Bundesamt
für Sicherheit in der
Informationstechnik

TR-03109-6

Smart Meter Gateway Administration

Version 1.0, Datum 26.11.2015

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

Inhaltsverzeichnis

1 Einleitung

Angesichts knapper werdender Rohstoffe und der damit zunehmenden Bedeutung erneuerbarer Energien ist die Energieversorgung in Deutschland sowie in Europa insgesamt im Wandel. Ressourcen wie Sonne und Windkraft lassen sich nicht planen oder steuern wie Kohle- oder Kernkraftwerke. Darüber hinaus führt die zunehmende Zahl dezentraler Erzeuger, wie zum Beispiel Photovoltaik-Anlagen, zu schwer vorhersehbaren Schwankungen und erheblichen Herausforderungen für die Stabilität im Stromnetz. Basis der zukünftigen Energieversorgung ist ein intelligentes Netz, das Energieerzeugung und -verbrauch effizient verknüpft und ausbalanciert. Kernbausteine eines solchen Netzes sind intelligente Messsysteme, auch „Smart Metering Systems“ genannt.

Sie sollen für eine aktuelle Verbrauchstransparenz und eine sichere Übermittlung von Messdaten sorgen. Zudem steuern sie elektronische Verbrauchsgeräte und Erzeugungsanlagen so, dass ein besseres Last- und Einspeisemanagement im Verteilnetz ermöglicht wird.

Da es beim Aufbau und der Nutzung eines intelligenten Netzes nicht zuletzt auch um die Verarbeitung personenbezogener Daten geht, sind die Sicherheit und der Schutz eben jener eine zentrale Voraussetzung für die öffentliche Akzeptanz intelligenter Messsysteme. Somit sind eine verbindliche Vorgabe für alle zukünftigen Messsysteme und deren sicherer Betrieb in Deutschland nötig, um ein hohes, angemessenes Maß an Integrität, Vertraulichkeit und Verfügbarkeit im Rahmen der Interoperabilität zu gewährleisten.

Zentrale Komponente ist hier die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway - SMGW) mit integriertem Sicherheitsmodul (SecMod). Insbesondere für die Installation, Inbetriebnahme, den Betrieb, die Wartung und Konfiguration des SMGW ist der Smart Meter Gateway Administrator (SMGW Admin) verantwortlich.

Aus der Kritikalität der am SMGW Admin gebündelten Prozess- und Datenverantwortung ergibt sich ein besonderer Schutzbedarf. Daher muss sichergestellt sein, dass der IT-Betrieb beim SMGW Admin Mindestanforderungen zur Durchsetzung der Informationssicherheit genügt.

Das vorliegende Dokument stellt normative Mindestanforderungen an die Informationssicherheit eines SMGW Admin. Diese Mindestanforderungen sind jeweils durch ein Informationssicherheits-managementsystem (ISMS) des SMGW Admin nach den Regelungen dieses Dokuments zu behandeln und konkret auszugestalten. Die Prüfung der Ausgestaltung werden in einem Auditierungsschema geregelt.

Dieses Dokument (Teil 6) gehört zur Technischen Richtlinie [BSI TR-03109], die technische Vorgaben für intelligente Messsysteme und deren sicheren Betrieb umfasst.

1.1 Zielsetzung des Dokuments

Um bei allen Marktteilnehmern, die die Aufgaben des SMGW Admin selber wahrnehmen oder als Dienstleister für Dritte anbieten möchten, ein vergleichbares Maß an Informationssicherheit einzufordern, beschreibt das vorliegende Dokument Anforderungen und Maßnahmen für die Mindestsicherheit beim SMGW Admin.

Das vorliegende Dokument ersetzt die bisherige Anlage V zur [BSI TR-03109-1] in der Version 1.0 vom 18.03.2013.

1.2 Zielgruppe

Das Dokument richtet sich in erster Linie an Marktteilnehmer, die für ihren eigenen Bereich den Betrieb des SMGW Admin planen sowie an Dienstleistungsunternehmen, die den Betrieb des SMGW Admin als Dienstleistung für Dritte im Markt anbieten wollen.

1.3 Terminologie

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

- MUSS bedeutet, dass es sich um eine normative Anforderung handelt.
- DARF NICHT / DARF KEIN bezeichnet den normativen Ausschluss einer Eigenschaft.
- SOLL beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen müssen begründet werden.
- SOLL NICHT / SOLL KEIN kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen zu diesen Festlegungen müssen begründet werden.
- KANN / DARF bedeutet, dass die Eigenschaften fakultativ oder optional sind.

Die Kapitel der Technischen Richtlinie sind grundsätzlich als normativ anzusehen. Informative Kapitel werden explizit am Anfang gekennzeichnet.

1.4 Versionshistorie

Version	Datum	Beschreibung
1.0-rc	11.11.2015	Vorversion zur Veröffentlichung
1.0	26.11.2015	Veröffentlichung der Version 1.0

2 Aufbau des Dokuments

Informatives Kapitel

Beginnend mit Kapitel 3 beschreibt das vorliegende Dokument zunächst die Aufgaben und Anwendungsfälle des SMGW Admin. Diese leiten sich im wesentlichen aus dem Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG) – Entwurf und [BSI TR-03109-1] ab und werden hier in übersichtlicher Form zusammengefasst.

Das zentrale Kapitel 4 definiert die Sicherheitsanforderungen an den Betrieb des SMGW Admin im Sinne der Informationssicherheit. Bei der Umsetzung der hier definierten Anforderungen sind zwei Alternativen möglich: Zum Einen die Vorgehensweise und Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz [IT-GS] oder zum Anderen die Vorgehensweise nach [ISO27001].

Die erste Alternative ist hinreichend durch die Grundschutz-Vorgehensweise und die BSI-Standards beschrieben und wird seit vielen Jahren in der Praxis angewandt.

Für die zweite Alternative gibt es mit der Normenreihe [ISO27001] ebenfalls ausreichend Dokumentationen und Erfahrungswerte.

Unabhängig von der gewählten Vorgehensweise sind in jedem Fall die Mindestanforderungen aus Kapitel 4 zu berücksichtigen und im Rahmen der jeweiligen Sicherheitskonzeption zu betrachten.

Abschließend werden in Kapitel 5 Rahmenbedingungen für die Auditierung und Zertifizierung aufgezeigt, mit denen die hier konzipierten Maßnahmen nachweislich geprüft und zertifiziert werden können.

3 Anwendungsfälle des Smart Meter Gateway Admin

Informatives Kapitel

Zur Ausgestaltung der Sicherheitskonzeption des Smart Meter Gateway Admin werden in diesem Kapitel die aus anderen normativen Vorgaben (z.B. aus dem gesetzlichen Rahmen oder [BSI TR-03109-1]) resultierenden Anwendungsfälle des SMGW Admin beschrieben. Die Beschreibung erfolgt in einem für die Sicherheitskonzeption erforderlichen Umfang und Detailtiefe.

Die Anwendungsfälle werden in die fünf Kategorien Dienste, Administration & Konfiguration, Monitoring, Unterstützung der Messwertverarbeitung und Fehlerbehandlung unterteilt (s. Abbildung 1). Eine Übersicht über alle in diesem Dokument behandelten Anwendungsfälle und ihre Einordnung wird in Abbildung 2 dargestellt.

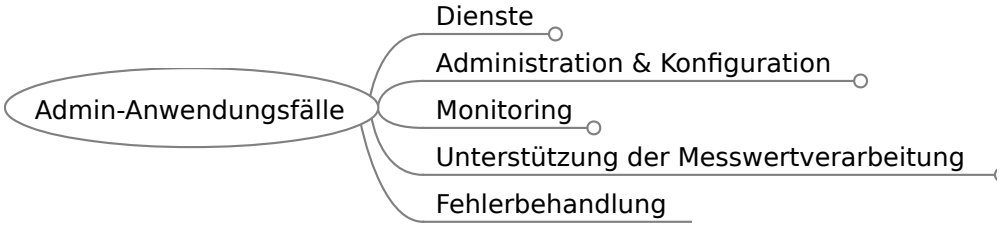

Abbildung 1: Aufteilung der SMGW Admin Anwendungsfälle

Die Anwendungsfälle selbst enthalten in ihrer Beschreibung die Verknüpfung zu den Dokumenten, aus denen der Anwendungsfall hervorgeht. Des Weiteren werden in den Anwendungsfällen die Beteiligten und die verwendeten Objekte [1]aufgelistet. Folgend werden die Rahmenbedingungen in Tabellenform dargestellt, die den Akteur, das auslösende Ereignis, die Voraussetzungen und die zu erwartenden Ergebnisse enthalten. In einer weiteren Tabelle wird der Kommunikationsablauf beschrieben.

Die im Folgenden beschriebenen Anwendungsfälle lassen sich unterteilen in

- Dienste, die als Service für die Kommunikationspartner des SMGW Admin zur Verfügung stehen (siehe Kapitel 3.2),
- in Administration und Konfiguration, bei denen der SMGW Admin aktiv Veränderungen am SMGW vornimmt (siehe Kapitel 3.3),
- des Weiteren in das Monitoring, mit dem der SMGW Admin das SMGW überwacht (siehe Kapitel 3.4),
- den Fall, bei dem der SMGW Admin bei der Messwertverarbeitung mitwirken muss (siehe Kapitel 3.5) und
- die Fehlerbehandlung (siehe Kapitel 3.6).

Als besonders wichtige übergreifende Aufgabe des SMGW Admin ist das Zertifikatsmanagement als Teil der Administration & Konfiguration zu sehen, welches u.a. eine Verwendung von geeignetem Schlüsselmaterial sowie Zertifikaten aus der SM-PKI erforderlich macht.

