Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03109-1

Anlage VI: Betriebsprozesse

Version 1.0, Datum 18.03.2013

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

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

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

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

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

Werden im Rahmen der Beschreibung der einzelnen Prozesse bestimmte Beteiligte bzw. Rollen genannt, so gelten die für diese gemachten Angaben auch für von ihnen rechtmäßig eingesetzte autorisierte Dienstleister.

Die in dieser Anlage behandelten Prozesse beschreiben Ausschnitte aus dem Lebenszyklus des SMGW von der Inbetriebnahme bis zur Außerbetriebnahme. Für Prozesse und Arbeitsschritte, die zeitlich vor den energiewirtschaftlichen oder energierechtlichen Prozessen bzw. Aktivitäten[2] erfolgen, wozu die Entwicklung, Produktion, Eichung, Beschaffung der SMGW zählen, werden keine Prozessbeschreibungen vorgenommen.

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

In dieser Anlage werden einige kritische Prozesse beschrieben. Bisher beschrieben sind die folgenden Prozesse:

- Inbetriebnahme des Smart Meter Gateways
- 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.

- Datenübertragung
- Administration
- Störungserkennung/Diagnose
- Wechsel des Smart Meter Gateway Administrators

Die Anlage kann sukzessive um die Beschreibung weiterer Prozesse erweitert werden, wie z.B.

- Austausch, Hinzufügen oder Entfernen von Zählern
- Wechsel des Lieferanten
- Außerbetriebnahme des Smart Meter Gateways

Die Beschreibungen zu den Prozessen in dieser Anlage sind grundsätzlich nur informativ. Ausnahmen können sich dort ergeben, wo es auf die genaue Einhaltung einzelner Schritte ankommt. Diese Prozesse bzw. Schritte sind entsprechend gekennzeichnet. Hinsichtlich der Definitionen der in dieser Anlage verwendeten Begriffe wird auf die BSI TR-03109-1 verwiesen.

Die Darstellung bezieht sich in der vorliegenden Version dieser Anlage vornehmlich auf den Bereich der Elektroenergie.

2 Inbetriebnahme des Smart Meter Gateways

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:

- (A) SMGW exklusive Sicherheitsmodul
- (B) Sicherheitsmodul
- (C) SMGW inklusive Sicherheitsmodul

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

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.

Grundsätzliche Anmerkungen:

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.

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 Marktkommunikation[3]. Gleichermaßen müssen die Zertifikate über die Marktkommunikation rechtzeitig an den SMGW-Admin übermittelt werden.

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 Verordnungsgeber[4] zu berücksichtigen sind.

[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.

2.1 Smart Meter Gateway exkl. Sicherheitsmodul (A)

2.1.1 Entwicklung

Rolle:

Hersteller des SMGW

Beschreibung:

Entwicklung des SMGW beim Hersteller.

2.1.2 Produktion

Rolle:

Hersteller des SMGW

Beschreibung:

Produktion des SMGW beim Hersteller.

2.1.3 Vor-Personalisierung beim Hersteller

Rolle:

Hersteller des SMGW

Beschreibung:

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

Vergabe einer eindeutigen SMGW-ID gemäß der Norm DIN 43863-5:2012-04 "Herstellerübergreifende Identifikationsnummer für Messeinrichtungen“.

2.2 Sicherheitsmodul (B)

2.2.1 Entwicklung

Rolle:

Hersteller des Sicherheitsmoduls

Beschreibung:

Entwicklung des Sicherheitsmoduls beim Hersteller.

2.2.2 Produktion

Rolle:

Hersteller des Sicherheitsmoduls

Beschreibung:

Produktion des Sicherheitsmoduls und Einspielung des Betriebssystems beim Hersteller.

2.2.3 Initialisierung

Rolle:

Initialisierer des Sicherheitsmoduls

Beschreibung:

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

2.3 Smart Meter Gateway inkl. Sicherheitsmodul (C)

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

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

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

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

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

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

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

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

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

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

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

2.3.1 Vor-Personalisierung und Integration

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

Die hier beschriebene Phase setzt sich aus den Teilphasen der *Vor-Personalisierung* und der *Integration* zusammen und wird beim Integrator durchgeführt. Die *Vor-Personalisierung* gliedert sich dabei in zwei Teilphasen. Während in der Teilphase *Vor-Personalisierung 1* Schlüssel- und Zertifikatsmaterial generiert und aufgebracht wird, das unabhängig vom späteren SMGW-Admin ist, wird in der Teilphase *Vor-Personalisierung 2* vom SMGW-Admin spezifisches Schlüssel- und Zertifikatsmaterial in das SMGW importiert.

