3.4)

208 Im Folgenden erfolgt eine detaillierte Beschreibung der zuvor genannten Phasen. Dabei werden
209 zum einen die durchzuführenden Aufgaben und Randbedingungen benannt. Zum anderen werden
210 jeweils auch die beteiligten Rollen, die einen Zugriff auf das SMGW bzw. auf das Sicherheitsmodul
211 haben, zugeordnet.

212 Folgende Rollen sind in den weiteren Phasen der „Inbetriebnahme“ involviert:

- 213 • Integrator (zuständig für die Integration von Sicherheitsmodul und SMGW)
- 214 • Erstkonfigurator (für die Parametrierung der Kommunikationsschnittstellen des SMGW im
215 Rahmen der Inbetriebnahme)
- 216 • SMGW-Admin (eigene Rolle, zuständig für die Administration des SMGW)

217 Darüber hinaus stützen sich die nachfolgend beschriebenen Phasen ausschließlich auf die für das
218 Smart Meter-System vorgesehene SM-PKI (siehe TR-03109-4).

219 **Hinweis:** Das Gateway besitzt eine lokale Schnittstelle, die im Rahmen der Phasen „Vor-
220 Personalisierung + Integration von Sicherheitsmodul und Gateway“ durch den Integrator und
221 „Installation + Vor-Ort-Inbetriebnahme des SMGW“ durch den Erstkonfigurator zum Daten-
222 import/-export bzw. zur Konfiguration genutzt werden kann. Aus Sicherheitsgründen ist diese
223 lokale Schnittstelle möglichst schlank gehalten und wird auf die unbedingt erforderliche

224 Funktionalität und den unbedingt notwendigen Datentransport beschränkt (siehe [TR-03109-
225 1] und [TR-03109-1A]).

226 Für die lokale Schnittstelle des Gateways ist aus physikalischer Sicht die HAN-Schnittstelle
227 des Gateways vorgesehen. Die Nutzung dieser lokalen Schnittstelle des Gateways in den Pha-
228 sen „Vor-Personalisierung + Integration von Sicherheitsmodul und Gateway“ und „Installati-
229 on + Vor-Ort-Inbetriebnahme des SMGW“ ist über einen geeigneten PIN-Mechanismus im
230 Gateway abgesichert. Der Integrator bzw. der Erstkonfigurator hat sich für eine Nutzung der
231 lokalen Schnittstelle des Gateways mittels PIN gegenüber dem Gateway zu authentisieren,
232 wobei Integrator und Erstkonfigurator jeweils eine eigene PIN verwenden („Integrator-PIN“,
233 „Erstkonfigurator-PIN“). Die Rolle des Erstkonfigurators erhält über die lokale Schnittstelle
234 keine Integrator-Rechte zur Vor-Personalisierung und Integration des Sicherheitsmoduls.

235 Der PIN-Mechanismus ist allein Aufgabe des Gateways; das Sicherheitsmodul ist in diesen
236 Mechanismus nicht involviert und leistet auch keinen weiteren funktionalen oder sicherheits-
237 technischen Beitrag zur Absicherung der lokalen Schnittstelle des Gateways. Die lokale
238 Schnittstelle des Gateways und ihr PIN-Sicherungsmechanismus ist Gegenstand der CC-
239 Zertifizierung des Gateways (CC-Aspekt ALC_DEL).

240 Die PIN-gesicherte lokale Schnittstelle des Gateways ist nur in den Phasen „Vor-
241 Personalisierung + Integration von Sicherheitsmodul und Gateway“ und „Installation + Vor-
242 Ort-Inbetriebnahme des SMGW“ verfügbar und wird mit Ende der Phase „Installation + Vor-
243 Ort-Inbetriebnahme des SMGW“ deaktiviert.

244 2.3.1 Vor-Personalisierung und Integration

245 Diese Phase dient der Integration von Gateway und (initialisiertem) Sicherheitsmodul sowie dem
246 Generieren und Aufbringen von initialem Schlüssel- und Zertifikatsmaterial.

247 Die hier beschriebene Phase setzt sich aus den Teilphasen der *Vor-Personalisierung* und der *In-*
248 *tegration* zusammen und wird beim Integrator durchgeführt. Die *Vor-Personalisierung* gliedert sich
249 dabei in zwei Teilphasen. Während in der Teilphase *Vor-Personalisierung 1* Schlüssel- und Zertifi-
250 katsmaterial generiert und aufgebracht wird, das unabhängig vom späteren SMGW-Admin ist, wird
251 in der Teilphase *Vor-Personalisierung 2* vom SMGW-Admin spezifisches Schlüssel- und Zertifi-
252 katsmaterial in das SMGW importiert.

253 Hinsichtlich der Reihenfolge der Teilphasen *Vor-Personalisierung 1*, *Vor-Personalisierung 2* und
254 *Integration* gilt:

- 255 • Die *Vor-Personalisierung 1* findet vor der *Vor-Personalisierung 2* statt.
- 256 • Die Integration findet alternativ vor der *Vor-Personalisierung 1* oder direkt danach statt
257 (also vor der *Vor-Personalisierung 2*).

258 **Hinweis:** Für den Import von Schlüsseln in dieser Phase werden sog. Import-Schlüssel ver-
259 wendet, siehe Dokument *Smartmeter SecMod – Filesystem, Zugriffsregeln und Kommandoset*,

260 Kap. 1.2. Initiale Import-Schlüssel werden bereits im Rahmen der Produktion (Initialisierung)
261 aufgebracht. Zum Abschluss der Phase *Vor-Personalisierung und Integration von Sicher-*
262 *heitsmodul und Gateway* müssen sämtliche Import-Schlüssel im Sicherheitsmodul (Key Pair-
263 Objekte, Public Key-Objekte) sicher gelöscht werden.

264 2.3.1.1 Vor-Personalisierung 1

265 **Rolle:**

266 Integrator

267 **Anforderungen an den Integrator:**

- 268 • Beim Integrator besteht eine ausreichend durch technische, organisatorische und personelle
269 Sicherheitsmaßnahmen gesicherte Umgebung.
- 270 • Sicherheitsmodul-spezifische weitere technische Sicherungsmaßnahmen sind zulässig. Ggf.
271 wird dazu erforderliches Sicherungsmaterial (z.B. Keys, PINs) im Rahmen des Initiali-
272 sierungsprozesses im Sicherheitsmodul hinterlegt und soweit erforderlich an den Integrator
273 zur Nutzung ausgeliefert. Hierzu setzen viele Sicherheitsmodul-Hersteller auf übliche
274 Sicherheitsmechanismen auf. In der [TR-03109] und im Protection Profile [PP 0077] zum
275 Sicherheitsmodul werden keine konkreten Sicherheitsmechanismen festgeschrieben, um den
276 Herstellern von Sicherheitsmodulen genügend Freiraum für ihre spezifischen, ggf. bereits
277 etablierten Sicherheitsmechanismen zu lassen.

278 **Aufgaben in der Vor-Personalisierung 1 von Sicherheitsmodul und Gateway:**

- 279 • Import des SM-PKI-Root-Zertifikates (ROOT_WAN_SIG_CRT) in das Sicherheitsmodul
280 **Hinweis:** Das SM-PKI-Root-Zertifikat stellt nachfolgend einen zentralen Sicherheitsanker
281 dar; seine Integrität und Authentizität ist daher sicherzustellen. Es erfolgt eine
282 vertrauenswürdige Übermittlung des Zertifikats an den Integrator. Die Authentizität wird
283 z.B. über einen Abgleich eines Fingerprints über einen zweiten Kanal sichergestellt.
 - 284 • Onboard-Generierung von Key-Paaren für das SMGW im Sicherheitsmodul (vorläufige
285 SMGW-Schlüssel für die WAN-Kommunikation):
 - 286 ○ (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
 - 287 ○ (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
 - 288 ○ (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)
 - 289 • Export der Public Keys:
 - 290 ○ GW_WAN_TLS_PUB_PRE
 - 291 ○ GW_WAN_SIG_PUB_PRE
 - 292 ○ GW_WAN_ENC_PUB_PRE
- 293 **Hinweis:** Die zugehörigen privaten Schlüssel verbleiben im Sicherheitsmodul und können
294 nicht ausgelesen werden.

- 295 • Erstellung von entsprechenden Zertifikatsrequests für die Gütesiegel-Zertifikate zu den
296 SMGW-Schlüsseln
- 297 • Senden der Requests „an die SM-PKI“
- 298 **Hinweis:** Hierzu benötigt der Integrator eine Verbindung zur SM-PKI. Es besteht hierbei
299 die Möglichkeit, dass der Integrator selbst eine Sub-CA in der SM-PKI betreibt.
- 300 • Import der Gütesiegel-Zertifikate in das Sicherheitsmodul:
- 301 ○ GW_WAN_TLS_CRT_PRE
- 302 ○ GW_WAN_SIG_CRT_PRE
- 303 ○ GW_WAN_ENC_CRT_PRE
- 304 **Hinweis:** Sämtliches im Rahmen der *Vor-Personalisierung 1* generiertes bzw. eingebrachtes
305 Schlüssel- und Zertifikatsmaterial ist unabhängig vom späteren konkreten SMGW-Admin.
- 306 **Hinweis:** Findet die Teilphase *Integration* vor der *Vor-Personalisierung 1* statt, ist die lokale
307 Schnittstelle des SMGW unter Nutzung der Integrator-PIN erforderlich.

308 2.3.1.2 Integration

309 **Rolle:**

310 Integrator

311 **Aufgaben in der *Integration* von Sicherheitsmodul und Gateway:**

- 312 • Einbau des Sicherheitsmoduls in das Gateway und Verbindung der Komponenten
- 313 • Generierung der Schlüssel für die Speicherverschlüsselung des SMGW
- 314 • ggf. Import der Schlüssel in das Sicherheitsmodul

315 Bei der ersten Inbetriebnahme des SMGW wird im SMGW eine Gateway-System-PIN generiert
316 und im Sicherheitsmodul gespeichert. Über die PIN wird eine Bindung zwischen SMGW und Si-
317 cherheitsmodul (sog. Pairing zwischen SMGW und Sicherheitsmodul) erreicht.

318 **Hinweis:** Findet die *Vor-Personalisierung 1* vor der *Integration* von Sicherheitsmodul und
319 SMGW statt, so ist bei dieser Reihenfolge ein direkter Zugriff auf das Sicherheitsmodul für
320 seine *Vor-Personalisierung 1* ohne Nutzung der lokalen Schnittstelle des SMGW möglich.
321 Sollte auf Seiten des Herstellers bzw. Integrators die *Vor-Personalisierung 1* erst nach der
322 *Integration* von Sicherheitsmodul und SMGW stattfinden und daher kein direkter Zugriff auf
323 das Sicherheitsmodul für seine *Vor-Personalisierung 1* mehr möglich sein, so ist die lokale
324 Schnittstelle des SMGW für die *Vor-Personalisierung 1* zu nutzen.

325

326

327 **2.3.1.3 Vor-Personalisierung 2**

328 **Rolle:**

329 Integrator

330 **Voraussetzungen:**

331 • Die *Vor-Personalisierung 1* und die *Integration* von Sicherheitsmodul und SMGW sind
332 abgeschlossen.

333 • Zum Zeitpunkt der *Vor-Personalisierung 2* ist der konkrete SMGW-Admin bekannt.

334 • Der SMGW-Admin hat seine Schlüsselpaare generiert:

335 ○ (GWADM_TLS_PRV, GWADM_TLS_PUB)

336 ○ (GWADM_SIG_PRV, GWADM_SIG_PUB)

337 ○ (GWADM_ENC_PRV, GWADM_ENC_PUB)

338 ○ (GWADM_AUT_PRV, GWADM_AUT_PUB)

339 **Hinweis:** An die Schlüsselgenerierung beim SMGW-Admin bestehen spezifische Anforde-
340 rungen wie z.B. die Nutzung eines HSM (siehe TR-03109-4).

341 • Der SMGW-Admin besitzt für seine zuvor genannten Schlüsselpaare jeweils ein Zertifikat
342 der SM-PKI, also:

343 ○ GWADM_TLS_CRT

344 ○ GWADM_SIG_CRT

345 ○ GWADM_ENC_CRT

346 ○ GWADM_AUT_CRT

347 • Der SMGW-Admin erstellt eine sog. Initiale Konfigurationsdatei, die mindestens die
348 folgenden Daten beinhaltet:

349 ○ Kommunikationsparameter des SMGW-Admins (SMGW-Admin-Adresse)

350 ○ Zertifikate GWADM_TLS_CRT, GWADM_SIG_CRT, GWADM_ENC_CRT und
351 GWADM_AUT_CRT mit zugehöriger Zertifikatskette (aus der SM-PKI) exklusive
352 SM-PKI-Root-Zertifikat

353 • Der SMGW-Admin signiert die Initiale Konfigurationsdatei mit seinem Signaturschlüssel
354 GWADM_SIG_PRV.