1 Folgende vier Objekt Typen werden in diesem Dokument unterschieden:
- Daten: Jede einzelne Information oder zusammengesetzte Information, die im Rahmen der Anwendungsfälle im SMGW oder im SMGW Admin-Betrieb verarbeitet wird (z.B. Profil, Letztverbraucher-ID, SMGW-ID, Schlüssel, Logeintrag)
- Dienst: Die in Informationstechnik realisierten Dienste im SMGW Admin-Betrieb.
- Anweisung: Ein Befehl / Kommando vom SMGW Admin an das SMGW zur Auslösung einer Aktion.
- Anbindung: Alle technischen Objekte (HW und SW) im Einflussbereich des SMGW Admin, die für eine "Verbindung" zum EMT notwendig sind (z.B. Router, sonstige Netzkomponenten)

Zukünftige Anwendungsfälle müssen in späteren Versionen des Dokuments ergänzt werden (z.B. Schalten und Steuern über die CLS-Schnittstelle).

Da für alle diese hier beschriebenen Anwendungsfälle eine bestehende Verbindung zwischen SMGW und SMGW Admin Voraussetzung ist, wird der Verbindungsaufbau einleitend in diesem Kapitel einmal beschrieben (Kapitel 3.1). Dieser Verbindungsaufbau ist immer dann vor einem Anwendungsfall seitens des SMGW Admin zu initiieren, wenn keine Verbindung zum SMGW besteht.

Im Folgenden wird von dem externen Marktteilnehmer (EMT) gemäß [BSI TR-03109-1] Kapitel 2.2 gesprochen. Es kann davon ausgegangen werden, dass es sich hierbei um einen EMT handelt, der einen Prozess durchlaufen hat, mit dem er sich dem SMGW Admin gegenüber eindeutig identifiziert hat und zusätzlich dem SMGW Admin zuverlässig mitgeteilt wurde, dass dieser EMT auch berechtigt ist. Diese Prozesse sind zum Teil in der Marktkommunikation zu regeln, wenn sie die Bereiche Strom und Gas betreffen, und sonst durch geeignete Vorgaben durch die zuständige Regulierungsbehörde zu definieren.

Ferner ist anzumerken, dass Teile der hier dargestellten Anwendungsfälle auch Kommunikationsanteile zwischen EMT und SMGW Admin beinhalten, die im Bereich der Marktkommunikation liegen und noch an anderer Stelle zu definieren sind.

Abbildung 2: Anwendungsfälle des SMGW Admin

3.1 Verbindungsaufbau

Kurze Beschreibung:

Das SMGW baut eine Verbindung zum SMGW Admin auf. Dabei werden die einzelnen Schritte des Verbindungsaufbaus betrachtet.

Lange Beschreibung:

Das SMGW kann nach [BSI TR-03109] aufgrund eines externen oder internen Ereignisses versuchen eine Verbindung zum SMGW Admin aufzubauen. Die Verbindung wird entsprechend eines, in das SMGW eingebrachten WAN-Kommunikationsprofils erstellt. Durch dieses WAN-Kommunikationsprofil wird auch das Kommunikationsszenario festgelegt, das bis zum Abbau der Verbindung gilt. Dabei bestimmt das Kommunikationsszenario die Rechte, mit denen der SMGW Admin auf das SMGW zugreifen darf. Zu den Ereignissen, die einen Verbindungsaufbau des SMGW zum SMGW Admin auslösen können, gehört z.B. das Wake-Up-Paket oder eine Zeitsynchronisation.

Gemäß [BSI TR-03109] gibt es vier Kommunikationsszenarien mit den Bezeichnungen

- MANAGEMENT,
- ADMIN-SERVICE,
- NTP-HTTPS und
- NTP-TLS,

die für die unterschiedlichen Aufgaben des SMGW Admin vorgesehen sind. Das fünfte Kommunikationsszenario INFO-REPORT dient alleine der direkten Kommunikation zwischen SMGW und EMT und wird hier nicht weiter betrachtet.

Beteiligte:

SMGW

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Profile	Daten	Kapitel 4.3.2.7 („Profile “)
SMGW Admin Logeintrag	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
SMGW Admin Log	Dienst	Kapitel 4.3.2.24 („Log des SMGW Admin“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)

Tabelle 1: Werthaltige Objekte beim Verbindungsaufbau

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW	Ein WAN-Kommunikationsprofil wurde durch ein Ereignis aktiviert bzw. ausgelöst.	- Das SMGW ist funktionsbereit. - Das SMGW verfügt über eine WAN-Verbindung. - Das SMGW besitzt gültige WAN-Kommunikationsprofile, um mit dem SMGW Admin eine Verbindung aufzubauen. - Das SMGW besitzt die benötigten Zertifikate.	Erfolg: Eine verschlüsselte Verbindung zwischen SMGW und SMGW Admin wurde aufgebaut.

Tabelle 2: Rahmenbedingungen beim Verbindungsaufbau

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Ereignis, das das SMGW eine Verbindung zum SMGW Admin aufbauen lässt.	Das SMGW baut eine Verbindung zum SMGW Admin unterhalb der TLS-Schicht auf.	SMGW	SMGW Admin	Identifikations- und Verbindungsinformationen.
2	TLS- Verbindungsanfrage eines SMGW	Das SMGW baut eine TLS-Verbindung zum SMGW Admin auf.	SMGW	SMGW Admin	TLS-Handshake

Tabelle 3: Kommunikationsablauf beim Verbindungsaufbau

3.2 Dienste

Die in diesem Kapitel beschriebenen Aufgaben werden durch Dienste des SMGW Admin abgedeckt. Sie ergeben sich aus den Anforderungen der WAN Anwendungsfällen aus [BSI TR-03109-1] Kapitel 3.2.2. Die Dienste werden in

- die Zeitsynchronisation (Kapitel 3.2.1),
- das Empfangen und Ausliefern von Messwerten (Kapitel 3.2.2),
- den Empfang von SMGW Alarmierungen und Benachrichtigungen (Kapitel 3.2.3),
- die Kommunikation zwischen EMT und CLS (Kapitel 3.2.4) und
- den Dienst für das Firmware-Download (Kapitel 3.2.5) unterteilt.

3.2.1 Zeitsynchronisation

Der SMGW Admin hat für alle SMGW in seinem Verantwortungsbereich mindestens einen Zeitserver zur Verfügung zu stellen, mit dem sich die Uhr jedes SMGW synchronisieren kann. Dieser Abschnitt beschäftigt sich mit der Zeitsynchronisation zwischen dem Zeitserver des SMGW Admin und dem Zeitserver der PTB

sowie zwischen SMGW Admin und SMGW. Die Zeitsynchronisation zwischen SMGW Admin und dem Zeitserver der PTB erfolgt gemäß den Vorgaben der PTB. Die Synchronisation zwischen SMGW Admin und SMGW wird durch [BSI TR-03109-1] definiert, sodass hier auf den genauen Protokollablauf nicht näher eingegangen werden muss.

3.2.1.1 Zeitsynchronisation mit PTB

Kurze Beschreibung:

Die Zeitserver des SMGW Admin synchronisieren sich mit dem Zeitserver der PTB.

Lange Beschreibung:

Die Zeitserver des SMGW Admin müssen mit den Zeitservern der PTB synchronisiert werden, um eine möglichst geringe Abweichung zur gesetzlichen Zeit vorweisen zu können. Die genauen Grenzen sind in [BSI TR-03109-1] Kapitel 3.2.6 definiert.

Beteiligte:

PTB

SMGW Admin

Zeitserver des SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Gesetzliche Zeit	Daten	Kapitel 4.3.2.1 („Gesetzliche Zeit“)
Zeitserver des SMGW Admin	Dienst	Kapitel 4.3.2.26 („Zeitserver SMGW Admin“)
PTB Anbindung	Anbindung	Kapitel 4.3.2.27 („PTB Anbindung“)

Tabelle 4: Werthaltige Objekte bei der Zeitsynchronisation mit der PTB

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Zyklischer / bzw. termingesteuerter oder manueller Anstoß der Zeitsynchronisation	Eine sichere Verbindung zum PTB Zeitserver existiert	Erfolg: Der Zeitserver des SMGW Admin wird synchronisiert.

Tabelle 5: Rahmenbedingungen bei der Zeitsynchronisation mit der PTB

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Zeitserver beim SMGW Admin muss eine Zeitsynchronisation durchführen.	Zeitserver SMGW Admin kontaktiert einen der Zeitserver bei PTB und führt eine Zeitsynchronisation durch.	Zeitserver bei SMGW Admin	PTB Zeitserver	Protokoll- und Zeitinformationen

Tabelle 6: Kommunikationsablauf bei der Zeitsynchronisation mit der PTB

3.2.1.2 Zeitsynchronisation mit SMGW

Kurze Beschreibung:

Durchführung einer Zeitsynchronisation des SMGW mit dem Zeitserver des SMGW Admin.

Lange Beschreibung:

Das SMGW benötigt für die Messwertverarbeitung eine gültige Zeit. Diese Zeit stellt die interne Uhr zur Verfügung. Eine Zeit ist dann gültig, wenn die Abweichung der Zeit gegenüber den Zeitservern des SMGW Admin nicht außerhalb der Toleranz gemäß PTB liegt. Um die Gültigkeit der Zeit des SMGW zu gewährleisten, muss das SMGW sich regelmäßig mit den Zeitservern des SMGW Admin, gemäß den Vorgaben in [BSI TR-03109-1] Kapitel 3.2.6, synchronisieren.