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

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

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

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

2.3.1.1 Vor-Personalisierung 1

Rolle:

Integrator

Anforderungen an den Integrator:

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

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

- Import des SM-PKI-Root-Zertifikates (ROOT_WAN_SIG_CRT) in das Sicherheitsmodul

  Hinweis: Das SM-PKI-Root-Zertifikat stellt nachfolgend einen zentralen Sicherheitsanker dar; seine Integrität und Authentizität ist daher sicherzustellen. Es erfolgt eine vertrauenswürdige Übermittlung des Zertifikats an den Integrator. Die Authentizität wird z.B. über einen Abgleich eines Fingerprints über einen zweiten Kanal sichergestellt.

- Onboard-Generierung von Key-Paaren für das SMGW im Sicherheitsmodul (vorläufige SMGW-Schlüssel für die WAN-Kommunikation):
  - (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
  - (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
  - (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)
- Export der Public Keys:
  - GW_WAN_TLS_PUB_PRE
  - GW_WAN_SIG_PUB_PRE
  - GW_WAN_ENC_PUB_PRE

  Hinweis: Die zugehörigen privaten Schlüssel verbleiben im Sicherheitsmodul und können nicht ausgelesen werden.

- Erstellung von entsprechenden Zertifikatsrequests für die Gütesiegel-Zertifikate zu den SMGW-Schlüsseln
- Senden der Requests „an die SM-PKI“

  Hinweis: Hierzu benötigt der Integrator eine Verbindung zur SM-PKI. Es besteht hierbei die Möglichkeit, dass der Integrator selbst eine Sub-CA in der SM-PKI betreibt.
- Import der Gütesiegel-Zertifikate in das Sicherheitsmodul:
  - GW_WAN_TLS_CRT_PRE
  - GW_WAN_SIG_CRT_PRE
  - GW_WAN_ENC_CRT_PRE

Hinweis: Sämtliches im Rahmen der *Vor-Personalisierung 1* generiertes bzw. eingebrachtes Schlüssel- und Zertifikatsmaterial ist unabhängig vom späteren konkreten SMGW-Admin.

Hinweis: Findet die Teilphase *Integration* vor der *Vor-Personalisierung 1* statt, ist die lokale Schnittstelle des SMGW unter Nutzung der Integrator-PIN erforderlich.

2.3.1.2 Integration

Rolle:

Integrator

Aufgaben in der *Integration* von Sicherheitsmodul und Gateway:

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

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

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

2.3.1.3 Vor-Personalisierung 2

Rolle:

Integrator

Voraussetzungen:

- Die *Vor-Personalisierung 1* und die *Integration* von Sicherheitsmodul und SMGW sind abgeschlossen.
- Zum Zeitpunkt der *Vor-Personalisierung 2* ist der konkrete SMGW-Admin bekannt.
- Der SMGW-Admin hat seine Schlüsselpaare generiert:
  - (GWADM_TLS_PRV, GWADM_TLS_PUB)
  - (GWADM_SIG_PRV, GWADM_SIG_PUB)
  - (GWADM_ENC_PRV, GWADM_ENC_PUB)
  - (GWADM_AUT_PRV, GWADM_AUT_PUB)

  Hinweis: An die Schlüsselgenerierung beim SMGW-Admin bestehen spezifische Anforderungen wie z.B. die Nutzung eines HSM (siehe TR-03109-4).
- Der SMGW-Admin besitzt für seine zuvor genannten Schlüsselpaare jeweils ein Zertifikat der SM-PKI, also:
  - GWADM_TLS_CRT
  - GWADM_SIG_CRT
  - GWADM_ENC_CRT
  - GWADM_AUT_CRT
- Der SMGW-Admin erstellt eine sog. Initiale Konfigurationsdatei, die mindestens die folgenden Daten beinhaltet:
  - Kommunikationsparameter des SMGW-Admins (SMGW-Admin-Adresse)
  - Zertifikate GWADM_TLS_CRT, GWADM_SIG_CRT, GWADM_ENC_CRT und GWADM_AUT_CRT mit zugehöriger Zertifikatskette (aus der SM-PKI) exklusive SM-PKI-Root-Zertifikat
- Der SMGW-Admin signiert die Initiale Konfigurationsdatei mit seinem Signaturschlüssel GWADM_SIG_PRV.
- Die signierte Initiale Konfigurationsdatei wird an den Integrator übermittelt.

Aufgaben in der Teilphase *Vor-Personalisierung 2*:

Einspielen der Kommunikationsparameter und Zertifikate des SMGW-Administrators unter Nutzung der lokalen Schnittstelle des SMGW, hierzu:

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

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

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

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

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

- Im Sicherheitsmodul
  - Gateway-System-PIN (Referenzwert)
  - ggf. Schlüssel für die Speicherverschlüsselung des SMGW
  - Zertifikat ROOT_WAN_SIG_CRT der SM-PKI-Root
  - 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 o Gütesiegel-Zertifikate
398 ▪ GW_WAN_TLS_CRT_PRE
399 ▪ GW_WAN_SIG_CRT_PRE
400 ▪ GW_WAN_ENC_CRT_PRE
401 o 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 o Gateway-System-PIN
408 o Schlüssel für die Speicherverschlüsselung des SMGW
409 o 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 o Kommunikationsparameter des SMGW-Admin (SMGW-Admin-Adresse)

417

418

2.3.2 Installation und Vor-Ort-Inbetriebnahme des SMGW

Rolle:

Erstkonfigurator

Vorbedingungen:

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

Aufgaben in dieser Phase:

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

2.3.3 Personalisierung

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

Rolle:

SMGW-Admin

Aufgaben in der *Personalisierung* des SMGW:

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

Personalisierung und Integration von Sicherheitsmodul und Gateway im Sicherheitsmodul vor.