355 • Die signierte Initiale Konfigurationsdatei wird an den Integrator übermittelt.

356 **Aufgaben in der Teilphase Vor-Personalisierung 2:**

357 Einspielen der Kommunikationsparameter und Zertifikate des SMGW-Administrators unter Nut-
358 zung der lokalen Schnittstelle des SMGW, hierzu:

- 359 • Der Integrator authentisiert sich gegenüber dem SMGW (unter Nutzung der Integrator-PIN)
360 und schaltet damit die lokale Schnittstelle des SMGW für die *Vor-Personalisierung 2* frei;
- 361 • der Integrator spielt über die lokale Schnittstelle die vom SMGW-Admin signierte Initiale
362 Konfigurationsdatei ein; Speicherung der Zertifikate und Zertifikatsketten im SMGW;
- 363 • Import der Public Keys des SMGW-Admins in das Sicherheitsmodul (enthalten in der
364 Initialen Konfigurationsdatei);
- 365 • im SMGW erfolgt automatisch die Überprüfung der in der Initialen Konfigurationsdatei
366 gelieferten Zertifikate des SMGW-Admins aus der SM-PKI; dies erfolgt unter Verwendung
367 der mitgelieferten Zertifikatsketten und des SM-PKI-Root-Zertifikats, das im Rahmen der
368 *Vor-Personalisierung 1* als Sicherheitsanker integer und authentisch in das Sicherheits-
369 modul eingebracht wurde und dort hinterlegt ist (s.o.);

370 **Hinweis:** Das Sicherheitsmodul unterstützt durch Bereitstellen der Kernroutine zur Signa-
371 turprüfung die Prüfung von X.509-Zertifikaten und -Zertifikatsketten. Die Prüfung von
372 X.509-Zertifikaten und -Zertifikatsketten findet im SMGW statt, wozu sich das SMGW der
373 Signaturprüfungsroutine des Sicherheitsmoduls bedient und die Daten für die Signaturprü-
374 fung im Sicherheitsmodul entsprechend aufbereitet. Das Sicherheitsmodul selbst stellt keine
375 komplette Funktionalität zur Prüfung von X.509-Zertifikaten und -Zertifikatsketten bereit
376 (üblicherweise prüfen Chipkarten allenfalls CV-Zertifikate; für die Prüfung von X.509-
377 Zertifikaten müssten proprietäre Routinen aufgesetzt werden);

- 378 • im SMGW erfolgt automatisch die Überprüfung der Signatur der Initialen Konfigurationsda-
379 tei;
- 380 • erst nach erfolgreicher Überprüfung der Zertifikate aus der SM-PKI und der Signatur der
381 Initialen Konfigurationsdatei werden die Kommunikationsdaten des SMGW-Admins (wie in
382 der Initialen Konfigurationsdatei geliefert) für ihre weitere Verwendung freigeschaltet bzw.
383 im SMGW gespeichert.

384 **Hinweis:** Die in der Phase *Vor-Personalisierung und Integration von Sicherheitsmodul und*
385 *Gateway* erforderliche sog. Initiale Konfigurationsdatei des SMGW-Admins für den Integrator
386 soll aus Sicherheitsgründen nur in dieser Phase verwendet werden können, da mit der Initialen
387 Konfigurationsdatei sicherheitskritische Schlüssel des SMGW-Admins importiert werden.

388 Zusammenfassung des am Ende dieser Phase vorliegenden Schlüssel- und Zertifikatsmaterials:

- 389 • Im Sicherheitsmodul
- 390 ○ Gateway-System-PIN (Referenzwert)
 - 391 ○ ggf. Schlüssel für die Speicherverschlüsselung des SMGW
 - 392 ○ Zertifikat ROOT_WAN_SIG_CRT der SM-PKI-Root
 - 393 ○ vorläufige Gateway-Schlüsselpaare

- 394 ▪ (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
- 395 ▪ (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
- 396 ▪ (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)
- 397 ○ Gütesiegel-Zertifikate
 - 398 ▪ GW_WAN_TLS_CRT_PRE
 - 399 ▪ GW_WAN_SIG_CRT_PRE
 - 400 ▪ GW_WAN_ENC_CRT_PRE
- 401 ○ Public Keys des SMGW-Admin
 - 402 ▪ GWADM_TLS_PUB
 - 403 ▪ GWADM_SIG_PUB
 - 404 ▪ GWADM_ENC_PUB
 - 405 ▪ GWADM_AUT_PUB
- 406 ● Im Smart Meter Gateway
 - 407 ○ Gateway-System-PIN
 - 408 ○ Schlüssel für die Speicherverschlüsselung des SMGW
 - 409 ○ Zertifikate des SMGW-Admin
 - 410 ▪ GWADM_TLS_CRT
 - 411 ▪ GWADM_SIG_CRT
 - 412 ▪ GWADM_ENC_CRT
 - 413 ▪ GWADM_AUT_CRT
 - 414 jeweils inkl. der zugehörigen Zertifikatskette (aus der SM-PKI) exklusive des SM-
 - 415 PKI-Root-Zertifikats
 - 416 ○ Kommunikationsparameter des SMGW-Admin (SMGW-Admin-Adresse)
 - 417
 - 418

419 **2.3.2 Installation und Vor-Ort-Inbetriebnahme des SMGW**

420 **Rolle:**

421 Erstkonfigurator

422 **Vorbedingungen:**

423 Die Phase *Vor-Personalisierung und Integration* (Ziffer 2.3.1) ist abgeschlossen.

424 **Aufgaben in dieser Phase:**

- 425 • Installationstätigkeiten (z.B. Einbau des SMGW beim Anschlussnehmer);
- 426 • Konfiguration des SMGW (z.B. Parametrierung und Konfiguration der physikalischen
427 Kommunikationsschnittstellen des SMGW);
- 428 • weitere Inbetriebnahme-Tätigkeiten (z.B. Diagnose mit lesendem Zugriff auf System-Log);
- 429 • falls erforderlich Update der Kommunikationsadresse des SMGW-Admins. Hierzu
430 authentisiert sich der Erstkonfigurator gegenüber dem SMGW (unter Nutzung der Erstkon-
431 figurator-PIN) und schaltet damit die lokale Schnittstelle des SMGW für die Übergabe der
432 neuen SMGW-Admin-Adresse an das SMGW frei;
- 433 • zum Abschluss dieser Phase *Installation und Vor-Ort-Inbetriebnahme des SMGW* wird die
434 lokale Schnittstelle des SMGW deaktiviert.

435 **2.3.3 Personalisierung**

436 Diese Phase beinhaltet insbesondere die initiale Konfiguration des SMGW durch den SMGW-
437 Admin und die Installation der Betriebsschlüssel.

438 **Rolle:**

439 SMGW-Admin

440 **Aufgaben in der *Personalisierung* des SMGW:**

- 441 • Das SMGW verbindet sich im WAN mit der im SMGW gespeicherten SMGW-Admin-
442 Adresse;
- 443 • Aufbau eines TLS-Kanals zwischen SMGW-Admin und SMGW, hierbei:
 - 444 ○ Nutzung der vorläufigen Gateway-Schlüssel (GW_WAN_TLS_PRIV_PRE,
445 GW_WAN_TLS_PUB_PRE) und des zugehörigen Gütesiegel-Zertifikats
446 GW_WAN_TLS_CRT_PRE;
 - 447 ○ Nutzung der SMGW-Admin-Schlüssel für TLS; das Zertifikat GWADM_TLS_CRT
448 liegt bereits aus der *Vor-Personalisierung und Integration von Sicherheitsmodul und*
449 *Gateway* im SMGW vor (und wurde dort mit seiner Zertifikatskette bis zur Root
450 geprüft); ferner liegt der Public Key GWADM_TLS_PUB bereits aus der *Vor-*

451 *Personalisierung und Integration von Sicherheitsmodul und Gateway im*
452 *Sicherheitsmodul vor.*

453 **Hinweis:** Aus der *Vor-Personalisierung und Integration von Sicherheitsmodul und*
454 *Gateway* liegen auch bereits die Zertifikate GWADM_SIG_CRT,
455 GWADM_ENC_CRT und GWADM_AUT_CRT im SMGW vor (und wurden dort mit
456 ihrer Zertifikatskette bis zur Root geprüft), so dass diese ebenfalls nicht mehr
457 personalisiert werden müssen; auch liegen die zugehörigen Public Keys
458 GWADM_SIG_PUB, GWADM_ENC_PUB und GWADM_AUT_PUB bereits aus der
459 *Vor-Personalisierung und Integration von Sicherheitsmodul und Gateway im*
460 *Sicherheitsmodul vor.*

461 • Authentisierung des SMGW-Admins gegenüber dem Sicherheitsmodul für die folgenden
462 Administrationstätigkeiten am Sicherheitsmodul (unter Nutzung der SMGW-Admin-
463 Schlüssel (GWADM_AUT_PRV, GWADM_AUT_PUB));

464 • Installation der Betriebsschlüssel sowie der Betriebszertifikate aus der SM-PKI im TLS-
465 Kanal, hierzu:

466 ○ auf Seiten des SMGW-Admins und des SMGW insbesondere Nutzung der SMGW-
467 Admin-Schlüssel (GWADM_SIG_PRV, GWADM_SIG_PUB) und
468 (GWADM_ENC_PRV, GWADM_ENC_PUB) und deren SM-PKI-Zertifikate sowie
469 Nutzung der vorläufigen Gateway-Schlüssel (GW_WAN_SIG_PRV_PRE,
470 GW_WAN_SIG_PUB_PRE) und (GW_WAN_ENC_PRV_PRE,
471 GW_WAN_ENC_PUB_PRE) und deren zugehörigen Gütesiegel-Zertifikate für die
472 im folgenden benötigten Administrationskommandos (Sicherung der Kommandos
473 mit Inhaltsdatenverschlüsselung und -signatur);

474 ○ Onboard-Generierung von neuen Schlüsselpaaren für das SMGW im
475 Sicherheitsmodul (Gateway-Betriebsschlüssel):

476 ▪ (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB)

477 ▪ (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB)

478 ▪ (GW_WAN_ENC_PRV, GW_WAN_ENC_PUB)

479 ○ Export der Public Keys GW_WAN_TLS_PUB, GW_WAN_SIG_PUB,
480 GW_WAN_ENC_PUB (die zugehörigen privaten Schlüssel verbleiben im Sicher-
481 heitsmodul und können nicht ausgelesen werden);

482 ○ Erstellung von entsprechenden Zertifikatsrequests für die Betriebszertifikate zu den
483 neuen SMGW-Schlüsseln und Senden des Requests „an die SM-PKI“;

484 ○ Import der „aus der SM-PKI“ gelieferten Betriebszertifikate GW_WAN_TLS_CRT,
485 GW_WAN_SIG_CRT, GW_WAN_ENC_CRT in das SMGW und Speicherung im
486 SMGW;

- 487 • Schließen des TLS-Kanals zwischen SMGW-Admin und SMGW.
- 488 Mit Abschluss der Personalisierung befindet sich das SMGW in seinem zertifizierten Zustand. Das
489 SMGW steht nun für die Nutzung im Normalbetrieb bereit.
- 490 Der SMGW-Admin kann nachfolgend weitere Administrationstätigkeiten am SMGW bzw. am Si-
491 cherheitsmodul vornehmen, siehe Kapitel 2.3.4.
- 492 Zusammenfassung des am Ende dieser Phase vorliegenden Schlüssel- und Zertifikatsmaterials:
- 493 • Im Sicherheitsmodul
- 494 ○ Gateway-System-PIN (Referenzwert)
- 495 ○ ggf. Schlüssel für die Speicherverschlüsselung des SMGW
- 496 ○ Zertifikat ROOT_WAN_SIG_CRT der SM-PKI-Root
- 497 ○ vorläufige Gateway-Schlüsselpaare
- 498 ▪ (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
- 499 ▪ (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
- 500 ▪ (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)
- 501 ○ Gütesiegel-Zertifikate
- 502 ▪ GW_WAN_TLS_CRT_PRE
- 503 ▪ GW_WAN_SIG_CRT_PRE
- 504 ▪ GW_WAN_ENC_CRT_PRE
- 505 ○ Public Keys des SMGW-Admin
- 506 ▪ GWADM_TLS_PUB
- 507 ▪ GWADM_SIG_PUB
- 508 ▪ GWADM_ENC_PUB
- 509 ▪ GWADM_AUT_PUB
- 510 ○ Gateway-Betriebsschlüsselpaare
- 511 ▪ (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB)
- 512 ▪ (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB)
- 513 ▪ (GW_WAN_ENC_PRV, GW_WAN_ENC_PUB)

- 514 • Im Smart Meter Gateway
- 515 ○ Gateway-System-PIN
- 516 ○ Schlüssel für die Speicherverschlüsselung des SMGW
- 517 ○ Zertifikate des SMGW-Admin:
 - 518 ▪ GWADM_TLS_CRT
 - 519 ▪ GWADM_SIG_CRT
 - 520 ▪ GWADM_ENC_CRT
 - 521 ▪ GWADM_AUT_CRT
- 522 jeweils inkl. der zugehörigen Zertifikatskette (aus der SM-PKI) exklusive des SM-
- 523 PKI-Root-Zertifikats
- 524 ○ Kommunikationsparameter des SMGW-Admin (SMGW-Admin-Adresse)
- 525 ○ Betriebszertifikate
 - 526 ▪ GW_WAN_TLS_CRT
 - 527 ▪ GW_WAN_SIG_CRT
 - 528 ▪ GW_WAN_ENC_CRT

529 **2.3.4 Normalbetrieb**

530 Nach erfolgreichem Aufbau eines neuen TLS-Kanals muss der SMGW-Admin das SMGW zur
531 Aufnahme des Messbetriebs weiter konfigurieren. Der SMGW-Admin führt zunächst folgende
532 Schritte aus:

- 533 • Zeitsynchronisation zwischen SMGW und SMGW-Admin,
- 534 • ggf. Firmware- und/oder Software-Update,
- 535 • Selbsttest des SMGW.