Beteiligte:

SMGW

SMGW Admin

Zeitserver / Zeitsynchronisation-Webservice des SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Gesetzliche Zeit	Daten	Kapitel 4.3.2.1 („Gesetzliche Zeit“)
Zeitserver des SMGW Admin	Dienst	Kapitel 4.3.2.26 („Zeitserver SMGW Admin“)
Zeitsynchronisation-Webservice des SMGW Admin	Dienst	Kapitel 4.3.2.28 („Zeitsynchronisation-Webservice des SMGW Admin“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)

Tabelle 7: Werthaltige Objekte bei der Zeitsynchronisation mit dem SMGW

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW	Regelmäßige Zeitsynchronisation	- WAN-Verbindung (siehe Kapitel 3.1) - Konfiguration für regelmäßige Synchronisation	Erfolg: Die Zeit des SMGW wurde mit dem Zeitserver des SMGW Admin synchronisiert.
SMGW Admin	Der SMGW Admin fordert, dass das SMGW sich mit dem Zeitserver / Zeitsynchronisation-Webservice synchronisiert.	WAN-Verbindung (siehe Kapitel 3.1)	

Tabelle 8: Rahmenbedingungen bei der Zeitsynchronisation mit dem SMGW

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	SMGW muss eine Zeitsynchronisation durchführen.	SMGW kontaktiert einen der Zeitserver / Zeitsynchronisation-Webservices des SMGW Admin und führt eine Zeitsynchronisation durch.	SMGW	SMGW Admin-Zeitserver	NTP Nutzinformationen nach [RFC5905]

Tabelle 9: Kommunikationsablauf bei der Zeitsynchronisation mit dem SMGW

3.2.2 Empfangen und Ausliefern von Messwerten

Das SMGW sendet die verarbeiteten Messwerte im Allgemeinen direkt an den berechtigten EMT. Für den Fall, dass das SMGW die verarbeiteten Messwerte zum SMGW Admin sendet, leitet dieser die Messwerte an den berechtigten EMT weiter (ähnlich der Funktion eines Proxyservers). Handelt es sich allerdings um pseudonymisierte Netzzustandsdaten, so müssen diese über den SMGW Admin verteilt werden, da dieser die äußere Signatur des SMGW entfernen muss. Die zugehörigen Anwendungsfälle werden im Kapitel 3.5 behandelt.

3.2.3 Empfang von SMGW Alarmierungen und Benachrichtigungen

Kurze Beschreibung:

Das SMGW kann Alarmierungen und Benachrichtigungen an den SMGW Admin senden. Diese müssen von einem Dienst beim SMGW Admin empfangen werden.

Lange Beschreibung:

Beim WAF3 (siehe [BSI TR-03109-1] Kapitel 3.2.2) ist beschrieben, dass ein SMGW im Fall von unerwarteten Ereignissen oder Fehlersituationen Alarmierungen an den SMGW Admin senden muss. Der SMGW Admin muss deshalb einen Dienst betreiben, der diese Alarmierungen empfängt und verarbeitet.

Beteiligte:

SMGW

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Nachricht von Typ Alarm	Daten	Kapitel 4.3.2.2 („SMGW Nachricht vom Typ Alarm“)
Nachricht von Typ Benachrichtigung	Daten	Kapitel 4.3.2.3 („SMGW Nachricht vom Typ Benachrichtigung“)
SMGW Admin Logeintrag	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
Nachrichten Empfangsservice des SMGW Admin	Dienst	Kapitel 4.3.2.30(„Nachrichten Empfangsservice des SMGW Admin“)
SMGW Admin-Log	Dienst	Kapitel 4.3.2.24 („Log des SMGW Admin“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)

Tabelle 10: Werthaltige Objekte beim Empfang von SMGW Alarmierungen und Benachrichtigungen

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW	Das SMGW sendet dem SMGW Admin eine Nachricht.	Eine gesicherte WAN-Verbindung (siehe Kapitel 3.1) zum SMGW Admin wurde etabliert.	Erfolg: - Handelt es sich bei der Nachricht um einen Alarm, so ist ein Eintrag ins Log des SMGW Admin vorzunehmen. - SMGW Admin verarbeitet die Nachricht.

Tabelle 11: Rahmenbedingungen beim Empfang von SMGW Alarmierungen und Benachrichtigungen

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	TLS Verbindung erfolgreich	SMGW sendet die Nachricht.	SMGW	SMGW Admin	Alarmierung oder Benachrichtigung
2	Nachricht wurde gesendet.	SMGW Admin bestätigt den Empfang.	SMGW Admin	SMGW	Empfangsbestätigung

Tabelle 12: Kommunikationsablauf beim Empfang von SMGW Alarmierungen und Benachrichtigungen

3.2.4 Kommunikation zwischen EMT und CLS

Kurze Beschreibung:

Der EMT nutzt den SMGW Admin, um eine Verbindung zwischen einem an das SMGW angeschlossenen CLS und dem EMT herzustellen (siehe [BSI TR-03109-1] Kapitel 3.4.3.4, HKS4).

Lange Beschreibung:

Wenn das CLS oder das SMGW nicht selbstständig eine Verbindung zwischen CLS und EMT aufbaut, kann der berechtigte EMT den Dienst des SMGW Admin in Anspruch nehmen. Dieser sendet ein Wake-Up Paket (siehe [BSI TR-03109-1] Kapitel 3.2.5) nach Überprüfung der Berechtigung des EMT an das SMGW und veranlasst dieses zu einem Verbindungsaufbau zwischen CLS und EMT (d.h. die TLS-Kanäle vom CLS zum SMGW und vom SMGW zum EMT sind etabliert). Hierzu wird auf im SMGW hinterlegte Kommunikationsprofile (siehe [BSI TR-03109-1] Kapitel 4.4) zurückgegriffen.

Beteiligte:

SMGW

SMGW Admin

EMT

CLS

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
CLS Identifikation (ID)	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Kommunikationsstatus SMGW Admin ↔ SMGW	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Bestätigung des SMGW	Daten	Kapitel 4.3.2.33 („Bestätigung oder Fehlermeldung eines SMGW“)
Wake-Up-Paket	Anweisung	Kapitel 4.3.2.12 („Wake-Up-Paket“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
EMT Anbindung	Anbindung	Kapitel 4.3.2.31(„EMT Anbindung“)

Tabelle 13: Werthaltige Objekte bei der Kommunikation zwischen EMT und CLS

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
EMT	Verbindungswunsch eines EMT mit einem CLS	- EMT besitzt die notwendigen Berechtigungen für zugeordnete CLS und ist dem SMGW Admin bekannt. - Die Kommunikationsprofile für EMT und das zugeordnete CLS sind im SMGW hinterlegt und gültig. - Zum EMT und CLS Gerät kann das SMGW eine TLS gesicherte Verbindung herstellen.	Erfolg: Die sichere Nachrichtenüber-mittlung zwischen EMT und CLS über den Proxy Dienst des SMGW ist möglich.

Tabelle 14: Rahmenbedingungen bei der Kommunikation zwischen EMT und CLS

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Es ist erforderlich, das CLS zu kontaktieren.	Der EMT kontaktiert ggf. den SMGW Admin und fordert ihn auf, eine Verbindung zwischen CLS und dem EMT herzustellen.	EMT	SMGW Admin	CLS ID
2	Erhalt einer Anforderung von einem EMT	Wenn der EMT berechtigt ist auf das CLS zuzugreifen, wird ein Wake-Up Paket an das SMGW (siehe 3.3.4) gesendet.	SMGW Admin	SMGW	siehe 3.3.4
3	Wake-Up Paket ist gültig.	Aufbau einer WAN-Verbindung gemäß 3.1	SMGW	SMGW Admin	
4	SMGW hat die Verbindung zum SMGW Admin erfolgreich aufgebaut.	Aktivieren des Proxy-Kommunikationsprofils für das entsprechende CLS.	SMGW Admin	SMGW	
5	Empfang des Befehls	Bestätigung	SMGW	SMGW Admin	Bestätigung

Tabelle 15: Kommunikationsablauf bei der Kommunikation zwischen EMT und CLS

3.2.5 Firmware-Download

Kurze Beschreibung:

Im Rahmen des WAF2 (siehe [BSI TR-03109-1] Kapitel 3.2.2) hat das SMGW die Möglichkeit Firmware-Updates über einen Dienst des SMGW Admin zu beziehen.

Lange Beschreibung:

Das SMGW muss einen Dienst beim SMGW Admin nutzen, um neue Firmware zu laden. Dieser Dienst darf nur vom SMGW Admin zur Verfügung gestellt werden. Die auf diesem Dienst befindlichen Firmware-Updates sind vom SMGW Admin vor Bereitstellung zu überprüfen (siehe Kapitel 3.3.1). Wenn der SMGW Admin das Firmware-Update über seinen Dienst bereitstellt, kann ein SMGW auf Befehl des SMGW Admin auf diesen Dienst zugreifen und das Firmware-Update laden.

Beteiligte:

SMGW

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Information über aktuelle Version Firmware auf einem SMGW	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
SMGW Firmware Update	Daten	Kapitel 4.3.2.5 („SMGW Firmware Update“)
Bestätigung des vollständigen Empfangs	Daten	Kapitel 4.3.2.33 („Bestätigung oder Fehlermeldung eines SMGW“)
SMGW Admin Update Dienst	Dienst	Kapitel 4.3.2.34 („SMGW Admin Update Dienst“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
Anweisung an SMGW zur Aktivierung Firmware-Update	Anweisung	Kapitel 4.3.2.6 („Anweisung an SMGW zur Aktivierung eines Firmware-Update„)

Tabelle 16: Werthaltige Objekte beim Firmware-Download

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW	Im SMGW wurde durch den SMGW Admin ein Updatevorgang initiiert.	WAN-Verbindung gemäß 3.1 .	Erfolg: SMGW bestätigt erfolgreichen Download der Firmware.