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

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

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

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

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

    - (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB)
    - (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB)
    - (GW_WAN_ENC_PRV, GW_WAN_ENC_PUB)

  - Export der Public Keys GW_WAN_TLS_PUB, GW_WAN_SIG_PUB, GW_WAN_ENC_PUB (die zugehörigen privaten Schlüssel verbleiben im Sicherheitsmodul und können nicht ausgelesen werden);

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

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

- Schließen des TLS-Kanals zwischen SMGW-Admin und SMGW.

Mit Abschluss der Personalisierung befindet sich das SMGW in seinem zertifizierten Zustand. Das SMGW steht nun für die Nutzung im Normalbetrieb bereit.

Der SMGW-Admin kann nachfolgend weitere Administrationstätigkeiten am SMGW bzw. am Sicherheitsmodul vornehmen, siehe Kapitel 2.3.4.

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

- Im Sicherheitsmodul
  - Gateway-System-PIN (Referenzwert)
  - ggf. Schlüssel für die Speicherverschlüsselung des SMGW
  - Zertifikat ROOT_WAN_SIG_CRT der SM-PKI-Root
  - vorläufige Gateway-Schlüsselpaare
    - (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE)
    - (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE)
    - (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE)
  - Gütesiegel-Zertifikate
    - GW_WAN_TLS_CRT_PRE
    - GW_WAN_SIG_CRT_PRE
    - GW_WAN_ENC_CRT_PRE
  - Public Keys des SMGW-Admin
    - GWADM_TLS_PUB
    - GWADM_SIG_PUB
    - GWADM_ENC_PUB
    - GWADM_AUT_PUB
  - Gateway-Betriebsschlüsselpaare
    - (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB)
    - (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB)
    - (GW_WAN_ENC_PRV, GW_WAN_ENC_PUB)

- Im Smart Meter Gateway
  - Gateway-System-PIN
  - Schlüssel für die Speicherverschlüsselung des SMGW
  - Zertifikate des SMGW-Admin:
    - GWADM_TLS_CRT
    - GWADM_SIG_CRT
    - GWADM_ENC_CRT
    - GWADM_AUT_CRT

    jeweils inkl. der zugehörigen Zertifikatskette (aus der SM-PKI) exklusive des SM-PKI-Root-Zertifikats
  - Kommunikationsparameter des SMGW-Admin (SMGW-Admin-Adresse)
  - Betriebszertifikate
    - GW_WAN_TLS_CRT
    - GW_WAN_SIG_CRT
    - GW_WAN_ENC_CRT

2.3.4 Normalbetrieb

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

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

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

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

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

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

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

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

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

2.4 Besondere (Sicherheits-)Anforderungen[6]

Während der Lagerung und beim Transport von vor-personalisierten SMGW, initialisierten Sicherheitsmodulen sowie von integrierten und personalisierten SMGW sind dem jeweiligen Schutzbedarf 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 erfor-
557 derlichen Profile eingerichtet und vom SMGW aktiviert worden sind (siehe den Prozess *Inbetrieb-*
558 *nahme des Smart Meter Gateways*), kann die Messung (der Entnahme oder Einspeisung) von Elekt-
559 rizität, Gas, Wasser, Wärme und anderen zu messenden Energien oder Stoffen und die Messung
560 von Netzzustandsdaten beginnen.

561 Die von den Messeinrichtungen an das SMGW übertragenen Messdaten werden im SMGW gespei-
562 chert. In der Folge werden diese Daten vom SMGW in seiner Funktion als „Datenaufbereiter" ver-
563 arbeitet (siehe BSI TR-03109-1, Kapitel 4) und die Ergebnisse dieser Verarbeitung werden vom
564 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 Abrech-
571 nung der bezogenen und eingespeisten Energie- oder Stoffmengen sowie die für den Zustand der
572 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.

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

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

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

Die Messwerte werden vom SMGW mit einem Zeitstempel und mit der Information versehen, ob der Wert gültig oder ungültig ist, und sodann im SMGW unverändert[8] und unveränderbar gespeichert (vgl. BSI TR-03109-1).