536 Anschließend kann das SMGW für den Beginn des Messbetriebs konfiguriert werden. Hierzu wer-
537 den vom SMGW-Admin insbesondere folgende Informationen auf das SMGW übertragen:

- 538 • Zertifikate und Schlüsselmaterial für die angeschlossenen Zähler (notwendig für das Pairing
539 von SMGW und Zählern),
- 540 • Profile (z.B. Tarifprofil, Kommunikationsprofile),

541 • ggf. Zertifikate und Schlüsselmaterial für die HAN-Schnittstelle (notwendig für das Pairing
542 mit der Anzeigeeinheit und ggf. für das Pairing mit CLS).

543 Vor Beginn des eigentlichen Messbetriebs ist es notwendig, die Zähler mit dem SMGW zu pairen.

544 Vor der Speicherung der empfangenen Administratorkommandos und Konfigurationsdaten prüft
545 das SMGW jeweils die beigefügte Signatur anhand des hinterlegten Zertifikats des SMGW-
546 Admins.

547 Im Rahmen der Marktkommunikation sind ggf. nach Aufnahme des Messbetriebs Informationen
548 vom SMGW-Admin an alle beteiligten externen Marktteilnehmer zu senden.⁵

549 Anschließend können weitere, hier im Anhang definierte, Prozesse durchlaufen werden.

550 **2.4 Besondere (Sicherheits-)Anforderungen⁶**

551 Während der Lagerung und beim Transport von vor-personalisierten SMGW, initialisierten Sicher-
552 heitsmodulen sowie von integrierten und personalisierten SMGW sind dem jeweiligen Schutzbedarf
553 angemessene Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit umzusetzen.

⁵ Die Marktkommunikation liegt in der Zuständigkeit der Bundesnetzagentur.

⁶ Bezüglich der Sicherheitsanforderungen sind die Vorgaben der TR-03109 insgesamt zu beachten. Hier werden nur bestimmte Aspekte hervorgehoben oder ergänzt.

554 **3 Messung**

555 **3.1 Verortung im Gesamtkontext**

556 Nachdem das Smart Meter Gateway (SMGW) installiert und initialisiert worden ist und die erforderlichen Profile eingerichtet und vom SMGW aktiviert worden sind (siehe den Prozess *Inbetriebnahme des Smart Meter Gateways*), kann die Messung (der Entnahme oder Einspeisung) von Elektrizität, Gas, Wasser, Wärme und anderen zu messenden Energien oder Stoffen und die Messung von Netzzustandsdaten beginnen.

561 Die von den Messeinrichtungen an das SMGW übertragenen Messdaten werden im SMGW gespeichert. In der Folge werden diese Daten vom SMGW in seiner Funktion als „Datenaufbereiter“ verarbeitet (siehe BSI TR-03109-1, Kapitel 4) und die Ergebnisse dieser Verarbeitung werden vom SMGW an autorisierte Empfänger übertragen (siehe den Prozess *Datenübertragung*).

565 **3.2 Beteiligte, Rollen und Funktionen**

- 566 • Smart Meter Gateway Administrator (SMGW-Admin)

567 Der Prozess der Messung und Messwertaufbereitung läuft automatisch ab.

568 Der SMGW-Admin überwacht den gesamten Prozess kontinuierlich.⁷

569 **3.3 Beschreibung und Zweck**

570 Zweck der Messung und Messwertaufbereitung ist die Verfügbarmachung von Werten zur Abrechnung der bezogenen und eingespeisten Energie- oder Stoffmengen sowie die für den Zustand der Netzauslastung erforderlichen Entnahme-/Bezugs-, Einspeise-/Liefer- und Statusdaten.

573 Der Prozess der Messung besteht aus den folgenden Hauptteilen:

- 574 • Messung
- 575 • Übertragung der Messwerte von der Messeinrichtung an das SMGW
- 576 • Auswertung der Messwerte im SMGW
- 577 • Speicherung der Messwerte im SMGW

578 Zusätzlich werden folgende Nebenprozesse durchgeführt:

- 579 • Überwachung der Funktionen des SMGW durch den SMGW-Admin
- 580 • Protokollierung in den Logs

⁷ Zu den Aufgaben des SMGW-Admin gehört die regelmäßige Überwachung der Gateway-Funktionalität. Dazu zählt insbesondere die anlassbezogene bzw. kontinuierliche, d.h. regelmäßige Auswertung der Logs.

581 Die Messung erfolgt durch die an das SMGW lokal angeschlossene/n Messeinrichtung/en. Eine
582 Beschreibung dieser Messung erfolgt in der Technischen Richtlinie nicht.

583 Die Übertragung der Messwerte von den lokal angeschlossenen Messeinrichtungen an das SMGW
584 erfolgt gemäß BSI TR-03109-1.

585 Nach der Messwerterfassung entschlüsselt das SMGW den Datensatz (die Messwerte), wertet das
586 jeweilige Anwendungsprotokoll aus und prüft die Integrität der Messwerte (vgl. BSI TR-03109-1).

587 Die Messwerte werden vom SMGW mit einem Zeitstempel und mit der Information versehen, ob
588 der Wert gültig oder ungültig ist, und sodann im SMGW unverändert⁸ und unveränderbar gespei-
589 chert (vgl. BSI TR-03109-1).

590 Der SMGW-Admin überwacht die Übertragung der Messwerte von den Messeinrichtungen an das
591 SMGW und den Prozess im SMGW kontinuierlich. Das SMGW protokolliert während des gesam-
592 ten Prozesses alle Aktionen des SMGW und des SMGW-Admins in den entsprechenden Logs (vgl.
593 BSI TR-03109-1).

594 **3.4 Zeitpunkt**

595 Der SMGW-Admin legt gemäß den vertraglichen Vereinbarungen zwischen den Beteiligten (Liefe-
596 rant[en], Endkunde[n]/Anschlussnehmer/Anschlussnutzer, weitere Dienstleister), gemäß den Aus-
597 wertungsprofilen und gemäß den technischen Voraussetzungen der angeschlossenen Messeinrich-
598 tungen die Zeitabstände fest, in denen das SMGW die Messwerte von den Messeinrichtungen emp-
599 fängt oder erfragt.

600 Die Entschlüsselung, Validierung und Auswertung der Messwerte und die Speicherung der mit
601 Zeitstempel versehenen Einträge erfolgen im SMGW so zügig wie technisch möglich nach der
602 Messwertübertragung.

603 **3.5 Verarbeitete Daten**

604 **Primärdaten⁹**

- 605 • Zähler-ID
- 606 • Zählpunktbezeichnung
- 607 • Messwerte
- 608 • Zeitstempel
- 609 • Information, ob der Wert gültig oder ungültig ist
- 610 • Wandlerfaktor

⁸ Gegebenenfalls wird dem Messwert ein Faktor (MeterValueFactor) gemäß BSI TR-03109-1 zugewiesen.

⁹ Primärdaten sind Daten, auf deren Datenverarbeitung das Verfahren vornehmlich abzielt (z.B. Messwerte), im Unterschied zu Sekundärdaten.

611 **Sekundärdaten**¹⁰

- 612 • Logging-Daten

613 **3.6 Ort, Art und Weise der Verarbeitung**

614 Die Messeinrichtung stellt die Messwerte zur Verfügung. Die Übertragung der Messwerte von der
615 Messeinrichtung an das SMGW erfolgt im LMN drahtgebunden oder drahtlos. Die Weiterverarbei-
616 tung im SMGW findet automatisch statt.

617 Die Art und Weise der Überwachung des Prozesses durch den SMGW-Admin liegt in dessen Er-
618 messen.¹¹

619 Die Protokollierung erfolgt in den Logs.

620 Speicher- und Löschfristen ergeben sich aus den datenschutzrechtlichen Vorgaben und vertragli-
621 chen Festlegungen. Die Messwerte werden solange aufbewahrt, bis das Ende des jeweiligen Ab-
622 rechnungszeitraums zuzüglich sechs Wochen überschritten ist (vgl. BSI TR-03109-1). Siehe zur
623 Löschung von Daten im SMGW auch BSI TR-03109-1. Vorgaben für die Speicherdauer der Daten
624 für die Anzeigeeinheit ergeben sich ebenfalls aus BSI TR-03109-1.

625 **3.7 Schnittstellen**

626 Im Prozess Messung finden nur die genannten Datenübertragungen zwischen Messeinrichtungen
627 und SMGW statt. Zwischen SMGW und SMGW-Admin erfolgt die Übertragung von Log-Dateien
628 zur Überwachung der Messung bzw. der SMGW-Admin hat durch den Einblick in das SystemLog
629 die Möglichkeit, die korrekte Datenübermittlung zwischen Messeinrichtung und SMGW zu über-
630 prüfen.

631 Schnittstelle zwischen Messeinrichtungen und SMGW: IF_GW_MTR (vgl. GW_PP Kap. 1.4.7)

632 Schnittstelle zwischen SMGW und SMGW-Admin: IF_GW_WAN (vgl. GW_PP Kap. 1.4.7)

633 **3.8 Besondere (Sicherheits-)Anforderungen**¹²

- 634 • Sichere Übertragung von Daten zwischen SMGW und SMGW-Admin (durch geeignete Si-
635 cherheitsmaßnahmen, z.B. Verschlüsselung nach Stand der Technik)

¹⁰ Sekundärdaten sind Daten, die aus unterschiedlichen Gründen zusätzlich bei der Datenverarbeitung anfallen, z.B. Protokolldaten, Authentifizierungsdaten.

¹¹ Der SMWG-Admin beachtet dabei die Gesetze, Verordnungen, TR und PP. Sein Konzept und seine Mittel der Überwachung sind angemessen und halten einer Überprüfung durch Dritte stand. Die konkrete Ausgestaltung seiner Überwachungstätigkeit (im Rahmen und nach den Vorgaben der anwendbaren Vorschriften) bleibt ihm selbst überlassen.

¹² Bezüglich der Sicherheitsanforderungen sind die Vorgaben der TR-03109 insgesamt zu beachten. Hier werden nur bestimmte Aspekte hervorgehoben oder ergänzt.

- 636 • Sichere Kommunikation des SMGW mit den Messeinrichtungen (vgl. die Vorgaben an die
- 637 Kommunikationsverbindungen und Protokolle in BSI TR-03109-1)
- 638 • Akzeptieren von Daten von Messeinrichtungen durch das SMGW nur dann, wenn es die
- 639 Messeinrichtungen in Form eines Zählerprofils kennt (vgl. BSI TR-03109-1)
- 640 • Unveränderlichkeit der Messwertlisten.