Tabelle 17: Rahmenbedingungen beim Firmware-Download

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Verbindungsaufbau erfolgreich.	SMGW fordert ein Firmware-Update vom SMGW Admin Update Dienst an.	SMGW	SMGW Admin Update Dienst	Zu ladende Firmware-Update Bezeichnung
2	Anforderung	Das SMGW lädt das Firmware-Update vom Dienst des SMGW Admin.	SMGW Admin Update Dienst	SMGW	Firmware-Update
3	Firmware-Update wurde empfangen.	Bestätigung des vollständigen Empfangs	SMGW	SMGW Admin Update Dienst	Bestätigung

Tabelle 18: Kommunikationsablauf beim Firmware-Download

3.3 Administration und Konfiguration

Hier werden die Anwendungsfälle behandelt, mit denen der SMGW Admin in die Konfiguration des SMGW eingreift und verändert (siehe [BSI TR-03109-1] Kapitel 3.2.2 WAF1). Dies beinhaltet das Einbringen und

Editieren von verschiedenen Konfigurationsprofilen. Ebenfalls werden Anwendungsfälle betrachtet, die eng mit diesen verknüpft sind. Zu diesen Anwendungsfällen gehört die Aktualisierung der Firmware des SMGW.

3.3.1 Bereitstellung von Firmware-Updates

Kurze Beschreibung:

Der SMGW Admin erhält ein Firmware-Update für das SMGW vom Hersteller des SMGW, prüft dieses und stellt es zum Download bereit.

Lange Beschreibung:

Der SMGW Admin ist die verantwortliche Instanz, die ein vom SMGWHersteller zur Verfügung gestelltes Firmware-Update für das SMGW vorbereitet (d.h. prüft und zum Download bereitstellt). Hierfür muss er das ihm zur Verfügung gestellte Firmware-Update auf Version, Vollständigkeit, Authentizität und Integrität überprüfen. Ebenfalls muss, außer in begründeten und mit dem BSI abgestimmten Ausnahmefällen, eine Zertifizierung für das zur Verfügung gestellte Firmware-Update nach [BSI CC-PP-0073]/[BSI TR-03109] vorhanden sein. Sollte die Überprüfung nicht erfolgreich ausfallen, muss der SMGW Admin eine klärende Abstimmung mit dem SMGW Hersteller herbeiführen.
Nach der erfolgreichen Überprüfung des Firmware-Updates muss der SMGW Admin das Firmware-Update für das SMGW gemäß Kapitel 3.2.5 („Firmware-Download“) zum Download bereitstellen .

Anmerkung:

Der genaue Ablauf/Prozess zur Einreichung, Prüfung, Zertifizierung, Behandlung von Ausnahmefällen, Behandlung eines sicherheitsrelevanten Firmware-Updates und Freigabe einer neuen Firmware-Version ist noch unter Beachtung der Rahmenbedingungen aus dem Mess- und Eichgesetz (MessEG) und der Mess- und Eichverordnung (MessEV) in [BSI TR-03109-1] zu definieren.

Beteiligte:

SMGW Hersteller

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Firmware Update	Daten	Kapitel 4.3.2.5 („SMGW Firmware Update“)
Zertifikat des SMGW Herstellers	Daten	Kapitel 4.3.2.9 („Zertifikate“)
SMGW Admin Logeintrag	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
SMGW Admin-Log	Dienst	Kapitel 4.3.2.24 („Log des SMGW Admin“)
SMGW Hersteller Anbindung	Anbindung	Kapitel 4.3.2.38 („SMGW Hersteller Anbindung“)

Tabelle 19: Werthaltige Objekte bei der Bereitstellung von Firmware-Updates

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Hersteller	Es steht ein neues Firmware-Update zu Verfügung.	- Verbindung zum SMGW Admin - SMGW Admin besitzt das von der der SM-PKI ausgestellte Zertifikat des SMGW Herstellers.	Erfolg: SMGW Admin bestätigt den Empfang des Firmware-Updates und protokolliert das Ereignis im SMGW Admin-Log.

Tabelle 20: Rahmenbedingungen bei der Bereitstellung von Firmware-Updates

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	SMGW Hersteller stellt ein neues Firmware-Update zur Verfügung.	Firmware-Update wird dem SMGW Admin vom SMGW Hersteller übermittelt.	SMGW Hersteller	SMGW Admin	Signiertes Firmware-Update des SMGW Herstellers
2	Firmware-Update wurde empfangen.	SMGW Admin prüft das Firmware-Update auf Authentizität und Integrität. Abhängig vom Ergebnis sendet er eine Antwort.	SMGW Admin	SMGW Hersteller	Empfangsbestätigung und ggf. Fehlermeldung.

Tabelle 21: Kommunikationsablauf bei der Bereitstellung von Firmware-Updates

3.3.2 Profilverwaltung

Kurze Beschreibung:

Verwaltung der Konfigurationsprofile im SMGW. Das Verwalten von Profilen beinhaltet das Einfügen[2], Löschen oder Lesen der Profile.

Lange Beschreibung:

Das SMGW wird über Konfigurationsprofile (Zählerprofile, Auswertungsprofile, (Proxy-) Kommunikationsprofile) konfiguriert. Mithilfe dieser Profile kann der SMGW Admin die Anbindung externer Geräte wie Zähler oder CLS konfigurieren, ebenso Erfassung, Verarbeitung und Versand von Messwerten sowie die gesamte Kommunikation des SMGW.

Die Profile bzw. die dafür notwendigen Daten werden dem SMGW Admin über die Marktkommunikation von den beteiligten EMT bereitgestellt. Die Prozeduren, mit denen die Profile verwaltet werden können, sind zu großen Teilen identisch und werden daher in einem Anwendungsfall zusammengefasst. Die Unterschiede, die sich hauptsächlich in den ausgetauschten Daten wiederfinden, werden einzeln unter den entsprechenden Punkten aufgeführt.

2 Gemäß der Technischen Richtlinien werden Änderungen an einem bereits hinterlegten Profil durch erneutes Einfügen des Profils mit geänderten Detailangaben implizit ermöglicht.

Zählerprofile: Diese enthalten die Konfiguration für das SMGW, um mit einem Zähler zu kommunizieren. Die Zählerprofile sind in [BSI TR-03109-1] Kapitel 4.4.2 beschrieben und beinhalten neben dem verwendeten Protokoll, dem Kommunikationsszenario, den OBIS-Kennzahlen und der Geräte-ID des Zählers auch das für die Kommunikation mit dem Zähler notwendige Schlüsselmaterial. Zählerprofile werden über die Geräte-IDs der Zähler in Auswertungsprofilen referenziert.

WAN-Kommunikationsprofile: In einem Kommunikationsprofil werden die Parameter hinterlegt, die für eine Kommunikation über die WAN-Schnittstelle notwendig sind. Die Beschreibung des Profils und die darin enthaltenen Parameter befinden sich in [BSI TR-03109-1] Kapitel 4.4.4.

Proxy-Kommunikationsprofile: Das Proxy-Kommunikationsprofil wird in [BSI TR-03109-1] Kapitel 3.4.6.3 beschrieben und behandelt die Kommunikation zwischen CLS und EMT.

Auswertungsprofile: Die Konfiguration sämtlicher Teilaspekte der Messwerterfassung und -verarbeitung werden durch den SMGW Admin über Auswertungsprofile konfiguriert, welche die Parameter für die verschiedenen Anwendungsfälle aus [BSI TR-03109-1] Kapitel 4.2 festlegen.

HAN-Kommunikationsprofile: In dem Kommunikationsprofil für die HAN Schnittstelle werden die Parameter für die Kommunikation des SMGW zum Letztverbraucher oder Servicetechniker festgelegt (vgl. [BSI TR-03109-1] Kapitel 3.4.6.2).

Beteiligte:

SMGW

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Konfigurationsprofile (Proxy Kommunikationsprofil, Auswertungsprofil, HAN Kommunikationsprofil, Zählerprofil, WAN Kommunikationsprofil)	Daten	Kapitel 4.3.2.7 („Profile “)
Profil ID	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Bestätigung des SMGW	Daten	Kapitel 4.3.2.33 („Bestätigung oder Fehlermeldung eines SMGW“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)

Tabelle 22: Werthaltige Objekte bei der Profilverwaltung

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Der SMGW Admin benötigt Zugriff auf ein Konfigurationsprofil im SMGW.	WAN-Verbindung (siehe 3.1) zum SMGW vorhanden.	Erfolg: Einfügen, Editieren, Löschen oder Lesen des Profils.

Tabelle 23: Rahmenbedingungen bei der Profilverwaltung

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1a	Zugriff auf ein Profil ist erforderlich.	- Einfügen eines Konfigurationsprofils - das SMGW protokolliert den Zugriff	SMGW Admin	SMGW	Konfigurationsprofil
1b		- Löschen[3] eines Profils - das SMGW protokolliert den Zugriff			Profil-ID
1c		- Lesen eines Konfigurationsprofils			Profil-ID
2	Befehl des SMGW Admin	Das SMGW führt die vom SMGW Admin gewünschte Aktion durch.	SMGW	SMGW Admin	- Bestätigung - beim lesenden Zugriff zusätzlich das Profil

Tabelle 24: Kommunikationsablauf bei der Profilverwaltung

3.3.3 Schlüssel-/Zertifikatsmanagement

Kurze Beschreibung:

Das Schlüssel- und Zertifikatsmanagement liegt im Aufgabenbereich des SMGW Admin. Hierzu gehört insbesondere die Aktualisierung von Schlüsseln in den Profilen der SMGW als auch der sichere Umgang mit nicht öffentlichen Schlüsseln. Ebenfalls fällt das Beantragen von neuen Zertifikaten bei der zuständigen Sub-CA für die SMGW in diesen Aufgabenbereich des SMGW Admin.