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

3.4 Zeitpunkt

Der SMGW-Admin legt gemäß den vertraglichen Vereinbarungen zwischen den Beteiligten (Lieferant[en], Endkunde[n]/Anschlussnehmer/Anschlussnutzer, weitere Dienstleister), gemäß den Auswertungsprofilen und gemäß den technischen Voraussetzungen der angeschlossenen Messeinrichtungen die Zeitabstände fest, in denen das SMGW die Messwerte von den Messeinrichtungen empfängt oder erfragt.

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

3.5 Verarbeitete Daten

Primärdaten[9]

- Zähler-ID
- Zählpunktbezeichnung
- Messwerte
- Zeitstempel
- Information, ob der Wert gültig oder ungültig ist
- 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.

Sekundärdaten[10]

- Logging-Daten

3.6 Ort, Art und Weise der Verarbeitung

Die Messeinrichtung stellt die Messwerte zur Verfügung. Die Übertragung der Messwerte von der Messeinrichtung an das SMGW erfolgt im LMN drahtgebunden oder drahtlos. Die Weiterverarbeitung im SMGW findet automatisch statt.

Die Art und Weise der Überwachung des Prozesses durch den SMGW-Admin liegt in dessen Ermessen.[11]

Die Protokollierung erfolgt in den Logs.

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

3.7 Schnittstellen

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

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

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

3.8 Besondere (Sicherheits-)Anforderungen[12]

- Sichere Übertragung von Daten zwischen SMGW und SMGW-Admin (durch geeignete Sicherheitsmaßnahmen, 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.

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

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-		

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

4 Datenübertragung

4.1 Verortung im Gesamtkontext

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

4.2 Beteiligte, Rollen und Funktionen

- Smart Meter Gateway-Administrator (SMGW-Admin)
- Externe Marktteilnehmer[13]

Die Externen Marktteilnehmer sind die Empfänger oder gegebenenfalls auch Sender von Datenübertragungen.

Der SMGW-Admin ermöglicht die erforderlichen Datenübertragungen[14] durch entsprechende Konfiguration des SMGW. Ferner überwacht er die Datenübertragung.

4.3 Beschreibung und Zweck

Zum Zwecke der vertraglich vereinbarten oder gegebenenfalls technisch erforderlichen Datenübertragungen von Mess- und Statuswerten (turnusmäßige Tarifdaten- und Netzzustandsdatenauslieferung, spontane Messwertauslesung) aus dem SMGW an Externe Marktteilnehmer oder von Steuerbefehlen der Externen Marktteilnehmer an das SMGW erfolgen die folgenden Schritte:

Voraussetzungen dafür, dass das SMGW Datenübertragungen an Externe Marktteilnehmer vornehmen kann, sind,

- dass der SMGW-Admin vorab im SMGW die als Empfänger von Datenübertragungen berechtigten Externen Marktteilnehmer (Kommunikationsendpunkte) in Kommunikationsprofilen 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).

- dort das notwendige Schlüsselmaterial hinterlegt,
- die Tarifprofile ins SMGW einbringt, nach welchen die Übertragungen an die Externen Marktteilnehmer inhaltlich und zeitlich gesteuert werden.

Die für die Konfiguration erforderlichen Informationen[15] werden von den Vertragspartnern des Anschlussnutzers dem SMGW-Admin zur Verfügung gestellt.

Bezüglich des Aufbaus und der Absicherung der Verbindung für die Übermittlung von Daten an Externe Marktteilnehmer vgl. BSI TR-03109-1.

Der Externe Marktteilnehmer kann - sofern er dazu berechtigt ist - den Administrator beauftragen,[16] das SMGW zum Aufbau einer Verbindung zu ihm zu veranlassen. Nach einem „Wake-Up“ durch den SMGW-Admin stellt das SMGW eine Verbindung mit dem Administrator her, der dann das SMGW veranlasst, eine Verbindung zum Externen Marktteilnehmer aufzubauen.

Ein Externer Marktteilnehmer kann Daten vom SMGW erhalten, die das SMGW an ihn adressiert und für ihn verschlüsselt und signiert hat.

Das SMGW protokolliert alle Datenübertragungen in den entsprechenden Logs (siehe BSI TR-03109-1).

Der SMGW-Admin stellt im Rahmen seiner Aufgaben durch geeignete Maßnahmen sicher, dass die Datenübertragung ordnungsgemäß abläuft.[17]

4.4 Zeitpunkt

Datenübertragungen finden im laufenden Betrieb statt.

Das SMGW überträgt die Registerwerte (gemäß Tarifprofilen) der im Profil definierten Register bei Eintreten eines bestimmten Auslösers (Trigger).[18] Das SMGW wartet für den Versand von Registerwerten auf den Aufbau der sicheren Verbindung zum Marktteilnehmer im WAN und versendet dann die Registerwerte unmittelbar nach dem Verbindungsaufbau. Das SMGW bestimmt jeden weiteren Versandzeitpunkt aus dem ersten Abrechnungs- bzw. Auswertungszeitpunkt und dem Abrechnungs- bzw. Auswertungsintervall.

4.5 Verarbeitete Daten

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.