641 **3.9 Prozessschritte im Überblick**

Nr.	SMGW-Admin	SMGW	lokal angeschlossene Messeinrichtung	Bemerkung
1 Messung				
1.1			misst Parameter gemäß Vorgaben aus gesetzlichen und technischen Vorschriften sowie aus Verträgen zwischen Lieferanten, Letztverbraucher, Netzbetreiber, Messstellenbetreiber und anderen Dienstleistern	Messung wird hier nicht weiter beschrieben; es wird auf die einschlägigen rechtlichen und technischen Vorschriften verwiesen
1.2			verschlüsselt und/oder signiert die Inhaltsdaten	
2 Übertragung				
2.1		empfängt (PUSH-Betrieb) oder erfragt und empfängt (PULL-Betrieb) im LMN in regelmäßigen Zeitabständen die Messwerte der lokal angeschlossenen Messeinrichtungen	sendet (von selbst oder auf Anfrage des SMGW) im LMN in regelmäßigen Zeitabständen die Messwerte an das SMGW	entweder PUSH- oder PULL-Betrieb
2.2		akzeptiert nur Daten von Messeinrichtungen, die es in Form eines Zählerprofils kennt		
2.3		verifiziert den Datensatz; bei falschem Ergebnis verwirft das SMGW den Datensatz		
2.4		entschlüsselt den Datensatz (die Messwerte)		
3 Auswertung, Integritäts- und Gültigkeitsprüfung, Zeitstempelung				
3.1		wertet das jeweilige Fachprotokoll aus		
3.2		prüft die Integrität der Messwerte		
3.3		versieht die Messwerte mit Zeitstempel		
3.4		versieht jeden Messwert mit der Information, ob dieser gültig oder ungültig ist		
4 Speicherung				
4.1		speichert alle mit Zeitstempel versehenen Messwerte unveränderlich		
5 Nebenprozesse				
5.1	überwacht den gesamten Prozess kontinuierlich			Auch der Anschlussnutzer kann diesen Prozess insoweit überwachen, als er über die HAN-Schnittstelle die Messwerte auslesen kann
5.2		protokolliert während des gesamten Prozesses alle Aktionen des SMGW und des SMGW-Admins in den entsprechenden Logs		
5.3		löscht oder überschreibt die Mess-		

27 Betriebsprozesse

Nr.	SMGW-Admin	SMGW	lokal angeschlossene Messeinrichtung	Bemerkung
		werte nach frühestens 13 Monaten lückenlos beginnend mit dem jeweils ältesten Wert		

642 Tabelle 1: Prozessschritte Messung

643 4 Datenübertragung

644 4.1 Verortung im Gesamtkontext

645 Das Smart Meter Gateway (SMGW) sendet über das Weitverkehrsnetz Daten an Externe Marktteil-
646 nehmer und kann auch von diesen Daten empfangen. Der Prozess *Datenübertragung* befasst sich
647 nur mit der Übertragung zwischen SMGW und Externen Marktteilnehmern. Diese Marktteilnehmer
648 werden mittels Kommunikationsprofilen im SMGW verwaltet. Folgende Datenübertragungen wer-
649 den hier nicht beschrieben: Übertragung von Messdaten von den Sensoren an das SMGW, Übertra-
650 gung von Steuerdaten für die Steuerung von CLS, die Kommunikation des SMGW mit dem
651 SMGW-Admin, die Übertragung von Messdaten an die Anzeigeeinheit zwecks Visualisierung für
652 den Anschlussnutzer.

653 4.2 Beteiligte, Rollen und Funktionen

- 654 • Smart Meter Gateway-Administrator (SMGW-Admin)
- 655 • Externe Marktteilnehmer¹³

656 Die Externen Marktteilnehmer sind die Empfänger oder gegebenenfalls auch Sender von Daten-
657 übertragungen.

658 Der SMGW-Admin ermöglicht die erforderlichen Datenübertragungen¹⁴ durch entsprechende Kon-
659 figuration des SMGW. Ferner überwacht er die Datenübertragung.

660 4.3 Beschreibung und Zweck

661 Zum Zwecke der vertraglich vereinbarten oder gegebenenfalls technisch erforderlichen Datenüber-
662 tragungen von Mess- und Statuswerten (turnusmäßige Tarifdaten- und Netzzustandsdatenausliefe-
663 rung, spontane Messwertauslesung) aus dem SMGW an Externe Marktteilnehmer oder von Steuer-
664 befehlen der Externen Marktteilnehmer an das SMGW erfolgen die folgenden Schritte:

665 Voraussetzungen dafür, dass das SMGW Datenübertragungen an Externe Marktteilnehmer vorneh-
666 men kann, sind,

- 667 • dass der SMGW-Admin vorab im SMGW die als Empfänger von Datenübertragungen be-
668 rechtigten Externen Marktteilnehmer (Kommunikationsendpunkte) in Kommunikationspro-
669 filen konfiguriert,

¹³ Externe Marktteilnehmer können Energie-, Wasser-, Gasversorger, Netzbetreiber oder andere Versorger oder Dienstleister sein, die mit dem Letztverbraucher einen Vertrag über die Entnahme, Einspeisung, Steuerung oder andere Dienstleistungen haben, die eine Übertragung von Daten zwischen dem SMGW und externen Marktteilnehmern erforderlich machen.

¹⁴ Diese ergeben sich aus dem zwischen dem Letztverbraucher und externen Marktteilnehmern oder zwischen diesen geschlossenen Verträgen oder gesetzlichen Vorschriften (z.B. zur Erfüllung der Aufgaben der Aufsichtsbehörden wie BNetzA, PTB).

- 670 • dort das notwendige Schlüsselmaterial hinterlegt,
- 671 • die Tarifprofile ins SMGW einbringt, nach welchen die Übertragungen an die Externen
- 672 Marktteilnehmer inhaltlich und zeitlich gesteuert werden.
- 673 Die für die Konfiguration erforderlichen Informationen¹⁵ werden von den Vertragspartnern des An-
- 674 schlussnutzers dem SMGW-Admin zur Verfügung gestellt.
- 675 Bezüglich des Aufbaus und der Absicherung der Verbindung für die Übermittlung von Daten an
- 676 Externe Marktteilnehmer vgl. BSI TR-03109-1.
- 677 Der Externe Marktteilnehmer kann - sofern er dazu berechtigt ist - den Administrator beauftragen,¹⁶
- 678 das SMGW zum Aufbau einer Verbindung zu ihm zu veranlassen. Nach einem „Wake-Up“ durch
- 679 den SMGW-Admin stellt das SMGW eine Verbindung mit dem Administrator her, der dann das
- 680 SMGW veranlasst, eine Verbindung zum Externen Marktteilnehmer aufzubauen.
- 681 Ein Externer Marktteilnehmer kann Daten vom SMGW erhalten, die das SMGW an ihn adressiert
- 682 und für ihn verschlüsselt und signiert hat.
- 683 Das SMGW protokolliert alle Datenübertragungen in den entsprechenden Logs (siehe BSI TR-
- 684 03109-1).
- 685 Der SMGW-Admin stellt im Rahmen seiner Aufgaben durch geeignete Maßnahmen sicher, dass die
- 686 Datenübertragung ordnungsgemäß abläuft.¹⁷

687 **4.4 Zeitpunkt**

- 688 Datenübertragungen finden im laufenden Betrieb statt.
- 689 Das SMGW überträgt die Registerwerte (gemäß Tarifprofilen) der im Profil definierten Register bei
- 690 Eintreten eines bestimmten Auslösers (Trigger).¹⁸ Das SMGW wartet für den Versand von Regis-
- 691 terwerten auf den Aufbau der sicheren Verbindung zum Marktteilnehmer im WAN und versendet
- 692 dann die Registerwerte unmittelbar nach dem Verbindungsaufbau. Das SMGW bestimmt jeden wei-
- 693 teren Versandzeitpunkt aus dem ersten Abrechnungs- bzw. Auswertungszeitpunkt und dem Ab-
- 694 rechnungs- bzw. Auswertungsintervall.

695 **4.5 Verarbeitete Daten**

696 **Primärdaten**

¹⁵ Informationen gemäß den Marktprozessen.

¹⁶ Ausgestaltung dieses Auftrags gemäß Marktprozessen.

¹⁷ Eine weitere Kontrolle, insbesondere der Rechtmäßigkeit der Datenübertragung, besteht in der Möglichkeit des Anschlussnutzers, der mittels der Anzeigeeinheit über das Kunden-Log feststellen kann, welche externen Marktteilnehmer berechtigt sind, Daten übertragen zu bekommen oder zu übertragen, und welche Datenübertragungen stattgefunden haben.

¹⁸ Dabei kann es sich um den Moment des Ablaufs eines jeden Abrechnungszeitraums, den Abschluss der Auswertung aller Register in einem Abrechnungsintervall oder um einen anderen Trigger handeln.

697 Es kommen je nach Anwendungsfall und Vertragsgestaltung diverse Inhaltsdaten in Frage, die un-
698 terschiedlich klassifiziert werden können, z.B.

- 699 • Messdaten
- 700 • Netzzustandsdaten
- 701 • abrechnungsrelevante Daten (für verschiedene Zwecke der Abrechnung und damit ggf.
702 verschiedene Empfänger)
- 703 • nicht abrechnungsrelevante Daten
- 704 • Gateway-ID
- 705 • Zähler-ID (oder Pseudonym)
- 706 • Marktteilnehmer-ID/-Adressen
- 707 • kryptografische Schlüssel und Signaturdaten
- 708 • Zeitstempel, Gültigkeit, OBIS-Kennzahl des Messwertsatzes und andere Zusatz-
709 informationen

710 **Sekundärdaten**

711 Logeinträge im Kunden-Log über die Datenübertragungen an Externe Marktteilnehmer

712 **4.6 Ort, Art und Weise der Verarbeitung**

713 Die Übertragung erfolgt verschlüsselt über das WAN. Zu den Vorgaben zu den Kommunikations-
714 verbindungen und Kommunikationsprotokollen siehe BSI TR-03109-1.

715 Das SMGW speichert zu versendende Daten so lange, bis der Versand erfolgt ist und von der Ge-
716 genstelle quittiert wurde.

717 Die Protokolldaten über die Datenübertragung an Externe Marktteilnehmer werden im Kunden-Log
718 gespeichert, das durch den Anschlussnutzer einseh- und abrufbar ist. Der SMGW-Admin kann
719 durch Einblick in das SystemLog prüfen, ob die Datenübertragungen erfolgreich waren.

720 **4.7 Schnittstellen**

721 Die Verbindung zwischen SMGW und den Externen Marktteilnehmern erfolgt über eine WAN-
722 Verbindung: IF_GW_WAN (vgl. GW_PP Kap. 1.4.7).

723 Für die Übertragung von nicht abrechnungsrelevanten Daten kann der SMGW-Admin als Schnitt-
724 stelle zur Sicherstellung der Pseudonymisierung gemäß BSI TR-03109-1 fungieren.

725 4.8 Besondere (Sicherheits-)Anforderungen¹⁹

- 726 • Neben den sich aus der BSI TR-03109-1 ergebenden Anforderungen an die Kommunikati-
727 onsprotokolle, an die Inhaltsdatenverschlüsselung, Signierung, Absicherung der Kommuni-
728 kation und Authentifizierung sind die Anforderungen aus § 21e Abs. 3 EnWG zu beachten:
- 729 • Danach müssen die an der Datenübermittlung beteiligten Stellen dem jeweiligen Stand der
730 Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicher-
731 heit treffen, die insbesondere die Vertraulichkeit und Integrität der Daten sowie die Fest-
732 stellbarkeit der Identität der übermittelnden Stelle gewährleisten. Im Falle der Nutzung all-
733 gemein zugänglicher Kommunikationsnetze müssen Verschlüsselungsverfahren angewendet
734 werden, die dem jeweiligen Stand der Technik entsprechen.
- 735 • Die personenbezogenen bzw. personenbeziehbaren Daten sowie jegliche Zuordnungen von
736 diesen Daten zu bestimmten oder bestimmbar natürlichen Personen dürfen nicht an Unbe-
737 fugte gelangen.
- 738 • Im Falle der Durchleitung löscht der Weiterleitende die Daten nach erfolgreicher Übertra-
739 gung an den vorgesehenen Empfänger.
- 740 • Beim Versand von nicht abrechnungsrelevanten Daten²⁰ muss das Verfahren der Pseudony-
741 misierung gemäß BSI TR-03109-1 durchgeführt werden können.²¹
- 742 • Alle auf vertraglicher Grundlage und ebenso alle auf gesetzlicher Anordnung basierenden
743 Datenübertragungen müssen den in der BSI TR-03109-1 dargestellten Anforderungen an die
744 Kommunikationsverbindungen, Kommunikationsprofile und an die Datensicherheit entspre-
745 chen.

746 4.9 Prozessschritte im Überblick

Nr.	SMGW-Admin	SMGW	Externer Marktteilnehmer	Bemerkung
1 Vorbedingungen				
1.1	erhält von den Vertragspartnern des Anschlussnutzers die für 1.2 erforderlichen Informationen			siehe Marktprozesse
1.2	konfiguriert im SMGW die als Empfänger von Datenübertragungen berechtigten Externen Marktteilnehmer (Kommunikationsendpunkte) in Kommunikationsprofilen (dort hinterlegt er auch das notwendige Schlüsselmaterial)			

¹⁹ Bezüglich der Sicherheitsanforderungen sind die Vorgaben der TR-03109 insgesamt zu beachten. Hier werden nur bestimmte Aspekte hervorgehoben oder ergänzt.

²⁰ Nicht abrechnungsrelevante Daten sind insbesondere die Netzzustandsdaten und alle Daten, die nicht für die Abrechnung zwischen dem Lieferanten und dem Letztverbraucher gemäß dem vereinbarten Tarif erforderlich sind.