Es sind die [BSI TR-03109-3], [BSI TR-03109-4] und die Certificate Policy [CP]der SM-PKI zu beachten.

Lange Beschreibung:

Die Schlüssel und Zertifikate, die von dem SMGW verwendet werden, sind im Sicherheitsmodul oder im SMGW gespeichert. Das SMGW selbst kann keine Schlüssel oder Zertifikate mit der PKI austauschen. Es ist in [BSI TR-03109] nicht vorgesehen, dass das SMGW eine selbstständige Verantwortung für die in ihm gespeicherten Schlüssel übernimmt.

Der SMGW Admin ist für sämtliche Schlüssel, die im SMGW gespeichert sind, zuständig. Es ist die Pflicht des SMGW Admin, Zertifikate und Schlüssel rechtzeitig vor Ablaufen der Gültigkeit zu ersetzten. Handelt es sich beim Schlüssel oder beim Zertifikat um die des SMGW für die WAN-Schnittstelle (GW_WAN_TLS_PUB/CRT, GW_WAN_SIG_PUB/CRT, GW_WAN_ENC_PUB/CRT), so muss der SMGW Admin vor Ablauf der Gültigkeit eine Verbindung zum SMGW aufbauen und das SMGW veranlassen, einen Zertifikatsrequest zu generieren. Diesen Zertifikatsrequest schickt der SMGW Admin an die Sub-CA und lädt den von der Sub-CA verarbeiteten Request zurück auf das SMGW.

Ferner ist der SMGW Admin für das Vorhalten, das regelmäßige Abholen und die Umsetzung / Nutzung von aktuellen Sperrlisten aus der SM-PKI verantwortlich (vgl. hierzu [BSI TR-03109-4]).

3 Wenn es Verknüpfungen gibt, die auf das Zählerprofil verweisen, so muss das SMGW die Löschung ablehnen.

Läuft die Gültigkeit von Schlüsseln oder Zertifikaten von EMT, Zählern oder CLS ab, so sind die entsprechenden Kommunikationsprofile gemäß den Anwendungsfällen der Profilverwaltung mit den neuen Schlüsseln oder Zertifikaten zu aktualisieren.

Beteiligte:

SMGW

SMGW Admin

Sub-CA

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Zertifikat	Daten	Kapitel 4.3.2.9 („Zertifikate“)
Schlüssel	Daten	Kapitel 4.3.2.8 („Private Schlüssel des SMGW Admin“)
Sperrliste	Daten	Kapitel 4.3.2.39 („Sperrliste„)
Anweisung an SMGW zur Generierung eines Zertifikats-requests	Anweisung	Kapitel 4.3.2.11(„Anweisung an SMGW zur Generierung eines Zertifikatsrequest„)
Zertifikatsrequest des SMGW	Daten	Kapitel 4.3.2.10 („Zertifikatsrequest“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
Sub-CA Anbindung	Anbindung	Kapitel 4.3.2.35 (Anbindung zur Sub-CA„)

Tabelle 25: Werthaltige Objekte beim Schlüssel-/Zertifikatsmanagement

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Schlüssel/Zertifikat eines SMGW läuft aus	- WAN-Verbindung (siehe 3.1) zum SMGW vorhanden - gesicherte Verbindung zur zuständigen Sub-CA vorhanden	Erfolg: Schlüssel und Zertifikat wurden aktualisiert.

Tabelle 26: Rahmenbedingungen beim Schlüssel-/Zertifikatsmanagement

Anmerkung:

Der Kommunikationsablauf ist noch nicht festgelegt und wird später ergänzt.

3.3.4 Senden eines Wake-Up Paketes

Kurze Beschreibung:

Das Senden eines Wake-Up Paketes an das SMGW ermöglicht dem SMGW Admin eine Verbindung mit dem SMGW herzustellen. Dieses Wake-Up Paket muss der SMGW Admin individuell für das SMGW erzeugen.

Lange Beschreibung:

Der SMGW Admin erstellt ein Wake-Up Paket und sendet es dem SMGW. Das SMGW überprüft das Wake-Up Paket entsprechend den Vorgaben der [BSI TR-03109-1] Kapitel 3.2.5. Ist das Paket gültig, so baut das SMGW entsprechend des WAN-Kommunikationsprofils eine Verbindung zum SMGW Admin auf. Ist das Paket ungültig, so erfolgt keine Reaktion des SMGW.

Beteiligte:

SMGW

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Profile	Daten	Kapitel 4.3.2.7 („Profile “)
Logeintrag im SMGW Admin Log	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
Log des SMGW Admin	Dienst	Kapitel 4.3.2.24 („Log des SMGW Admin“)
Wake-Up-Paket	Anweisung	Kapitel 4.3.2.12 („Wake-Up-Paket“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)

Tabelle 27: Werthaltige Objekte beim Senden eines Wake-Up Paketes

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Der SMGW Admin benötigt eine Verbindung zum SMGW.	Zum Wake-Up Paket konfigurierte Kommunikationsmöglichkeit ins WAN muss vorhanden sein.	Erfolg: Das SMGW nimmt Kontakt zum SMGW Admin auf.

Tabelle 28: Rahmenbedingungen beim Senden eines Wake-Up Paketes

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Verbindungs-wunsch zum SMGW	Der SMGW Admin erstellt ein Wake-Up Paket und sendet es dem SMGW.	SMGW Admin	SMGW	Wake-Up Paket (siehe [BSI TR-03109-1] Anhang A)
2a	SMGW erhält Wake-Up Paket	Ist das Wake-Up Paket gültig, stellt das SMGW eine Verbindung zum SMGW Admin her	SMGW	SMGW Admin	
2b		- Ist das Wake-Up Paket ungültig, folgt keine Reaktion des SMGW. - Protokollierung des Time Outs im SMGW Admin-Log			

Tabelle 29: Kommunikationsablauf beim Senden eines Wake-Up Paketes

3.3.5 Löschen von Teilen des Letztverbraucher Logs

Kurze Beschreibung:

Das SMGW löscht Teile des Letztverbraucher-Logs nach Ablauf der Speicherfrist. Die Speicherfrist kann durch den SMGW Admin auf Anforderung durch den Letztverbraucher angepasst werden.

Lange Beschreibung:

Im [BSI TR-03109-1] Kapitel 5.3.2 ist definiert, wie lange Einträge im Letztverbraucher-Log mindestens vorgehalten werden müssen. Das [BSI CC-PP-0073] Kapitel 6.2.1 legt fest, dass der Letztverbraucher bestimmen kann, nach welchem Zeitraum die Einträge im Letztverbraucher-Log gelöscht werden müssen. Diese Speicherfrist kann durch den Letztverbraucher geändert werden, wobei hier ggf. gesetzlich vorgegebene Speicherfristen zu berücksichtigen sind.

Nach Ablauf der Speicherfrist erfolgt das Löschen der betreffenden Einträge im Letztverbraucher-Log durch das SMGW. Einträge in anderen Logs auf dem SMGW dürfen hierdurch nicht verändert oder gelöscht werden.

Beteiligte:

EMT

Letztverbraucher

SMGW

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Letztverbraucher-ID	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Speicherfrist vom Letztverbraucher	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Logeintrag im SMGW Admin Log	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
Anweisung an SMGW über Speicherfrist	Anweisung	Kapitel 4.3.2.13 („Anweisung an SMGW zum Setzen der Speicherfrist für das Letztverbraucher-Log„)
Log des SMGW Admin	Dienst	Kapitel 4.3.2.24 („Log des SMGW Admin“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
EMT Anbindung	Anbindung	Kapitel 4.3.2.31 („EMT Anbindung“)

Tabelle 30: Werthaltige Objekte beim Löschen von Teilen des Letztverbraucher Logs

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Der SMGW Admin hat die Speicherfrist vom Letztverbraucher (über den EMT) erhalten, während der die Einträge im Letztverbraucher-Log gespeichert werden sollen.	Es besteht eine (siehe 3.1) WAN-Verbindung zum SMGW.	Erfolg: - Eintrag in das SMGW Admin-Log. - Einträge im Letztverbraucher-Log des SMGW werden nicht länger als die angegebene Frist gespeichert.

Tabelle 31: Rahmenbedingungen beim Löschen von Teilen des Letztverbraucher Logs

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Auftrag durch Letztverbraucher an EMT	Der SMGW Admin trägt einen Zeitraum im SMGW ein, für den die Daten im Letztverbraucher-Log gespeichert werden.	SMGW Admin	SMGW	- Letztverbraucher-ID - Frist
2	Befehl des SMGW Admin	Das SMGW bestätigt den Erhalt und die Umsetzung der Aufgabe.	SMGW	SMGW Admin	Bestätigung

Tabelle 32: Kommunikationsablauf beim Löschen von Teilen des Letztverbraucher Logs

Anmerkung:

Diese Aufgabe muss, nach Konfiguration durch den SMGW Admin, das SMGW übernehmen, da der SMGW Admin selbst keine lesenden oder schreibenden Zugriffsrechte auf das Letztverbraucher-Log besitzt. Zu beachten ist, dass eine solche Konfiguration für den Letztverbraucher nachvollziehbar sein muss. Im Rahmen der Weiterentwicklung der [BSI TR-03109-1] wird dieser Anwendungsfall ergänzt und spezifiziert.