Es kommen je nach Anwendungsfall und Vertragsgestaltung diverse Inhaltsdaten in Frage, die unterschiedlich klassifiziert werden können, z.B.

- Messdaten
- Netzzustandsdaten
- abrechnungsrelevante Daten (für verschiedene Zwecke der Abrechnung und damit ggf. verschiedene Empfänger)
- nicht abrechnungsrelevante Daten
- Gateway-ID
- Zähler-ID (oder Pseudonym)
- Marktteilnehmer-ID/-Adressen
- kryptografische Schlüssel und Signaturdaten
- Zeitstempel, Gültigkeit, OBIS-Kennzahl des Messwertsatzes und andere Zusatzinformationen

Sekundärdaten

Logeinträge im Kunden-Log über die Datenübertragungen an Externe Marktteilnehmer

4.6 Ort, Art und Weise der Verarbeitung

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

Das SMGW speichert zu versendende Daten so lange, bis der Versand erfolgt ist und von der Gegenstelle quittiert wurde.

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

4.7 Schnittstellen

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

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

4.8 Besondere (Sicherheits-)Anforderungen[19]

- Neben den sich aus der BSI TR-03109-1 ergebenden Anforderungen an die Kommunikationsprotokolle, an die Inhaltsdatenverschlüsselung, Signierung, Absicherung der Kommunikation und Authentifizierung sind die Anforderungen aus § 21e Abs. 3 EnWG zu beachten:
- Danach müssen die an der Datenübermittlung beteiligten Stellen dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit treffen, die insbesondere die Vertraulichkeit und Integrität der Daten sowie die Feststellbarkeit der Identität der übermittelnden Stelle gewährleisten. Im Falle der Nutzung allgemein zugänglicher Kommunikationsnetze müssen Verschlüsselungsverfahren angewendet werden, die dem jeweiligen Stand der Technik entsprechen.
- Die personenbezogenen bzw. personenbeziehbaren Daten sowie jegliche Zuordnungen von diesen Daten zu bestimmten oder bestimmbaren natürlichen Personen dürfen nicht an Unbefugte gelangen.
- Im Falle der Durchleitung löscht der Weiterleitende die Daten nach erfolgreicher Übertragung an den vorgesehenen Empfänger.
- Beim Versand von nicht abrechnungsrelevanten Daten[20] muss das Verfahren der Pseudonymisierung gemäß BSI TR-03109-1 durchgeführt werden können.[21]
- Alle auf vertraglicher Grundlage und ebenso alle auf gesetzlicher Anordnung basierenden Datenübertragungen müssen den in der BSI TR-03109-1 dargestellten Anforderungen an die Kommunikationsverbindungen, Kommunikationsprofile und an die Datensicherheit entsprechen.

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.

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 Netzzustandsdaten)
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	

747 Tabelle 2: Prozessschritte Datenübertragung

5 Administration

5.1 Verortung im Gesamtkontext

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

- Geräteverwaltung (Geräte, d.h. Zähler, CLS-Geräte, Anzeigeeinheiten im SMGW registrieren und einem Letztverbraucher zuordnen und diese Zuordnung wieder aufheben und Geräte löschen)
- Mandantenverwaltung (Letztverbraucher anlegen, bearbeiten, löschen und zugeordnete Zertifikate einrichten oder löschen; Verwaltung Kennung/Passwort für Anzeigeeinheit)
- Profilverwaltung (Kommunikationsprofile und Regelwerke zur Tarifierung bzw. Netzzustandsmeldung einbringen, aktivieren und löschen)
- Schlüssel-/Zertifikatsmanagement (Schlüssel und Zertifikate für die Kommunikation mit Zählern, CLS-Geräten, externen Marktteilnehmern einbringen, aktivieren, deaktivieren bzw. löschen; Umschalten auf anderen Kryptoalgorithmus im Sicherheits-Modul)
- Firmware-Update (neue Firmware aufspielen, verifizieren und aktivieren)
- Wake-Up-Konfiguration (Adresse des Wake-Up-Services konfigurieren)
- Monitoring des SMGW (Zustand des SMGW abfragen, Logeinträge aus dem System- und eichtechnischen Log auslesen und auswerten, Reaktion auf Alarmmeldungen)
- Einspielen von Sicherheits-Updates
- Einspielen von Anwendungs-Software

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

5.2 Beteiligte, Rollen und Funktionen

- SMGW-Admin
- Autorisierte Service-Techniker
- Prüfstellen, Eichbehörde
- Anschlussnutzer

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

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

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

5.3 Beschreibung und Zweck

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

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

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

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

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

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

Der SMGW-Admin stellt durch von ihm zu treffende geeignete Maßnahmen sicher, dass seine Tätigkeiten nicht zu fehlerhaften Funktionen des SMGW führen. Bei Fehlfunktionen ergreift er die erforderlichen Korrekturmaßnahmen. Das Konzept und die Mittel des SMGW-Admins für Monitoring, Überprüfungen und Korrekturmaßnahmen unterliegen einer regelmäßigen Kontrolle und Zertifizierung durch vom BSI anerkannte Prüfstellen. Diese überprüfen zudem die korrekte Durchführung der Maßnahmen des Sicherheitskonzepts des SMGW-Admins (siehe Anlage V - Anforderungen zum Betrieb beim Administrator).