²¹ Für bestimmte Netzzustandswerte ist es indes natürlich erforderlich, dass sie bestimmten Netzanschlusspunkten zugeordnet sind. Hier ist die Netzanschlusspunkt-ID als Pseudonym zu behandeln, das von der Stelle, die die Statuswerte benötigt, keiner natürlichen Person zugeordnet wird.

32 Betriebsprozesse

Nr.	SMGW-Admin	SMGW	Externer Marktteilnehmer	Bemerkung
1.3	hinterlegt die Tarifprofile im SMGW, nach welchen die Externen Marktteilnehmer bestimmte Daten erhalten			
1.4		verarbeitet die zu übermittelnden Daten		
2 Übertragung an Externe Marktteilnehmer				
2.1 Verbindungsaufbau durch das SMGW				
		baut Verbindung zum Externen Marktteilnehmer auf		
2.2 Verbindungsaufbau durch den externen Marktteilnehmer				
2.2.1			beauftragt den SMGW-Admin, das SMGW zum Aufbau einer Verbindung zum externen Marktteilnehmer zu veranlassen (nicht der Regelfall)	gemäß Marktprozessen
2.2.2	stellt Zulässigkeit des Auftrags fest			
2.2.3	führt Wake-Up-Call durch			
2.2.4		stellt TLS-Verbindung mit SMGW-Admin her		
2.2.5	veranlasst das SMGW, Verbindung zum externen Marktteilnehmer herzustellen			
2.2.6		baut in der Rolle eines TLS-Clients einen beidseitig authentifizierten TLS-Kanal zum externen Marktteilnehmer auf		
2.3 Anforderung von Messwerten im Sinne einer Spontanauslesung				
2.3.1			beauftragt den SMGW-Admin, das SMGW zur Übersendung bestimmter Werte zu veranlassen	gemäß Marktprozessen
2.3.2	stellt Zulässigkeit des Auftrags fest			
2.3.3	führt Wake-Up-Call durch			
2.3.4		stellt TLS-Verbindung mit SMGW-Admin her		
2.3.5	veranlasst die Spontanauslesung am SMGW			
2.3.6		führt die erforderliche Datenverarbeitung durch und versendet die Daten		
2.4 Sicherung der Kommunikation				
		sichert die Inhaltsdaten und die Kommunikation mit dem externen Marktteilnehmer ab (TLS, Inhaltsdatenverschlüsselung und -signierung für die Übermittlung von Netzstatusdaten und abrechnungsrelevanten Daten)		
3 Versand von Messwerten				
3.1 Versand von Registerwerten				
3.1.1		versendet Registerwerte (gemäß Tarifprofilen) der im Profil definierten Register nach Ablauf eines jeden Abrechnungszeitraums		
3.1.2		versendet Statusdaten an externe Marktteilnehmer		
3.1.3		wartet für den Versand der Daten auf Aufbau der Verbindung zum Marktteilnehmer im WAN		
3.1.4		versendet die Daten bei beste-		

Nr.	SMGW-Admin	SMGW	Externer Marktteilnehmer	Bemerkung
		hender TLS-Verbindung sofort		
3.1.5		bewahrt bei Nichtbestehen des TLS- Kanals die Daten solange auf, bis der Kanal besteht, und versendet sie sodann		
3.2 Alternativen: pseudonymer/nicht pseudonymer Versand von Messwerten				
3.2.1		überträgt die Daten ohne Pseudonymisierung an externe Marktteilnehmer		nicht pseudonymer Versand von abrechnungsrelevanten Daten
3.2.2		führt Pseudonymisierung durch (entfernt die Zähler-ID und ersetzt diese durch ein im Auswertungsprofil hinterlegtes Pseudonym)		pseudonymer Versand von nicht abrechnungsrelevanten Daten
3.2.3		verschlüsselt diese Daten an den Empfänger und signiert sie		
3.2.4		überträgt diese Daten an den SMGW-Admin		
3.2.5	prüft die Signatur des SMGW und entfernt die Gateway-Signatur			
3.2.6	überträgt das Datenpaket an den vorgesehenen Empfänger			
3.2.7			entschlüsselt die Daten	
3.3 Datenübertragung per Durchleitung				
3.3.1		adressiert und verschlüsselt Daten an einen externen Marktteilnehmer (Endempfänger)		
3.3.2		übermittelt diese Daten an Betreiber eines TLS-Endpunktes (externer Marktteilnehmer, der nicht der Endempfänger ist)		
3.3.3			Betreiber des TLS-Endpunktes prüft die Signatur des SMGW und entfernt diese gegebenenfalls	Entfernung der Signatur dient zur Pseudonymisierung (z. B. von Netzstandsdaten)
3.3.4			leitet die an den Endempfänger verschlüsselten Daten an diesen weiter	Weiterleitung mittels geeignet gesicherter Marktprozesse
4 Nebenprozesse				
4.1		versendet selbsttätig bestimmte Meldungen (z. B. zu Störungen) an externe Marktteilnehmer		
4.2		protokolliert die Übermittlungen in den Logs		
4.3	stellt durch Überwachungsmaßnahmen sicher, dass die Datenübermittlung ordnungsgemäß funktioniert			
4.4	beachtet Aufbewahrungspflichten und Löschfristen	speichert bzw. löscht gemäß Vorgaben	beachtet Aufbewahrungspflichten und Löschfristen	

748 5 Administration

749 5.1 Verortung im Gesamtkontext

750 Im laufenden Betrieb können Administrationstätigkeiten erforderlich werden, die über diejenigen
751 Tätigkeiten des Smart Meter Gateway Administrators (SMGW-Admin) hinausgehen, die er im Zu-
752 sammenhang mit anderen Prozessen ausführt. Zu den Administrationstätigkeiten gehören insbeson-
753 dere (vgl. auch BSI TR-03109-1):

- 754 • Geräteverwaltung (Geräte, d.h. Zähler, CLS-Geräte, Anzeigeeinheiten im SMGW registrie-
755 ren und einem Letztverbraucher zuordnen und diese Zuordnung wieder aufheben und Geräte
756 löschen)
- 757 • Mandantenverwaltung (Letztverbraucher anlegen, bearbeiten, löschen und zugeordnete Zer-
758 tifikate einrichten oder löschen; Verwaltung Kennung/Passwort für Anzeigeeinheit)
- 759 • Profilverwaltung (Kommunikationsprofile und Regelwerke zur Tarifierung bzw. Netzzu-
760 standsmeldung einbringen, aktivieren und löschen)
- 761 • Schlüssel-/Zertifikatsmanagement (Schlüssel und Zertifikate für die Kommunikation mit
762 Zählern, CLS-Geräten, externen Marktteilnehmern einbringen, aktivieren, deaktivieren bzw.
763 löschen; Umschalten auf anderen Kryptoalgorithmus im Sicherheits-Modul)
- 764 • Firmware-Update (neue Firmware aufspielen, verifizieren und aktivieren)
- 765 • Wake-Up-Konfiguration (Adresse des Wake-Up-Services konfigurieren)
- 766 • Monitoring des SMGW (Zustand des SMGW abfragen, Logeinträge aus dem System- und
767 eichtechnischen Log auslesen und auswerten, Reaktion auf Alarmmeldungen)
- 768 • Einspielen von Sicherheits-Updates
- 769 • Einspielen von Anwendungs-Software

770 Der SMGW-Admin stellt dem SMGW zudem Dienste zur Verfügung, auf die das SMGW im Be-
771 trieb angewiesen ist, z.B. den Zeitservice (siehe BSI TR-03109-1).

772 5.2 Beteiligte, Rollen und Funktionen

- 773 • SMGW-Admin
- 774 • Autorisierte Service-Techniker
- 775 • Prüfstellen, Eichbehörde
- 776 • Anschlussnutzer

777 Die ausführende Rolle hat der SMGW-Admin inne. In Ausnahmefällen können die Aufgaben des
778 SMGW-Admins bezüglich Störungserkennung und Diagnose von einem Service-Techniker im Auf-
779 trag des SMGW-Admins vor Ort am SMGW ausgeführt werden.

780 Anerkannte Prüfstellen überprüfen die Tätigkeiten des SMGW-Admins (insbesondere ISO-
781 Zertifizierung). Eine Überwachung durch die Eichbehörde ist möglich.

782 Der Anschlussnutzer erhält über die Anzeigeeinheit Informationen über die Aktivitäten des
783 SMGW-Admins und hat damit auch eine Möglichkeit, dessen Tätigkeit zu überprüfen.

784 **5.3 Beschreibung und Zweck**

785 Der Zweck einer Administrationstätigkeit ist grundsätzlich das Planen, Installieren, Konfigurieren
786 und die Pflege einer IT-technischen Infrastruktur. Im Hinblick auf das SMGW schließt das insbe-
787 sondere die Erhaltung der Funktionsfähigkeit und Sicherheit des SMGW, seiner Komponenten und
788 Schnittstellen und die Anpassung des SMGW an technische Neuerungen ein.

789 Sowohl zum Senden von Administrationskommandos als auch zum Aufspielen von Updates fordert
790 der SMGW-Admin mittels eines Wake-Up-Calls das SMGW dazu auf, eine gesicherte TLS-
791 Verbindung zwischen SMGW-Admin und SMGW aufzubauen, sofern nicht ein bereits zwischen
792 ihnen bestehender Kanal genutzt werden kann.

793 Sobald der TLS-Kanal offen ist, sendet der SMGW-Admin z.B. einen Befehl zum Update an das
794 SMGW, das die Signatur des Update-Befehls verifiziert und dann die neue Software über eine ver-
795 schlüsselte und authentifizierte Verbindung von einem Update-Server herunterlädt, die TLS-
796 Verbindung daraufhin schließt und die neue Software aktiviert.

797 Im Anschluss an ein Update und nach Umsetzung von anderen Administrationskommandos führt
798 das SMGW Selbsttests durch. Der SMGW-Admin überwacht die Selbsttests durch geeignetes Mo-
799 nitoring und stichprobenartige Überprüfungen. Bei Fehlfunktionen ergreift er die erforderlichen
800 Maßnahmen.

801 Firmware-Updates werden grundsätzlich vor ihrem Einspielen auf das SMGW durch eine anerkannte
802 Prüfstelle gemäß der Technischen Richtlinie und den Schutzprofilen zertifiziert. Im Ausnahme-
803 fall besteht die Möglichkeit, notwendige Patches sofort einzuspielen, die im Nachgang zertifiziert
804 werden.

805 Das SMGW protokolliert alle Aktivitäten des SMGW-Admins in den Logs (vgl. BSI TR-03109-1).

806 Der SMGW-Admin stellt durch von ihm zu treffende geeignete Maßnahmen sicher, dass seine Tä-
807 tigkeiten nicht zu fehlerhaften Funktionen des SMGW führen. Bei Fehlfunktionen ergreift er die
808 erforderlichen Korrekturmaßnahmen. Das Konzept und die Mittel des SMGW-Admins für Monito-
809 ring, Überprüfungen und Korrekturmaßnahmen unterliegen einer regelmäßigen Kontrolle und Zerti-
810 fizierung durch vom BSI anerkannte Prüfstellen. Diese überprüfen zudem die korrekte Durchfüh-
811 rung der Maßnahmen des Sicherheitskonzepts des SMGW-Admins (siehe Anlage V - Anforderun-
812 gen zum Betrieb beim Administrator).

813 Ist das SMGW über die WAN-Verbindung vom SMGW-Admin nicht zu erreichen, so kann dieser
814 den Service-Techniker beauftragen, vor Ort am SMGW die Störung zu ermitteln und Diagnostik-
815 tätigkeiten durchzuführen (siehe Prozess *Störungserkennung/Diagnose*).

816 **5.4 Zeitpunkt**

817 Die Administrationstätigkeiten erfolgen jederzeit im laufenden Betrieb.

818 **5.5 Verarbeitete Daten**

819 **Primärdaten**

820 Zur Dokumentation der Tätigkeiten des SMGW-Admins (bei ihm selbst bzw. in den Logs des
821 SMGW oder gegenüber den Aufsichtsbehörden) werden verwendet:

- 822 • eindeutige Bezeichner der betroffenen SMGW (Gateway-ID)
- 823 • eindeutige Bezeichner der Messeinrichtungen (Zähler-ID)
- 824 • ggf. eindeutige Bezeichner der Komponenten im SMGW (Komponenten-ID)
- 825 • Administrationsdaten (z.B. die einzuspielende Software, Profile, Schlüssel, Zertifikate)

826 Bei etwaigen Tätigkeiten an einem SMGW vor Ort (z.B. Kontrolle, Austausch) geht der SMGW-
827 Admin oder eine Person oder Stelle in seinem Auftrag (Service-Techniker) mit den folgenden Da-
828 ten um:

- 829 • Personennamen
- 830 • Adressdaten
- 831 • Kommunikationsdaten
- 832 • Gateway-ID, Zähler-ID, Komponenten-ID

833 **Sekundärdaten**

- 834 • Protokolldaten über alle Maßnahmen des SMGW-Admins (Protokollierung in den)

835 **5.6 Ort, Art und Weise der Verarbeitung**

836 Updates und Administrationen sowie die Überprüfung der Ordnungsmäßigkeit werden durch den
837 SMGW-Admin im Fernzugriff über die WAN-Schnittstelle durchgeführt. Die Implementierung der
838 Updates und die Umsetzung der Administrationsbefehle erfolgen im SMGW und gegebenenfalls im
839 Sicherheitsmodul. Selbsttests finden im SMGW automatisch statt.