3.3.6 Bereitstellung der initialen Konfigurationsdatei

Kurze Beschreibung:

Für die Phase „Vor-Personalisierung 2“ des SMGW benötigt der Integrator vom SMGW Admin eine initiale Konfigurationsdatei mit Kommunikationsparametern des SMGW Admin und Zertifikaten mit zugehöriger Zertifikatskette (aus der SM-PKI).

Lange Beschreibung:

Der Phase der „Vor-Personalisierung 2“ ist in [BSI TR-03109-1] Anlage VI ausführlich beschrieben.

Beteiligte:

Integrator

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Initiale Konfigurationsdatei	Daten	Kapitel 4.3.2.14 („Initiale Konfigurationsdatei“)

Tabelle 33: Werthaltige Objekte bei der Bereitstellung der initialen Konfigurationsdatei

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Der Integrator benötigt die initiale Konfigurationsdatei.	Kommunikationsweg, bei dem die Integrität, Vertraulichkeit und Authentizität der Daten gewährleistet ist.	Erfolg: Der Integrator erhält die initiale Konfigurationsdatei.

Tabelle 34: Rahmenbedingungen bei der Bereitstellung der initialen Konfigurationsdatei

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	SMGW Admin stellt die initiale Konfigurationsdatei zur Verfügung.	Die initiale Konfigurationsdatei wird dem Integrator vom SMGW Admin übermittelt.	SMGW Admin	Integrator	Initiale Konfigurationsdatei
2	Initiale Konfigurationsdatei wurde empfangen.	Integrator prüft die initiale Konfigurationsdatei auf Authentizität und Integrität. Abhängig vom Ergebnis sendet er eine Antwort.	Integrator	SMGW Admin	Empfangsbestätigung und ggf. Fehlermeldung.

Tabelle 35: Kommunikationsablauf bei der Bereitstellung der initialen Konfigurationsdatei

3.4 Monitoring

Das Monitoring umfasst die Möglichkeiten des SMGW Admin das SMGW mit den in [BSI TR-03109] vorgegebenen Mitteln zu überwachen. Dieses Monitoring stützt sich hauptsächlich auf das Lesen und Auswerten der Nachrichten und Logs des SMGW.

3.4.1 Auswerten der SMGW Nachrichten

Kurze Beschreibung:

Auswerten der Nachrichten, die das SMGW an den SMGW Admin sendet.

Lange Beschreibung:

Das SMGW kann Nachrichten an den in Kapitel 3.2.3 beschriebenen Dienst des SMGW Admin senden. Bei den dort empfangenen Nachrichten kann es sich um Status-, Fehler- und Alarmmeldungen handeln. Die

hier beschriebene Aufgabe behandelt die Möglichkeit des SMGW Admin, diese Nachrichten zu lesen und auszuwerten.

Beteiligte:

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Status-Meldung eines SMGW	Daten	Kapitel 4.3.2.3 („SMGW Nachricht vom Typ Benachrichtigung“)
Fehler-Meldung eines SMGW	Daten	Kapitel 4.3.2.3 („SMGW Nachricht vom Typ Benachrichtigung“)
Alarm-Meldung eines SMGW	Daten	Kapitel 4.3.2.2 („SMGW Nachricht vom Typ Alarm“)

Tabelle 36: Werthaltige Objekte beim Auswerten der SMGW Nachrichten

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Neuer Log-Eintrag / Alarm wird gemeldet	Das SMGW hat eine Nachricht an den SMGW Admin gesendet (siehe Kapitel 3.2.3).	Der SMGW Admin hat auf die Log-Einträge/ Alarme reagiert und geeignete Aktionen ausgelöst

Tabelle 37: Rahmenbedingungen beim Auswerten der SMGW Nachrichten

Anmerkung:

In [BSI TR-03109] werden keine Angaben gemacht, wie diese Nachrichten zu verarbeiten sind. Der SMGW Admin hat die Nachrichten gemäß interner individueller Betriebsprozesse so zu verwenden, dass die Funktionalität und der sichere Betrieb des SMGW sichergestellt werden kann. Insofern kann ein Kommunikationsablauf nicht skizziert werden.

3.4.2 Lesen und Speichern der SMGW-Logs

Kurze Beschreibung:

Der SMGW Admin kann das eichtechnische Log und das System-Log des SMGW lesen und speichern.

Lange Beschreibung:

Der SMGW Admin hat lesenden Zugriff auf das System-Log und das eichtechnische Log des SMGW. Im Rahmen seiner Aufgaben muss er diese Logs lesen und auswerten. Dazu gibt der SMGW Admin dem SMGW die Anweisung zur Übermittlung der vom SMGW signierten Logdaten und empfängt die vom SMGW gesendeten SMGW-Logs. Sofern die SMGW-Logs vom SMGW Admin gespeichert werden, muss die Integrität der Logdaten mittels Signatur des SMGW prüfbar sein.

Das eichtechnische Log ist auf Verlangen einer Eichbehörde dieser zur Verfügung zu stellen. Damit unterstützt der SMGW Admin die Eichbehörden bei der Erfüllung ihrer gesetzlichen Aufgaben (z.B. im

Rahmen einer Befundprüfung) gemäß Mess- und Eichgesetz (MessEG) und der Mess- und Eichverordnung (MessEV).

Beteiligte:

SMGW

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Logeintrag System-Log	Daten	Kapitel 4.3.2.15 („Logeintrag System-Log“)
Logeintrag eichtechn. Log	Daten	Kapitel 4.3.2.16 („Logeintrag eichtechn. Log“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
Anweisung an SMGW zur Übermittlung von Logdaten	Anweisung	Kapitel 4.3.2.20 („Anweisung an SMGW zur Übermittlung von Logdaten“)

Tabelle 38: Werthaltige Objekte beim Lesen und Speichern der SMGW-Logs

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Der SMGW Admin benötigt Zugriff auf das System- bzw. eichtechn. Log im SMGW.	Eine WAN-Verbindung (siehe 3.1) zum SMGW ist aufgebaut.	Erfolg: Der SMGW Admin erhält die gewünschten Teile der SMGW-Logs.

Tabelle 39: Rahmenbedingungen beim Lesen und Speichern der SMGW-Logs

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	SMGW Admin wünscht Zugriff auf die SMGW-Logs.	Der SMGW Admin sendet dem SMGW die Anweisung und die benötigten Informationen für den Zugriff auf die Log(abschnitte).	SMGW Admin	SMGW	Zugriffs-informationen
2	Anfrage SMGW Admin	Das SMGW sendet die verlangten Daten.	SMGW	SMGW Admin	Log-Daten

Tabelle 40: Kommunikationsablauf beim Lesen und Speichern der SMGW-Logs

Anmerkung:

Es kann sinnvoll sein, dass die Logs oder Teile davon über den SMGW Admin auch anderen Berechtigten zweckgebunden zur Verfügung gestellt werden (z.B. könnte das System-Log für den SMGW Hersteller zur Fehlerdiagnose wichtig sein). Weitere Fälle, in denen ein berechtigtes Interesse der Kenntnis der SMGW-Logs nachgewiesen wurde, können später ergänzt werden.

3.4.3 Selbsttest des SMGW anstoßen

Kurze Beschreibung:

Der SMGW Admin stößt den Selbsttest des SMGW an.

Lange Beschreibung:

Im Rahmen des Monitorings und der Entstörung hat der SMGW Admin die Möglichkeit, das SMGW anzuweisen, einen Selbsttest durchzuführen. Dieser Selbsttest ist in [BSI TR-03109] noch nicht genauer beschrieben. Ein erster Ansatz ist in der [PTB-A 50.8] zu finden.

Beteiligte:

SMGW

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Ergebnisdaten eines SMGW Selbsttests	Daten	Kapitel 4.3.2.19 („Ergebnisdaten eines SMGW Selbsttests“)
Anweisung an SMGW zur Durchführung eines Selbsttests	Anweisung	Kapitel 4.3.2.18 („Anweisung an SMGW zur Durchführung eines Selbsttests“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)

Tabelle 41: Werthaltige Objekte beim Selbsttest des SMGW anstoßen

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	SMGW Admin fordert das SMGW zum Selbsttest auf.	WAN-Verbindung (siehe 3.1) zum SMGW	Erfolg: Der SMGW Admin erhält die Ergebnisdaten des Selbsttests.

Tabelle 42: Rahmenbedingungen beim Selbsttest des SMGW anstoßen

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Der SMGW Admin benötigt einen Selbsttest des SMGW	Der SMGW Admin sendet dem SMGW den Befehl, einen Selbsttest durchzuführen.	SMGW Admin	SMGW	Befehl: Selbsttest
2	Empfang des Befehls zum Durchführen des Selbsttests.	Das SMGW führt den Selbsttest erfolgreich durch und schickt das Ergebnis dem SMGW Admin.	SMGW	SMGW Admin	Ergebnisdaten

Tabelle 43: Kommunikationsablauf beim Selbsttest des SMGW anstoßen

Anmerkung:

Da die Tarifierung im SMGW eine elementare Funktion ist, wird sie ebenfalls Teil des Selbsttests sein. Somit muss ebenfalls angenommen werden, dass bei entsprechenden Fehlern im Selbsttest Daten aus diesem Bereich im Rahmen der Fehlermeldung dem SMGW Admin zur Verfügung gestellt werden.