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

5.4 Zeitpunkt

Die Administrationstätigkeiten erfolgen jederzeit im laufenden Betrieb.

5.5 Verarbeitete Daten

Primärdaten

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

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

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

- Personennamen
- Adressdaten
- Kommunikationsdaten
- Gateway-ID, Zähler-ID, Komponenten-ID

Sekundärdaten

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

5.6 Ort, Art und Weise der Verarbeitung

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

Überprüfungen durch anerkannte Prüfstellen und gegebenenfalls durch die Eichbehörde erfolgen beim SMGW-Admin und auf der Grundlage der von diesem auf Anforderung zur Verfügung gestellten Daten.

Die für den Anschlussnutzer vorgesehenen Informationen werden im Kundenlog gespeichert. Dieses wird ihm über die Anzeigeeinheit verfügbar gemacht.

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

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

Es erfolgen Verarbeitungen und Speicherungen von Daten auch beim SMGW-Admin bzw. auf dessen Systemen und gegebenenfalls auf den vom Service-Techniker für den Einsatz am SMGW mitgeführten mobilen Verarbeitungs- und Speichermedien.

Die Protokollierungsdaten werden in den Logs des SMGW gespeichert.

5.7 Schnittstellen

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

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

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

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

5.8 Besondere (Sicherheits-)Anforderungen[22]

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

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

874 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 *Nacheichung im laufenden Betrieb*
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		

Nr.	SMGW	SMGW-Admin	Bemerkung
5.9		beachtet Aufbewahrungspflichten und Lösch-fristen	

Tabelle 3: Prozessschritte Administration

6 Störungserkennung/Diagnose

6.1 Verortung im Gesamtkontext

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

6.2 Beteiligte, Rollen und Funktionen

- Smart Meter Gateway Administrator
- Autorisierter Service-Techniker

6.3 Beschreibung und Zweck

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

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

Der Einsatz des autorisierten Service-Technikers vor Ort am SMGW kann beispielsweise bei folgenden Störungen erforderlich werden:

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

- das SMGW hat in seinen Logs häufige Fehler eines oder mehrerer Zähler vermerkt
- das SMGW meldet Gehäusebruch an den SMGW-Admin
- oder es liegen ähnliche Konstellationen oder andere unklare Probleme vor, die ein Eingreifen des SMGW-Admins bzw. des autorisierten Service Technikers erforderlich machen.

Der autorisierte Service-Techniker authentisiert sich am SMGW mit seinem Zertifikat aus der SM-PKI.

Der autorisierte Service-Techniker wird auf Anweisung des SMGW-Admins tätig. Über die HAN-Schnittstelle verbindet er sein mobiles Gerät (z.B. Laptop) am SMGW, das einen TLS-Kanal etabliert. Sodann ruft der Service-Techniker, sofern möglich, Diagnosedaten ab.[23] Dafür steht ihm ausschließlich ein lesender Zugriff (read-only) zur Verfügung. Danach meldet sich der Service-Techniker am SMGW ab, das die lokale Verbindung zum Gerät des Service-Technikers terminiert.

Der autorisierte Service-Techniker kann auf Anweisung des SMGW-Admins die vor Ort erhobenen Diagnosedaten an den SMGW-Admin übertragen (z.B. über eine gesicherte Funkverbindung).[24]

Der autorisierte Service-Techniker übermittelt seinen Diagnosebericht (mitsamt optisch wahrgenommenen Feststellungen, z.B. Siegel- oder Gehäusebruch, ggf. auch seinen Bericht über die durch ihn vor Ort durchgeführte Fehlerbehebung) an den SMGW-Admin. Danach archiviert der SMGW-Admin die erforderlichen und löscht die nicht erforderlichen Daten. Der Service-Techniker löscht nach erfolgreicher Übertragung von Daten aus dem SMGW an den SMGW-Admin selbige auf seinen Geräten.

Das SMGW protokolliert während des gesamten Prozesses alle Aktionen des SMGW, des SMGW-Admins und des autorisierten Service-Technikers in den entsprechenden Logs.

Die sich an die Ermittlung der Daten anschließende Fehlerdiagnose und daraufhin die Fehlerbehebung werden je nach Problemfall und Vertragskonstrukt hinsichtlich der Zusammenarbeit zwischen SMGW-Admin und autorisiertem Service-Techniker durch einen von beiden oder durch beide arbeitsteilig durchgeführt.

6.4 Zeitpunkt

Der Prozess ist grundsätzlich jederzeit im laufenden Betrieb möglich.