840 Überprüfungen durch anerkannte Prüfstellen und gegebenenfalls durch die Eichbehörde erfolgen
841 beim SMGW-Admin und auf der Grundlage der von diesem auf Anforderung zur Verfügung ge-
842 stellten Daten.

843 Die für den Anschlussnutzer vorgesehenen Informationen werden im Kundenlog gespeichert. Die-
844 ses wird ihm über die Anzeigeeinheit verfügbar gemacht.

845 Sofern zu Prüf- und Dokumentationszwecken eindeutige Bezeichner von SMGW, einzelnen Kom-
846 ponenten oder Messeinrichtungen bestimmten natürlichen Personen zugeordnet worden sind, sind

847 für diese Datenkombinationen die datenschutzrechtlichen Vorgaben an die Löschung, Sperrung
848 oder Pseudonymisierung zu beachten.

849 Es erfolgen Verarbeitungen und Speicherungen von Daten auch beim SMGW-Admin bzw. auf des-
850 sen Systemen und gegebenenfalls auf den vom Service-Techniker für den Einsatz am SMGW mit-
851 geführten mobilen Verarbeitungs- und Speichermedien.

852 Die Protokollierungsdaten werden in den Logs des SMGW gespeichert.

853 **5.7 Schnittstellen**

854 Administrationsbefehle werden nur vom SMGW-Admin an das SMGW gesendet. Updates werden
855 vom SMGW-Admin auf das SMGW eingespielt. Alternativ nutzt das SMGW einen Dienst beim
856 SMGW-Admin, um neue Firmware herunterzuladen.

857 Es kann vorgesehen werden, dass das SMGW nach Implementierung von Updates oder Umsetzung
858 von bestimmten Administrationskommandos eine Nachricht an externe Marktteilnehmer sendet.

859 Der SMGW-Admin führt die Administrationstätigkeiten über die WAN-Schnittstelle
860 IF_GW_WAN (vgl. GW_PP Kap. 1.4.7) aus. Zu den Vorgaben an die Kommunikationsverbindun-
861 gen und -protokolle für die Administration über das WAN wird auf BSI TR-03109-1 verwiesen.

862 Wird der Service-Techniker vor Ort am SMGW im Auftrag des SMGW-Admins tätig, erfolgen die
863 ihm aufgetragenen Tätigkeiten über die HAN-Schnittstelle am SMGW.

864 **5.8 Besondere (Sicherheits-)Anforderungen²²**

- 865 • Inhaltsdatenverschlüsselung und -signierung der Administrationskommandos und von deren
866 Parametern
- 867 • Implementierung des Updateprozesses „fail safe“, sodass Prozessfehler nicht zum Ausfall
868 des SMGW führen
- 869 • Gewährleistung, dass der Updateprozess keinen Einfluss auf die im SMGW gespeicherten
870 Daten oder Profile hat

871

872

873

²² Bezüglich der Sicherheitsanforderungen sind die Vorgaben der TR-03109 insgesamt zu beachten. Hier werden nur bestimmte Aspekte hervorgehoben oder ergänzt.

5.9 Prozessschritte im Überblick

Nr.	SMGW	SMGW-Admin	Bemerkung
1 Vorbedingungen			
1.1		die zur Administration benötigten Daten/Informationen liegen dem SMGW-Admin vor	wird in den Marktprozessen geregelt
2 Administration (allgemein)			
2.1		sendet Administrationskommandos und Administrationsdaten an das SMGW	
2.2	setzt die Administrationskommandos nach Prüfung der beigefügten Signatur um		
2.3	führt Selbsttest(s) aus (siehe unten 5.2)		mindestens bei eichrechtlich relevanten Updates erfolgt ein Selbsttest
3 Updates (Beispiel für bestimmtes Admin-Kommando)			
3.1		führt Wake-Up-Call durch (vgl. Kap. 3.2.5)	
3.2	baut TLS-Verbindung zum SMGW-Admin auf		
3.3		sendet Befehl zum Update an das SMGW	
3.4	verifiziert die Signatur des Update-Befehls		
3.5	lädt die neue Software über verschlüsselte und authentifizierte Verbindung von einem Update Server herunter		alternativ Nutzung eines bestehenden TLS-Kanals alternativ bringt der SMGW-Admin das Update ein
3.6	schließt den TLS-Kanal		
3.7	aktiviert die neue Software		
3.8	führt Selbsttest(s) aus (siehe unten 5.2)		mindestens bei eichrechtlich relevanten Updates erfolgt ein Selbsttest
4 Sicherheitskritische Updates			
4.1		spielt bei Bedarf noch nicht zertifizierte Software für ein Software-Update ein	nur in Fällen eines erhöhten Sicherheitsrisikos können erforderliche Updates vor der Zertifizierung aufgespielt werden. (Es wird noch definiert, in welchen Fällen und unter welchen Voraussetzungen noch nicht zertifizierte Software eingespielt werden darf.)
4.2		sorgt nach dem Update für unverzügliche Nachholung der Zertifizierung	unverzüglich bedeutet, dass der Hersteller der jeweiligen SW die Zertifizierung sofort anstoßen muss (sofortige Information des BSI –ggf. durch SMGW-Admin –, und dann Zertifizierung gemäß Absprache mit dem BSI)
5 Nebenprozesse			
5.1	stößt gegebenenfalls erforderliche Nacheichung an		siehe Prozess <i>Nacheichung im laufenden Betrieb</i>
5.2	führt ggf. nach der Umsetzung von Administrationsbefehlen Selbsttest(s) aus		
5.3	protokolliert im eichtechnischen Log den Selbsttest und das Ergebnis		
5.4		überwacht die Selbsttests durch geeignetes Monitoring und stichprobenartige Überprüfungen	
5.5		ergreift bei Fehlfunktionen unverzüglich die erforderlichen Maßnahmen	
5.6	protokolliert alle Aktivitäten des SMGW-Admins in den Logs		
5.7	stellt dem Anschlussnutzer im Kunden-Log Informationen über Updates, Wartung und ggf. Administrationsaktivitäten zur Verfügung		
5.8	informiert den Anschlussnutzer ggf. über besondere Vorfälle über die Anzeigeeinheit		

39 Betriebsprozesse

Nr.	SMGW	SMGW-Admin	Bemerkung
5.9		beachtet Aufbewahrungspflichten und Löschfristen	

875 Tabelle 3: Prozessschritte Administration

876 **6 Störungserkennung/Diagnose**

877 **6.1 Verortung im Gesamtkontext**

878 Während des Wirkbetriebes des Smart Meter Gateways (SMGW) können Störungen auftreten.
879 Grundsätzlich erfolgt die Störungserkennung durch den Smart Meter Gateway Administrator
880 (SMGW-Admin) über das WAN (die hier nicht beschreiben wird). Ist die Störungsermittlung durch
881 den SMGW-Admin über das WAN nicht möglich, erfolgt die in diesem Prozess beschriebene Stö-
882 rungserkennung/Diagnose im Rahmen einer Vor-Ort-Überprüfung durch den autorisierten Service-
883 Techniker. An die Störungserkennung/Diagnose schließt sich die Störungsbehebung an, die, wie
884 auch eine spätere mögliche Plausibilisierung oder Ersatzwertbildung nicht Bestandteil dieses Pro-
885 zesses ist.

886 **6.2 Beteiligte, Rollen und Funktionen**

- 887 • Smart Meter Gateway Administrator
- 888 • Autorisierter Service-Techniker

889 **6.3 Beschreibung und Zweck**

890 Tritt im laufenden Betrieb eine Störung ein, die die normalen Prozesse beeinträchtigt oder verhin-
891 dert und die der SMGW-Admin nicht über das WAN ermitteln kann, wird die Störungsermittlung
892 vor Ort am SMGW erforderlich, die der autorisierte Service-Techniker ausführt.

893 Ziel des Einsatzes des autorisierten Service-Technikers ist, die für die Ermittlung und Behebung
894 einer Störung notwendigen Daten und Informationen zu erheben, damit entweder durch Eingreifen
895 vor Ort durch den autorisierten Service-Techniker oder durch darüberhinausgehende Maßnahmen
896 (ggf. des SMGW-Admins oder Dritter) das SMGW wieder in den normalen Betriebsmodus versetzt
897 werden kann. Dafür sind zunächst das Erkennen der Störung und dann die Diagnose erforderlich,
898 um die Ursache der Störung zu ermitteln.

899 Der Einsatz des autorisierten Service-Technikers vor Ort am SMGW kann beispielsweise bei fol-
900 genden Störungen erforderlich werden:

- 901 • die Kommunikation zwischen SMGW-Admin und dem SMGW kommt nicht oder nicht feh-
902 llerfrei zustande
- 903 • es ist mehrfach keine störungsfreie Kommunikation zustande gekommen
- 904 • der SMGW-Admin hat mehrfach vergeblich versucht, über den Wake-up-Call das SMGW
905 zu erreichen
- 906 • das SMGW hat sich zu den vorkonfigurierten Sendeintervallen nicht gemeldet
- 907 • das SMGW führt die vorgesehenen Prozesse nicht, nicht vollständig oder nicht fehlerfrei aus

- 908 • das SMGW hat in seinen Logs häufige Fehler eines oder mehrerer Zähler vermerkt
 - 909 • das SMGW meldet Gehäusebruch an den SMGW-Admin
 - 910 • oder es liegen ähnliche Konstellationen oder andere unklare Probleme vor, die ein Eingrei-
911 fen des SMGW-Admins bzw. des autorisierten Service Technikers erforderlich machen.
- 912 Der autorisierte Service-Techniker authentisiert sich am SMGW mit seinem Zertifikat aus der SM-
913 PKI.
- 914 Der autorisierte Service-Techniker wird auf Anweisung des SMGW-Admins tätig. Über die HAN-
915 Schnittstelle verbindet er sein mobiles Gerät (z.B. Laptop) am SMGW, das einen TLS-Kanal etab-
916 liert. Sodann ruft der Service-Techniker, sofern möglich, Diagnosedaten ab.²³ Dafür steht ihm aus-
917 schließlich ein lesender Zugriff (read-only) zur Verfügung. Danach meldet sich der Service-
918 Techniker am SMGW ab, das die lokale Verbindung zum Gerät des Service-Technikers terminiert.
- 919 Der autorisierte Service-Techniker kann auf Anweisung des SMGW-Admins die vor Ort erhobenen
920 Diagnosedaten an den SMGW-Admin übertragen (z.B. über eine gesicherte Funkverbindung).²⁴
- 921 Der autorisierte Service-Techniker übermittelt seinen Diagnosebericht (mitsamt optisch wahrge-
922 nommenen Feststellungen, z.B. Siegel- oder Gehäusebruch, ggf. auch seinen Bericht über die durch
923 ihn vor Ort durchgeführte Fehlerbehebung) an den SMGW-Admin. Danach archiviert der SMGW-
924 Admin die erforderlichen und löscht die nicht erforderlichen Daten. Der Service-Techniker löscht
925 nach erfolgreicher Übertragung von Daten aus dem SMGW an den SMGW-Admin selbige auf sei-
926 nen Geräten.
- 927 Das SMGW protokolliert während des gesamten Prozesses alle Aktionen des SMGW, des SMGW-
928 Admins und des autorisierten Service-Technikers in den entsprechenden Logs.
- 929 Die sich an die Ermittlung der Daten anschließende Fehlerdiagnose und daraufhin die Fehlerbehe-
930 bung werden je nach Problemfall und Vertragskonstrukt hinsichtlich der Zusammenarbeit zwischen
931 SMGW-Admin und autorisiertem Service-Techniker durch einen von beiden oder durch beide ar-
932 beitsteilig durchgeführt.

933 **6.4 Zeitpunkt**

934 Der Prozess ist grundsätzlich jederzeit im laufenden Betrieb möglich.

935 **6.5 Verarbeitete Daten**

936 **Primärdaten**

²³ Diagnosedaten können vom SMGW gelieferte strukturierte, logfile-ähnliche Daten mit aktuellem Zustand des SMGW, der Zählernetzwerke (z.B. angeschlossene/sichtbare Zähler, aktuelle Adressierung der Zähler, Vorhandensein von Zertifikaten und deren Gültigkeit, Bestehen einer TLS-Verbindung, Bestehen einer Applikationsdaten-Verbindung) sein.