Der Selbsttest ist in [BSI TR-03109-1] bisher nicht genau beschrieben, sodass der Anwendungsfall noch zusätzliche Schritte enthalten kann, die hier zur Zeit nicht aufgeführt sind (z.B. eine Bestätigung des SMGW, dass der Selbsttest gestartet wird).

3.4.4 Führen eines SMGW Admin-Logs

Kurze Beschreibung:

Der SMGW Admin muss seine Aktionen in einem von ihm geführten SMGW Admin-Log aufzeichnen.

Lange Beschreibung:

Die hier genannte Aufgabe, ein eigenes Log beim SMGW Admin zu führen, wurde bisher nicht durch [BSI TR-03109] gefordert, sondern vielmehr als grundsätzliche „Admin-Aufgabe“ verstanden. Aus diesem Grund wird sie hier aufgeführt.

Für viele Operationen muss der SMGW Admin die getätigten Aktionen in einem eigenen SMGW Admin-Log protokollieren. In Kombination mit den Logs des SMGW ermöglicht dies die Handlungen des SMGW Admin am SMGW nachzuvollziehen, insbesondere wenn eine Kommunikation zwischen SMGW und SMGW Admin fehlschlägt.

Beteiligte:

SMGW Admin

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
SMGW Admin Logeintrag	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
Log des SMGW Admin	Dienst	Kapitel 4.3.2.24 („Log des SMGW Admin“)

Tabelle 44: Werthaltige Objekte beim Führen eines SMGW Admin-Logs

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Ein für die Protokollierung im SMGW Admin-Log relevantes Ereignis ist eingetreten.	keine	Erfolg: Eintrag ins SMGW Admin-Log

Tabelle 45: Rahmenbedingungen beim Führen eines SMGW Admin-Logs

3.5 Unterstützung der Messwertverarbeitung

Die Anwendungsfälle, die der SMGW Admin im Rahmen der Unterstützung der Messwertverarbeitung übernehmen muss, sind in diesem Kapitel zusammengefasst. Hierzu zählen die regelmäßige Weiterleitung von Messwerten (tarifierte Messwerte, Zählerstandsgänge, Netzzustandsdaten, Ist-Einspeiseleistung) an berechtigte EMT, der Abruf von Messwerten im Bedarfsfall und das Auslösen eines Tarifstufenwechsels.

3.5.1 Tarifierte Messwerte

Kurze Beschreibung:

Das SMGW erstellt, verschlüsselt und signiert die tarifierten Messwerte und versendet diese anschließend zu einem im TAF festgelegten Zeitpunkt an den berechtigten EMT. Dies kann entweder direkt durch das SMGW geschehen oder indirekt durch den SMGW Admin angefordert werden.

Lange Beschreibung:

Die Tarifierung wird über das Auswertungsprofil konfiguriert, dieses verweist auf ein WAN-Kommunikationsprofil. Der in diesem WAN-Kommunikationsprofil angegebene Empfänger für die tarifierten Daten ist ein berechtigter EMT. Die tarifierten Daten können direkt zu dem berechtigten EMT oder über den SMGW Admin an den berechtigten EMT versendet werden. Für diesen Fall muss der SMGW Admin einen Service bieten, der die Daten vom SMGW empfängt und an den berechtigten EMT weiterleitet. Die tarifierten Messwerte werden vom SMGW verschlüsselt sowie signiert und können nur vom berechtigten EMT gelesen werden. Dieser Anwendungsfall betrifft den SMGW Admin nur, wenn er das Versenden der Daten übernehmen muss. Somit wird auch nur dieser Fall betrachtet.

Die Tarifierung im SMGW wird in [BSI TR-03109-1] Kapitel 4.2.2 behandelt.

Beteiligte:

SMGW

SMGW Admin

EMT

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Verschlüsselte und signierte Messwerte	Daten	Kapitel 4.3.2.21 („Verschlüsselte und signierte Messwerte“)
SMGW Admin Logeintrag	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
Empfangsbestätigung	Daten	Kapitel 4.3.2.33 („Bestätigung oder Fehlermeldung eines SMGW“)
Dienst zum Empfang und Ausliefern von Messwerten	Dienst	Kapitel 4.3.2.25 („Dienst zum Empfang und Ausliefern von Messwerten“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
EMT Anbindung	Anbindung	Kapitel 4.3.2.31 („EMT Anbindung“)

Tabelle 46: Werthaltige Objekte bei den tarifierten Messwerten

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW	Das in dem TAF angegebene Ereignis tritt ein.	WAN-Verbindung (siehe 3.1) besteht.	Erfolg: - Übertragung der Daten an den SMGW Admin - dort Eintrag in das SMGW Admin-Log.

Tabelle 47: Rahmenbedingungen bei den tarifierten Messwerten

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Ereignisgesteuertes Ausliefern der Messwerte.	Das SMGW verschlüsselt und signiert die tarifierten Messwerte.	SMGW	SMGW Admin	Tarifierte Messwerte, verschlüsselt und signiert (siehe [BSI TR-03109-1] Kapitel 5.1.2).
2	Empfang der tarifierten Messwerte	Bestätigung des Empfangs	SMGW Admin	SMGW	Empfangsbestätigung
3	Empfang der tarifierten Messwerte	Versenden der tarifierten Messwerte an den berechtigten EMT	SMGW Admin	EMT	Tarifierte Messwerte, verschlüsselt und signiert.

Tabelle 48: Kommunikationsablauf bei den tarifierten Messwerten

3.5.2 Netzzustandsdaten

Kurze Beschreibung:

Die vom SMGW erhobenen Netzzustandsdaten werden vom SMGW Admin empfangen und an berechtigte EMT weitergeleitet.

Lange Beschreibung:

Im Gegensatz zu den tarifierten Messwerten müssen pseudonymisierte Netzzustandsdaten zuerst an den SMGW Admin gesendet werden. Auch wenn die Netzzustandsdaten durch das SMGW pseudonymisiert wurden, so sind diese weiterhin vom SMGW zunächst für den Empfänger verschlüsselt und signiert. Der Empfänger kann anhand der Signatur das SMGW identifizieren. Der SMGW Admin muss daher die äußere Signatur des SMGW entfernen (siehe [BSI TR-03109-1] Kapitel 3.2.4.3). Die noch verschlüsselten Netzzustandsdaten werden dann an berechtigte EMT weitergeleitet. Die [BSI TR-03109-1] erlaubt, wenn eine berechtigte Begründung vorliegt, den Versand von nicht pseudonymisierten Netzzustandsdaten.

Die Verarbeitung von Netzzustandsdaten im SMGW wird in [BSI TR-03109-1] Kapitel 4.2.4 behandelt.

Beteiligte:

SMGW

SMGW Admin

EMT

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Pseudonymisierte Netzzustandsdaten	Daten	Kapitel 4.3.2.22 („Pseudonymisierte Netzzustandsdaten“)
SMGW Admin Logeintrag	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
Empfangsbestätigung vom SMGW Admin	Daten	Kapitel 4.3.2.33 („Bestätigung oder Fehlermeldung eines SMGW“)
Dienst zum Empfang und Ausliefern von Messwerten	Dienst	Kapitel 4.3.2.25 („Dienst zum Empfang und Ausliefern von Messwerten“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
EMT Anbindung	Anbindung	Kapitel 4.3.2.31 („EMT Anbindung“)

Tabelle 49: Werthaltige Objekte bei den Netzzustandsdaten

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW	Das im TAF angegebene Ereignis ist eingetroffen.	Eine WAN-Verbindung (siehe 3.1) besteht.	Erfolg: - Übertragung der Daten - Eintrag in das Log des SMGW Admin.

Tabelle 50: Rahmenbedingungen bei den Netzzustandsdaten

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Das im TAF angegebene Ereignis ist eingetroffen.	Das SMGW pseudonymisiert, verschlüsselt und signiert die Netzzustandsdaten.	SMGW	SMGW Admin	Pseudonymisierte Netzzustandsdaten, verschlüsselt und signiert (siehe [BSI TR-03109-1] Kapitel 5.1.2).
2	Erhalt der Messwerte	Bestätigung des Empfangs	SMGW Admin	SMGW	Empfangsbestätigung
3	Erhalt der Messwerte	- Der SMGW Admin entfernt die äußere Signatur des SMGW - Die Netzzustandsdaten werden dem berechtigten EMT weitergeleitet.	SMGW Admin	EMT	Pseudonymisierte Netzzustandsdaten, verschlüsselt.

Tabelle 51: Kommunikationsablauf bei den Netzzustandsdaten

3.5.3 Wechsel der Tarifstufen

Kurze Beschreibung:

Gemäß [BSI TR-03109-1] Kapitel 4.2.2.5 kann neben anderen Möglichkeiten der SMGW Admin für den TAF5 eine Nachricht an das SMGW senden, um einen Tarifstufen-Wechsel herbeizuführen.

Lange Beschreibung:

Die [BSI TR-03109-1] ermöglicht unterschiedliche Anwendungsfälle für die Tarifierung und Bilanzierung der gemessenen Werte. Der in [BSI TR-03109-1] Kapitel 4.2.2.5 beschriebene Fall TAF5 ermöglicht einen Wechsel zwischen Tarifstufen innerhalb eines Tarifes. Der SMGW Admin hat im Rahmen dieses Tarifs die Möglichkeit die Liste der Tarifwechselzeitpunkte zu ändern, mit der das SMGW tarifiert.