6.5 Verarbeitete Daten

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.

- Gateway-ID
- Zähler-ID
- Zuordnung der IDs zu den konkreten Letztverbrauchern (Personennamen, Adressen, Kommunikationsdaten)
- Log-Einträge
- Diagnosedaten
- Inhalte des Diagnose- und ggf. des Störungsbehebungsberichts des Service-Technikers

Sekundärdaten

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

6.6 Ort, Art und Weise der Verarbeitung

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

Die Protokollierungsdaten werden in den Logs des SMGW gespeichert.

6.7 Schnittstellen

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

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

6.8 Besondere (Sicherheits-)Anforderungen[25]

- Für die Sicherheit der vom autorisierten Service-Techniker erhobenen Daten während der Erhebung, während ihrer Speicherung bzw. Verarbeitung auf den Geräten des Service-Technikers und während ihrer Übertragung an den SMGW-Admin sind dem Schutzbedarf angemessene technische und organisatorische Maßnahmen zu ergreifen (Gewährleistung einer durchgehend hohen Sicherheit gemäß den Anforderungen der BSI TR-03109-1 zu den Kommunikationsverbindungen).
- Hinsichtlich der personenbezogenen Daten, insbesondere der aus dem SMGW ausgelesenen 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 Leistungserschleichungen 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

7 Wechsel des Smart Meter Gateway Administrators

7.1 Verortung im Gesamtkontext

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

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

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

Grundsätzlicher Hinweis:

Ein Wechsel des SMGW-Admin stellt ein umfangreiches Projekt dar, in den alle vertraglich verbundenen Partner involviert werden müssen. Alle Beteiligten sollten sich im Voraus auf einen Projektablauf einigen und klare Verantwortlichkeiten festlegen. Besonderes Augenmerk ist dabei auf die verlustfreie Übergabe der Daten, die Aufrechterhaltung des Betriebes und die lückenlose Messwerterfassung bzw. Tarifierung zu richten.

7.2 Beteiligte, Rollen und Funktionen

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

7.3 Beschreibung und Zweck

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

Vorbedingungen für die Durchführung des Administratorwechsels sind:

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

- der SMGW-Admin-N ist berechtigt, die Rolle des SMGW-Admins wahrzunehmen; insbesondere muss er hierfür sicherheitszertifiziert sein (siehe TR-03109-1, Anlage V: Anforderungen zum Betrieb beim Administrator);
- das SMGW befindet sich im normalen Betriebsmodus, d.h. insbesondere, dass die WAN-Kommunikation funktioniert; andernfalls ist eine Störungsermittlung (siehe Prozess *Störungserkennung/Diagnose*) und Störungsbehebung erforderlich;
- der SMGW-Admin-A verfügt über Zugriffsrechte auf das SMGW, das auf den SMGW-Admin-A konfiguriert ist;
- SMGW-Admin-A und SMGW-Admin-N haben die notwendigen Informationen ausgetauscht (im Rahmen der Marktkommunikation);
- der SMGW-Admin-N besitzt sein SMGW-Admin-Zertifikat aus der SM-PKI, das er anderenfalls bei der SM-PKI beantragt.

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

Der SMGW-Admin-A sendet dem SMGW-Admin-N die Informationen zur bestehenden Mess-Infrastruktur des SMGW. Hierzu zählen insbesondere Informationen zu den angeschlossenen Zählern. Nicht zur Verfügung gestellt werden müssen hingegen z.B. Informationen zu bestehenden Tarifprofilen oder Kommunikationsprofilen.

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

Je nach eventuell bestehenden vertraglichen Vereinbarungen zwischen dem Letztverbraucher, Externen Marktteilnehmern und dem SMGW-Admin-A sichert der SMGW-Admin-A die Daten vom SMGW oder löscht alle nicht mehr benötigten Daten auf dem SMGW. Für eine Sicherung der Daten kommen grundsätzlich alle Daten infrage, insbesondere aber die abrechnungsrelevanten Messwerte.

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

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

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

Der SMGW-Admin-A überträgt die Verbindungs-Daten für den SMGW-Admin-N auf das SMGW. Diese 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 und die Zertifikatskette zur Prüfung der Konfigurations-Signatur.

Das SMGW prüft die Signatur der vorstehenden Konfiguration anhand des Zertifikats des SMGW-Admin-A und prüft die Signatur des Zertifikats des SMGW-Admin-N gegen das Root-Zertifikat. Danach baut das SMGW eine Verbindung zum SMGW-Admin-N auf.

Hinweis: Evtl. ist die Übergabe der Kommunikationstechnik zu regeln. Ggf. muss die Kommunikationstechnik beim Letztverbraucher vorher getauscht werden.