²⁴ Für die Gewährleistung der sicheren Übertragung per Telekommunikationsverbindung oder des sicheren Transports von Daten im Speichermedium des Service-Technikers ist der SMGW-Admin verantwortlich.

- 937 • Gateway-ID
- 938 • Zähler-ID
- 939 • Zuordnung der IDs zu den konkreten Letztverbrauchern (Personennamen, Adressen, Kom-
- 940 munikationsdaten)
- 941 • Log-Einträge
- 942 • Diagnosedaten
- 943 • Inhalte des Diagnose- und ggf. des Störungsbehebungsberichts des Service-Technikers

944 **Sekundärdaten**

- 945 • während des Prozesses durch das SMGW in den Logs aufgezeichnete Daten

946 **6.6 Ort, Art und Weise der Verarbeitung**

947 Die Erhebung, Verarbeitung bzw. Nutzung der Daten findet im SMGW, gegebenenfalls auf mobi-
948 len Diagnosegeräten des autorisierten Service-Technikers, auf mobilen Speicher- oder Sendemedien
949 des autorisierten Service-Technikers und beim SMGW-Admin statt. Die Datenübertragung erfolgt
950 über die unten angegebenen Schnittstellen.

951 Die Protokollierungsdaten werden in den Logs des SMGW gespeichert.

952 **6.7 Schnittstellen**

953 Zum Zwecke der Durchführung des Prozesses finden Datenübertragungen zwischen dem SMGW
954 und dem autorisierten Service-Techniker und zwischen diesem und dem SMGW-Admin statt.

- 955 • Schnittstelle zwischen SMGW-Admin und SMGW: IF_GW_WAN
- 956 • Schnittstelle zwischen autorisiertem Service Techniker und SMGW: IF_GW_HAN

957 **6.8 Besondere (Sicherheits-)Anforderungen²⁵**

- 958 • Für die Sicherheit der vom autorisierten Service-Techniker erhobenen Daten während der
959 Erhebung, während ihrer Speicherung bzw. Verarbeitung auf den Geräten des Service-
960 Technikers und während ihrer Übertragung an den SMGW-Admin sind dem Schutzbedarf
961 angemessene technische und organisatorische Maßnahmen zu ergreifen (Gewährleistung ei-
962 ner durchgehend hohen Sicherheit gemäß den Anforderungen der BSI TR-03109-1 zu den
963 Kommunikationsverbindungen).
- 964 • Hinsichtlich der personenbezogenen Daten, insbesondere der aus dem SMGW ausgelesenen
965 Log-Einträge, sind die datenschutzrechtlichen Regelungen zu beachten.

²⁵ Bezüglich der Sicherheitsanforderungen sind die Vorgaben der TR-03109 insgesamt zu beachten. Hier werden nur bestimmte Aspekte hervorgehoben oder ergänzt.

- 966 • Liegen tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme eines Messsys-
 967 tems vor, sind hinsichtlich des Umgangs mit den Daten zum Aufklären oder Unterbinden
 968 von Leistungerschleichungen die Vorgaben des § 21g Abs. 1 Nr. 8 in Verbindung mit Abs.
 969 3 EnWG zu beachten.

970 6.9 Prozessschritte im Überblick

Nr.	SMGW-Admin	SMGW	Autorisierter Service-Techniker	Bemerkung
1 Vorbedingungen				
1.1		Problemfall tritt auf		siehe Beispiele oben in Kap. 7.3
1.2	kann über die WAN-Verbindung Fehlerdiagnose nicht durchführen			
1.3			verfügt über ein gültiges Zertifikat zur Anmeldung am SMGW	Zertifikat ist aus der SM-PKI
2 Kernprozess				
2.1	weist den autorisierten Service Techniker an, am SMGW Diagnosedaten zu erheben			
2.2			verbindet sich am SMGW	mittels HAN-Schnittstelle
2.3		etabliert TLS-Kanal		
2.4			authentisiert sich gegenüber dem SMGW mittels Zertifikat	
2.5		prüft das Zertifikat des autorisierten Service Technikers		
2.6			ruft, sofern möglich, Diagnosedaten ab	es ist ausschließlich ein lesender Zugriff (read-only) erlaubt; ggf. können vom SMGW separierte Kommunikationsmodule konfiguriert werden
2.7			meldet sich am SMGW ab	
3 Nachbedingungen				
3.1	lokalisiert anhand der Diagnose-Daten den Fehler		lokalisiert anhand der Diagnose-Daten den Fehler	je nach Fall und Vertragskonstrukt durch den SMGW-Admin oder den Service-Techniker oder durch beide gemeinsam
3.2	nimmt die Fehlerbehebung vor oder initiiert sie		nimmt die Fehlerbehebung vor oder initiiert sie	
4 Nebenprozesse				
4.1			übermittelt vor Ort erhobene Diagnosedaten gesichert an den SMGW-Admin	übermittelt an den SMGW-Admin ggf. auch Diagnosebericht und Bericht über die durchgeführte Fehlerbehebung
4.2	archiviert die erforderlichen und löscht die nicht erforderlichen Daten			
4.3			löscht nach erfolgreicher Übermittlung der Daten aus dem SMGW an den SMGW-Admin selbige auf seinen Geräten	
4.4		protokolliert während des gesamten Prozesses alle Aktionen des SMGW, des SMGW-Admins und des autorisierten Service-Technikers in den entsprechenden Logs		

971 Tabelle 4: Prozessschritte Störungserkennung/Diagnose

972 **7 Wechsel des Smart Meter Gateway Administra-** 973 **tors**

974 **7.1 Verortung im Gesamtkontext**

975 Während des Betriebs des Smart Meter Gateways (SMGW) kann es grundsätzlich jederzeit zu ei-
976 nem Wechsel des Smart Meter Gateway Administrators (SMGW-Admin) kommen. Dabei wird
977 darauf abgezielt, dass es zu keiner Unterbrechung der Versorgung oder zu Lücken in der Erhebung
978 und Auswertung von Messwerten kommt.

979 Vor Beginn des hier beschriebenen technischen Wechsel-Prozesses sind ggf. im Rahmen der
980 Marktkommunikation zwischen den bei einem SMGW-Admin-Wechsel beteiligten Externen
981 Marktteilnehmern weitere, hier nicht genannte Informationen auszutauschen.

982 Der hier beschriebene Prozess geht davon aus, dass bei dem Wechsel des SMGW-Admins das
983 SMGW nicht gewechselt wird. Die eventuell im Rahmen einer Übergabe von beteiligten SMGW-
984 Admins vereinbarte visuelle Abnahme des SMGW durch einen autorisierten Service-Techniker
985 wird ebenfalls nicht betrachtet.

986 Grundsätzlicher Hinweis:

987 Ein Wechsel des SMGW-Admin stellt ein umfangreiches Projekt dar, in den alle vertraglich ver-
988 bundenen Partner involviert werden müssen. Alle Beteiligten sollten sich im Voraus auf einen Pro-
989 jektablauf einigen und klare Verantwortlichkeiten festlegen. Besonderes Augenmerk ist dabei auf
990 die verlustfreie Übergabe der Daten, die Aufrechterhaltung des Betriebes und die lückenlose Mess-
991 werterfassung bzw. Tarifierung zu richten.

992 **7.2 Beteiligte, Rollen und Funktionen**

- 993 • Smart Meter SMGW-Admin Alt (SMGW-Admin-A)
- 994 • Smart Meter SMGW-Admin Neu (SMGW-Admin-N)
- 995 • weitere beteiligte Externe Marktteilnehmer (im Rahmen der Marktkommunikation)

996 **7.3 Beschreibung und Zweck**

997 Zweck dieses Prozesses ist der Übergang des Betriebs eines SMGW von dem SMGW-Admin-A
998 zum SMGW-Admin-N.

999 Vorbedingungen für die Durchführung des Administratorwechsels sind:

- 1000 • die notwendigen Informationen zwischen allen beteiligten Externen Marktteilnehmern sind
1001 gemäß den Marktprozessen ausgetauscht worden;

- 1002 • der SMGW-Admin-N ist berechtigt, die Rolle des SMGW-Admins wahrzunehmen; insbe-
1003 sondere muss er hierfür sicherheitszertifiziert sein (siehe TR-03109-1, Anlage V: Anforde-
1004 rungen zum Betrieb beim Administrator);
- 1005 • das SMGW befindet sich im normalen Betriebsmodus, d.h. insbesondere, dass die WAN-
1006 Kommunikation funktioniert; andernfalls ist eine Störungsermittlung (siehe Prozess *Stö-*
1007 *rungserkennung/Diagnose*) und Störungsbehebung erforderlich;
- 1008 • der SMGW-Admin-A verfügt über Zugriffsrechte auf das SMGW, das auf den SMGW-
1009 Admin-A konfiguriert ist;
- 1010 • SMGW-Admin-A und SMGW-Admin-N haben die notwendigen Informationen ausge-
1011 tauscht (im Rahmen der Marktkommunikation);
- 1012 • der SMGW-Admin-N besitzt sein SMGW-Admin-Zertifikat aus der SM-PKI, das er ande-
1013 renfalls bei der SM-PKI beantragt.

1014 Bei Vorliegen der vorgenannten Voraussetzungen meldet der SMGW-Admin-N den Wechsel beim
1015 SMGW-Admin-A an.

1016 Der SMGW-Admin-A sendet dem SMGW-Admin-N die Informationen zur bestehenden Mess-
1017 Infrastruktur des SMGW. Hierzu zählen insbesondere Informationen zu den angeschlossenen Zäh-
1018 lern. Nicht zur Verfügung gestellt werden müssen hingegen z.B. Informationen zu bestehenden Ta-
1019 rifprofilen oder Kommunikationsprofilen.

1020 Der SMGW-Admin-N sendet seine Zertifikate und Verbindungsdaten an den SMGW-Admin-A, der
1021 eine Gültigkeitsprüfung des SMGW-Admin-N-Zertifikats durchführt.

1022 Je nach eventuell bestehenden vertraglichen Vereinbarungen zwischen dem Letztverbraucher, Ex-
1023 ternen Marktteilnehmern und dem SMGW-Admin-A sichert der SMGW-Admin-A die Daten vom
1024 SMGW oder löscht alle nicht mehr benötigten Daten auf dem SMGW. Für eine Sicherung der Da-
1025 ten kommen grundsätzlich alle Daten infrage, insbesondere aber die abrechnungsrelevanten Mess-
1026 werte.

1027 Zu löschen sind grundsätzlich, soweit keine anderen vertraglichen oder gesetzlichen Aufbewah-
1028 rungspflichten entgegenstehen, insbesondere die Tarifprofile und Kommunikationsprofile (die der
1029 SMGW-Admin-N nicht sehen soll).

1030 Nicht gelöscht werden dürfen die von den Zählern gelieferten Messwerte und die Logs.

1031 Zudem löscht der SMGW-Admin-A Daten auf dem SMGW oder in seinen eigenen Systemen, die
1032 der SMGW-Admin-N benötigt oder die für die Abrechnung relevant sind, erst dann, wenn der
1033 SMWG-Admin-N den Erhalt der entsprechenden Daten gegenüber dem SMGW-Admin-A quittiert
1034 hat. Abrechnungsrelevante Daten bewahrt der SMGW-Admin-A zumindest bis zur nächsten Ab-
1035 rechnungsperiode auf. Näheres zu Aufbewahrung und Löschung ergibt sich aus der Rechtsverord-
1036 nung und aus den Festlegungen zu den Marktprozessen.

- 1037 Der SMGW-Admin-A überträgt die Verbindungs-Daten für den SMGW-Admin-N auf das SMGW.
1038 Diese Konfiguration enthält u.a. Kommunikationsparameter für das WAN (z.B. GSM-Parameter),
1039 Verbindungsadresse zum SMGW-Admin-N (evtl. temporäre Adresse), Zertifikate des SMGW-
1040 Admin-N und die Zertifikatskette zur Prüfung der Konfigurations-Signatur.
- 1041 Das SMGW prüft die Signatur der vorstehenden Konfiguration anhand des Zertifikats des SMGW-
1042 Admin-A und prüft die Signatur des Zertifikats des SMGW-Admin-N gegen das Root-Zertifikat.
1043 Danach baut das SMGW eine Verbindung zum SMGW-Admin-N auf.
- 1044 Hinweis: Evtl. ist die Übergabe der Kommunikationstechnik zu regeln. Ggf. muss die Kommunika-
1045 tionstechnik beim Letztverbraucher vorher getauscht werden.
- 1046 Im Fehlerfall, wenn z.B. die Kommunikation nicht zustande kommt, nimmt das SMGW einen ent-
1047 sprechenden Eintrag im System-Log vor und meldet den Fehler an den SMGW-Admin-A. Nach
1048 Fehlerermittlung und -behebung durch den SMGW-Admin-A (ggf. unter Hinzuziehung des autori-
1049 sierten Service-Technikers gemäß dem Prozess *Störungserkennung/Diagnose*) sendet der SMWG-
1050 Admin-A erneut die Verbindungsdaten für SMGW-Admin-N an das SMGW. Ggf. ist auch erforder-
1051 lich, dass der SMGW-Admin-A erneut vom SMWG-Admin-N Zertifikate und Verbindungsdaten
1052 anfordert.
- 1053 Ist die Verbindung zwischen SMGW und SMGW-Admin-N zustande gekommen, liest der SMGW-
1054 Admin-N die Konfiguration aus dem SMGW aus und prüft diese. Die Prüfung durch den SMGW-
1055 Admin-N erfolgt anhand der zu Beginn des Wechselprozesses vom SMGW-Admin-A zur Verfü-
1056 gung gestellten Informationen und ggf. weiterer Informationen vom SMGW-Admin-A oder Exter-
1057 nen Marktteilnehmern gemäß den Marktprozessen.
- 1058 Das Ergebnis der vorgenannten Prüfung trägt der SMGW-Admin-N in das System-Log ein. Ist das
1059 Ergebnis negativ, dann prüft der SMGW-Admin-N den Sachverhalt. Bei negativem Ergebnis kann
1060 der Wechselprozess zunächst nicht zu Ende geführt werden.
- 1061 Der SMGW-Admin-A wird darüber informiert, dass der Prozess gestoppt worden ist. Damit bleibt
1062 der SMGW-Admin-A als verantwortlicher SMGW-Admin konfiguriert. Der SMGW-Admin-A
1063 löscht auf dem SMGW die zu Beginn des gestoppten Prozesses eingebrachten Verbindungsdaten
1064 für den SMGW-Admin-N.
- 1065 Das zugrundeliegende Problem und die Lösung werden dann vom SMGW-Admin-N ggf. mit dem
1066 SMGW-Admin-A und den beteiligten externen Marktteilnehmern geklärt. Nach Lösung des Prob-
1067 lems setzt der Wechselprozess erneut damit ein, dass der SMWG-Admin-A die Verbindungsdaten
1068 für den SMGW-Admin-N an das SMGW sendet. Ggf. ist auch erforderlich, dass der SMGW-
1069 Admin-A erneut vom SMWG-Admin-N Zertifikate und Verbindungsdaten anfordert.
- 1070 Resultiert die Ursache des Problems in der Marktkommunikation mit den externen Marktteilneh-
1071 mern, wird der Prozess an dieser Stelle verlassen.
- 1072 Ist die Verbindung zwischen SMGW und SMGW-Admin-N zustande gekommen und das Ergebnis
1073 der Prüfung der Konfiguration positiv, so unterbricht der SMGW-Admin-N die Verbindung zum

1074 SMGW und sendet einen Wake-Up-Call an das SMGW. Dieses prüft den Wake-Up-Call und etab-
1075 liert einen TLS-Kanal zum SMGW-Admin-N.

1076 Ab diesem Zeitpunkt geht die Verantwortung für den Betrieb des SMGW an den SMGW-Admin-N
1077 über.

1078 Der SMGW-Admin-N löscht den SMGW-Admin-A auf dem SMGW (gelöscht wird insbesondere
1079 das Kommunikationsprofil zum SMGW-Admin-A). Der SMGW-Admin-A hat danach keinen Zu-
1080 griff mehr auf das SMGW.

1081 Danach führt der SMGW-Admin-N die weitere Konfiguration des SMGW durch. Das SMGW ist
1082 anschließend wieder im normalen Betriebsmodus.

1083 Gemäß den vertraglichen Vereinbarungen oder den Festlegungen der Marktprozesse meldet der
1084 SMGW-Admin-N an den SMGW-Admin-A, dass der Wechsel erfolgreich durchgeführt worden ist,
1085 und teilt ihm die aktuellen Zählerstände nach Übernahme des SMGW mit und tauscht mit ihm ggf.
1086 abschließende Informationen aus. Zudem erhalten gemäß den Festlegungen der Marktprozesse alle
1087 beteiligten Externen Marktteilnehmer eine Nachricht über den vollzogenen Wechsel des SMGW-
1088 Admins.

1089 Erst nachdem der SMGW-Admin-A die Mitteilung erhalten hat, dass der Wechsel erfolgreich voll-
1090 zogen worden ist, und der SMGW-Admin-A nicht erneut die Rolle des SMGW-Admins überneh-
1091 men muss, werden die Zertifikate/Schlüssel des SMGW-Admin-A auf dem SMGW gelöscht.

1092 In den entsprechenden Logs des SMGW werden während des gesamten Prozesses alle Aktionen des
1093 SMGW, des SMGW-Admin-A und des SMGW-Admin-N protokolliert.

1094 **7.4 Zeitpunkt**

1095 Der Übergang des Betriebs von dem SMGW-Admin-A zum SMGW-Admin-N ist jederzeit mög-
1096 lich. Eine vorübergehende Einschränkung kann sich ggf. für den Zeitraum ergeben, in dem ein an-
1097 derer Wechselprozess ausgeführt wird (z.B. Wechsel des SMGW).

1098 **7.5 Verarbeitete Daten**

1099 **Primärdaten**

- 1100 • Gateway-ID
- 1101 • Zähler-ID
- 1102 • Zuordnung der IDs zu den konkreten Letztverbrauchern

- 1103 • Log-Einträge und weitere im SMGW gespeicherte Daten²⁶

1104 **Sekundärdaten**

- 1105 • Logging-Daten

1106 **7.6 Ort, Art und Weise der Verarbeitung**

1107 Die Datenverarbeitung findet im SMGW, beim SMGW-Admin-A und beim SMGW-Admin-N statt.

1108 Die Datenübertragung erfolgt elektronisch über die unten angegebenen Schnittstellen.

1109 Das SMGW speichert während des Prozesses des Administratorwechsels Logging-Daten in den
1110 Logs.

1111 **7.7 Schnittstellen**

1112 Zum Zwecke der Durchführung des Wechselprozesses finden Datenübertragungen zwischen dem
1113 SMGW-Admin-A und dem SMGW-Admin-N bzw. zwischen diesen und dem SMGW statt.

- 1114 • Schnittstelle zwischen SMGW-Admin-A und SMGW: IF_GW_WAN

- 1115 • Schnittstelle zwischen SMGW-Admin-N und SMGW: IF_GW_WAN

1116 Empfänger der aus dem SMGW ausgelesenen Daten (Log-Einträge und weitere im SMGW gespei-
1117 cherte Daten) ist der SMGW-Admin-A. Sofern vertraglich mit dem Letztverbraucher vorgesehen,
1118 kann der SMGW-Admin-A diese Daten für einen bestimmten Zeitraum speichern oder auch an eine
1119 andere Stelle weiterleiten.

1120 Im Rahmen der Marktkommunikation ist die Schnittstelle zwischen dem SMGW-Admin-A und
1121 dem SMGW-Admin-N zu beschreiben.

1122 **7.8 Besondere (Sicherheits-)Anforderungen²⁷**

- 1123 • Bezüglich der personenbezogenen Daten, insbesondere den aus dem SMGW ausgelesenen
1124 Messwerten und Log-Einträgen sind die datenschutzrechtlichen Regelungen zu beachten.

- 1125 • Für die vom SMGW-Admin-A ausgelesenen Daten gilt grundsätzlich dieselbe Höchstspei-
1126 cherdauer, die für diese Daten auch im Betrieb ohne Administratorwechsel gelten würde.

²⁶ Die zu sichernden Daten sind z.B. System-Log, Eichtechnisches Log, komplette Messwertliste, tarifierte Werte etc. (die Sicherung der Daten ist notwendig z.B. für spätere Nachvollziehbarkeit oder für Rückfragen des Letztverbrauchers).

²⁷ Bezüglich der Sicherheitsanforderungen sind die Vorgaben der TR-03109 insgesamt zu beachten. Hier werden nur bestimmte Aspekte hervorgehoben oder ergänzt.

7.9 Prozessschritte im Überblick

Nr.	Smart Meter Gateway Admin Alt (SMGW-Admin-A)	SMGW	Smart Meter Gateway Admin Neu (SMGW-Admin-N)	Bemerkung
1 Vorbedingungen				
1.1				die notwendigen Informationen zwischen allen beteiligten Externen Marktteilnehmern wurden ausgetauscht (siehe Marktkommunikation)
1.2			ist berechtigt ist, die Rolle des SMGW-Admins wahrzunehmen; insbesondere liegt ein Zertifikat über die Sicherheit vor	Zertifizierung des IT-Betriebs beim SMGW-Admin gemäß Anlage V zur TR-03109-1
1.3		befindet sich im normalen Betriebsmodus		d.h. insbesondere, dass die WAN-Kommunikation funktioniert
1.4	hat Zugriffsrechte auf das SMGW	ist auf den SMGW-Admin-A konfiguriert	hat keine Zugriffsrechte auf das SMGW	
1.5	hat mit dem SMGW-Admin-N die notwendigen Informationen ausgetauscht		hat mit dem SMGW-Admin-A die notwendigen Informationen ausgetauscht	Marktkommunikation
1.6			besitzt sein SMGW-Admin-Zertifikat aus der SM-PKI	ansonsten Beantragung eines SMGW-Admin-Zertifikats bei der SM-PKI
2 Kernprozess				
2.1			meldet den Wechsel beim SMGW-Admin-A an	
2.2	sendet dem SMGW-Admin-N die Informationen zur bestehenden Mess-Infrastruktur des SMGW			
2.3			sendet seine Zertifikate und Verbindungsdaten an den SMGW-Admin-A	
2.4				Gültigkeitsprüfung gegen PKI-Sperrliste
2.5	sichert Daten vom SMGW	optional: löscht alle nicht mehr benötigten Daten und Profile auf dem SMGW		siehe Erläuterung oben im Kapitel
2.6	überträgt Verbindungs-Daten für SMGW-Admin-N auf das SMGW	Empfang der Daten von SMGW-Admin-A		die Konfiguration enthält u.a. Kommunikationsparameter für das WAN (z.B. GSM-Parameter), Verbindungsadresse zum SMGW-Admin-N (evtl. temporäre Adresse), Zertifikate des SMGW-Admin-N, Zertifikatskette zur Prüfung der Konfigurations-Signatur
2.7		prüft Signatur der Konfiguration anhand des Zertifikats von SMGW-Admin-A		
2.8		prüft Signatur des Zertifikats des SMGW-Admin-N gegen das Root-Zertifikat		
2.9		meldet sich beim SMGW-Admin-N an (baut Verbindung zum SMGW-Admin-N auf)		

Nr.	Smart Meter Gateway Admin Alt (SMGW-Admin-A)	SMGW	Smart Meter Gateway Admin Neu (SMGW-Admin-N)	Bemerkung
2.10			liest die Konfiguration aus dem SMGW aus und prüft diese	Prüfung erfolgt anhand der vom SMGW-Admin-A zur Verfügung gestellten Informationen aus Schritt 2.2 und weiterer Informationen, die aus der Marktkommunikation (Schritt 1.1) entstammen
2.11			trägt das Ergebnis der Prüfung in das System-Log ein	für den Fall eines negativen Ergebnisses siehe Beschreibung oben im Kapitel
2.12			unterbricht Verbindung zum SMGW und sendet Wake-Up-Call an das SMGW	
2.13		prüft Wake-Up-Call und etabliert TLS-Kanal zum SMGW-Admin-N		ab hier geht Verantwortung für SMGW-Betrieb an SMGW-Admin-N über
2.14			SMGW-Admin-N löscht SMGW-Admin-A auf SMGW	insbesondere das Kommunikationsprofil zum SMGW-Admin-A
2.15			führt ggf. weitere Konfiguration des SMGW durch	
2.16	erhält Bestätigung, dass der Wechsel erfolgreich durchgeführt wurde; ggf. mitsamt des aktuellen Zählerstandes im Zeitpunkt der Übernahme des SMGW			alle beteiligten Externen Marktteilnehmer erhalten eine Nachricht über den vollzogenen Wechsel des SMGW-Admins (gemäß Marktkommunikation)
3 Nachbedingungen				
3.1	die Bestätigung des erfolgreichen Wechsels liegt vor			
3.2	hat keine Zugriffsrechte mehr auf das SMGW			
3.3		der SMGW-Admin-N ist konfiguriert		
3.4	tauscht ggf. abschließende Informationen mit SMGW-Admin-N aus		tauscht ggf. abschließende Informationen mit SMGW-Admin-A aus	wenn nicht schon in Schritt 2.16 geregelt
3.5		ist im normalen Betriebsmodus		
4 Nebenprozesse				
4.1		protokolliert während des gesamten Prozesses alle Aktionen des SMGW und des SMGW-Admin-A und des SMGW-Admin-N in den entsprechenden Logs		