Im Fehlerfall, wenn z.B. die Kommunikation nicht zustande kommt, nimmt das SMGW einen entsprechenden Eintrag im System-Log vor und meldet den Fehler an den SMGW-Admin-A. Nach Fehlerermittlung und -behebung durch den SMGW-Admin-A (ggf. unter Hinzuziehung des autorisierten Service-Technikers gemäß dem Prozess *Störungserkennung/Diagnose*) sendet der SMWG-Admin-A erneut die Verbindungsdaten für SMGW-Admin-N an das SMGW. Ggf. ist auch erforderlich, dass der SMGW-Admin-A erneut vom SMWG-Admin-N Zertifikate und Verbindungsdaten anfordert.

Ist die Verbindung zwischen SMGW und SMGW-Admin-N zustande gekommen, liest der SMGW-Admin-N die Konfiguration aus dem SMGW aus und prüft diese. Die Prüfung durch den SMGW-Admin-N erfolgt anhand der zu Beginn des Wechselprozesses vom SMGW-Admin-A zur Verfügung gestellten Informationen und ggf. weiterer Informationen vom SMGW-Admin-A oder Externen Marktteilnehmern gemäß den Marktprozessen.

Das Ergebnis der vorgenannten Prüfung trägt der SMGW-Admin-N in das System-Log ein. Ist das Ergebnis negativ, dann prüft der SMGW-Admin-N den Sachverhalt. Bei negativem Ergebnis kann der Wechselprozess zunächst nicht zu Ende geführt werden.

Der SMGW-Admin-A wird darüber informiert, dass der Prozess gestoppt worden ist. Damit bleibt der SMGW-Admin-A als verantwortlicher SMGW-Admin konfiguriert. Der SMGW-Admin-A löscht auf dem SMGW die zu Beginn des gestoppten Prozesses eingebrachten Verbindungsdaten für den SMGW-Admin-N.

Das zugrundeliegende Problem und die Lösung werden dann vom SMGW-Admin-N ggf. mit dem SMGW-Admin-A und den beteiligten externen Marktteilnehmern geklärt. Nach Lösung des Problems setzt der Wechselprozess erneut damit ein, dass der SMWG-Admin-A die Verbindungsdaten für den SMGW-Admin-N an das SMGW sendet. Ggf. ist auch erforderlich, dass der SMGW-Admin-A erneut vom SMWG-Admin-N Zertifikate und Verbindungsdaten anfordert.

Resultiert die Ursache des Problems in der Marktkommunikation mit den externen Marktteilnehmern, wird der Prozess an dieser Stelle verlassen.

Ist die Verbindung zwischen SMGW und SMGW-Admin-N zustande gekommen und das Ergebnis der Prüfung der Konfiguration positiv, so unterbricht der SMGW-Admin-N die Verbindung zum

SMGW und sendet einen Wake-Up-Call an das SMGW. Dieses prüft den Wake-Up-Call und etabliert einen TLS-Kanal zum SMGW-Admin-N.

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

Der SMGW-Admin-N löscht den SMGW-Admin-A auf dem SMGW (gelöscht wird insbesondere das Kommunikationsprofil zum SMGW-Admin-A). Der SMGW-Admin-A hat danach keinen Zugriff mehr auf das SMGW.

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

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

Erst nachdem der SMGW-Admin-A die Mitteilung erhalten hat, dass der Wechsel erfolgreich vollzogen worden ist, und der SMGW-Admin-A nicht erneut die Rolle des SMGW-Admins übernehmen muss, werden die Zertifikate/Schlüssel des SMGW-Admin-A auf dem SMGW gelöscht.

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

7.4 Zeitpunkt

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

7.5 Verarbeitete Daten

Primärdaten

- Gateway-ID
- Zähler-ID
- Zuordnung der IDs zu den konkreten Letztverbrauchern

- Log-Einträge und weitere im SMGW gespeicherte Daten[26]

Sekundärdaten

- Logging-Daten

7.6 Ort, Art und Weise der Verarbeitung

Die Datenverarbeitung findet im SMGW, beim SMGW-Admin-A und beim SMGW-Admin-N statt. Die Datenübertragung erfolgt elektronisch über die unten angegebenen Schnittstellen.

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

7.7 Schnittstellen

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

- Schnittstelle zwischen SMGW-Admin-A und SMGW: IF_GW_WAN
- Schnittstelle zwischen SMGW-Admin-N und SMGW: IF_GW_WAN

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

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

7.8 Besondere (Sicherheits-)Anforderungen[27]

- Bezüglich der personenbezogenen Daten, insbesondere den aus dem SMGW ausgelesenen Messwerten und Log-Einträgen sind die datenschutzrechtlichen Regelungen zu beachten.
- Für die vom SMGW-Admin-A ausgelesenen Daten gilt grundsätzlich dieselbe Höchstspeicherdauer, 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	führt eine Gültigkeitsprüfung des SMGW-Admin-N-Zertifikats durch			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 Kommunikations-profil 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 erfolg-reichen 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		

1128 Tabelle 5: Prozessschritte Wechsel Smart Meter Gateway Admin