Beteiligte:

SMGW

SMGW Admin

EMT

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Notwendige Parameter für das Regelwerk	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Anweisung an SMGW zum Wechsel der Tarifstufe	Daten	Kapitel 4.3.2.23 („Anweisung an SMGW zur Unterstützung der Messwertverarbeitung“)
SMGW Admin Logeintrag	Daten	Kapitel 4.3.2.17 („SMGW Admin Logeintrag“)
Bestätigung vom SMGW	Daten	Kapitel 4.3.2.33 („Bestätigung oder Fehlermeldung eines SMGW“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
EMT Anbindung	Anbindung	Kapitel 4.3.2.31 („EMT Anbindung“)

Tabelle 52: Werthaltige Objekte beim Wechsel der Tarifstufen

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
SMGW Admin	Tarifstufe muss gewechselt werden.	WAN-Verbindung (siehe 3.1) zum SMGW	Erfolg: - Tarifstufe ist gewechselt - Eintrag ins SMGW Admin-Log

Tabelle 53: Rahmenbedingungen beim Wechsel der Tarifstufen

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Ein vorher definiertes Ereignis tritt ein, das einen Tarifstufen-wechsel auslöst.	EMT sendet Auftrag und Informationen zum Wechsel der Tarifstufe	EMT	SMGW Admin	- Neue Tarifstufe - Ereignis, das den Wechsel ausgelöst hat.
2	Mitteilung des EMT, dass die Tarifstufe gewechselt werden muss.	SMGW Admin sendet dem SMGW den Befehl zum Wechsel der Tarifstufe.	SMGW Admin	SMGW	- Notwendige Parameter für das Regelwerk - Ereignis, das den Wechsel ausgelöst hat.
3	Befehl zum Wechsel der Tarifstufe	Das SMGW wechselt erfolgreich die Tarifstufe.	SMGW	SMGW Admin	Bestätigung

Tabelle 54: Kommunikationsablauf beim Wechsel der Tarifstufen

3.5.4 Abruf von Messwerten im Bedarfsfall

Kurze Beschreibung:

Dieser Fall beschreibt die Umsetzung des TAF6 aus [BSI TR-03109-1] Kapitel 4.2.2.6.

Lange Beschreibung:

Der TAF6 dient zum Abruf von Messwerten im Bedarfsfall. Dieser Anwendungsfall ist immer in einem SMGW aktiv und kann in begründeten Ausnahmefällen vom SMGW Admin genutzt werden, um rückwirkend Ablesungen zu einem bestimmten Stichtag vorzunehmen. Bei den Messwerten handelt es sich um tagesaktuelle Zählerstände und Stände der abgeleiteten Register, die das SMGW für die letzten 6 Wochen vorzuhalten hat. Ein in [BSI TR-03109-1] vorgesehener Bedarfsfall ist beispielsweise der Wechsel des SMGW oder ein Wechsel des Letztverbrauchers.

Beteiligte:

SMGW

SMGW Admin

EMT

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Betriebsinformationen (Zählpunkt-ID, Zähler-ID)	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Anweisung an SMGW zum Auslösen des entsprechenden Auswertungsprofils	Daten	Kapitel 4.3.2.23 („Anweisung an SMGW zur Unterstützung der Messwertverarbeitung“)
Verschlüsselte und signierte Messwerte	Daten	Kapitel 4.3.2.21 („Verschlüsselte und signierte Messwerte“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
EMT Anbindung	Anbindung	Kapitel 4.3.2.31 („EMT Anbindung“)

Tabelle 55: Werthaltige Objekte beim Abruf von Messwerten im Bedarfsfall

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
EMT	Die Messwerte müssen abgerufen werden.	- WAN-Verbindung (siehe 3.1) zwischen SMGW Admin und SMGW steht zur Verfügung. - Verbindung zwischen EMT und SMGW Admin steht zur Verfügung.	Erfolg: Der EMT erhält die Messwerte.

Tabelle 56: Rahmenbedingungen beim Abruf von Messwerten im Bedarfsfall

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Bedarfsfall tritt ein.	Der EMT kontaktiert den SMGW Admin, um einen Abruf von Messwerten im Bedarfsfall durchzuführen.	EMT	SMGW Admin	Zählpunkt-ID Zähler-ID
2	Der SMGW Admin hat die benötigten Daten vom EMT erhalten.	Der SMGW Admin löst das entsprechende Auswertungsprofil zum Abruf der Messwerte im Bedarfsfall aus.	SMGW Admin	SMGW	Befehl: Auswertungsprofil ausführen.
3	Auswertungsprofil wurde ausgelöst.	Das SMGW erstellt die Liste der verschlüsselten Messwerte und versendet sie an den SMGW Admin.	SMGW	SMGW Admin	Messwerte, verschlüsselt und signiert.
4	SMGW Admin erhält die verschlüsselten Messwerte.	Der SMGW Admin leitet die verschlüsselten Messwerte an den/die berechtigten EMT weiter.	SMGW Admin	EMT	

Tabelle 57: Kommunikationsablauf beim Abruf von Messwerten im Bedarfsfall

3.5.5 Auslesen der Ist-Einspeiseleistung

Kurze Beschreibung:

Dieser Fall beschreibt die Umsetzung des TAF9 aus [BSI TR-03109-1] Kapitel 4.2.3.1.

Lange Beschreibung:

Der TAF9 dient zum Auslesen der aktuellen Ist-Einspeiseleistung einer Erzeugungsanlage im Rahmen einer aktuell durchgeführten Einspeisemanagementmaßnahme, um die Messwerte einem berechtigten externen Marktteilnehmer zur Verfügung zu stellen.

Beteiligte:

SMGW

SMGW Admin

EMT

Werthaltige Objekte (Assets):

Objekt Bezeichnung	Objekt Typ	Normative Mindestvorgaben zu den Schutzzielen
Zählpunkt-ID	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Zähler-ID	Daten	Kapitel 4.3.2.4 („Betriebsinformationen zu einem SMGW“)
Anweisung an SMGW zum Auslesen der Ist-Einspeiseleistung	Daten	Kapitel 4.3.2.23 („Anweisung an SMGW zur Unterstützung der Messwertverarbeitung“)
Verschlüsselte Ist-Einspeiseleistung	Daten	Kapitel 4.3.2.21 („Verschlüsselte und signierte Messwerte“)
WAN Anbindung	Anbindung	Kapitel 4.3.2.29 („WAN Anbindung“)
EMT Anbindung	Anbindung	Kapitel 4.3.2.31 („EMT Anbindung“)

Tabelle 58: Werthaltige Objekte beim Auslesen der Ist-Einspeiseleistung

In der nachfolgenden Tabelle werden die Rahmenbedingungen für diesen Anwendungsfall beschrieben:

Akteur	Auslösendes Ereignis	Voraussetzung	Ergebnis
EMT	Die Ist-Einspeiseleistung muss abgerufen werden.	- WAN-Verbindung (siehe 3.1) zwischen SMGW Admin und SMGW steht zur Verfügung. - Verbindung zwischen EMT und SMGW Admin steht zur Verfügung.	Erfolg: Der EMT erhält die Ist-Einspeiseleistung.

Tabelle 59: Rahmenbedingungen beim Auslesen der Ist-Einspeiseleistung

Kommunikationsablauf:

Nr.	Auslösendes Ereignis	Beschreibung des Prozesses	Sender	Empfänger	Ausgetauschte Informationen
1	Bedarfsfall tritt ein.	Der EMT kontaktiert den SMGW Admin, um das Auslesen der Ist-Einspeiseleistung durchzuführen.	EMT	SMGW Admin	Zählpunkt-ID Zähler-ID
2	Der SMGW Admin hat die benötigten Daten vom EMT erhalten.	Der SMGW Admin löst das entsprechende Auswertungsprofil zum Auslesen der Ist-Einspeise-leistung aus.	SMGW Admin	SMGW	- Auswertungsprofil - Befehl: Auswertungsprofil ausführen.
3a	Auswertungsprofil wurde ausgelöst.	Das SMGW erstellt die verschlüsselte Ist-Einspeiseleistung und versendet sie an den/die laut WAN-Kommunikationsprofil berechtigten Marktteilnehmer oder den SMGW Admin.	SMGW	EMT	Ist-Einspeiseleistung
3b				SMGW Admin	
4b	SMGW Admin erhält die verschlüsselte Ist-Einspeiseleistung.	Der SMGW Admin leitet die verschlüsselte Ist-Einspeiseleistung an den/die berechtigten EMT weiter.	SMGW Admin	EMT	

Tabelle 60: Kommunikationsablauf beim Auslesen der Ist-Einspeiseleistung

3.6 Fehlerbehandlung

Tritt bei der Verarbeitung eines Befehls durch das SMGW ein Fehler auf, so sendet dieses im Allgemeinen eine Fehlermeldung an den SMGW Admin. Bei allen Fehlern, die dem SMGW Admin bekannt werden, erfolgt ein Eintrag in das SMGW Admin-Log.

Ebenso erfolgt ein Eintrag in das SMGW Admin-Log, wenn nach Kontaktaufnahme des SMGW Admin mit einem SMGW innerhalb der vorgesehenen Zeit keine Reaktion erfolgt.

Liegt bei einem Fehler eine Störung im SMGW vor, so führt der SMGW Admin im Bedarfsfall geeignete Entstörungsmaßnahmen durch.

4 Sicherheitsanforderungen an den Admin-Betrieb

Der folgende Text hat informativen Charakter, während alle nachfolgenden Unterkapitel normative Inhalte aufweisen.

Gemäß dem gesetzlichen Rahmen übernimmt der verantwortliche Messstellenbetreiber, oder ein in dessen Auftrag handelnder Dritter, die Funktion des Smart Meter Gateway Administrator (SMGW Admin).

In Kapitel 3 („Anwendungsfälle des Smart Meter Gateway Admin") dieses Dokumentes sind Anwendungsfälle beschrieben, die für den Geschäftsbetrieb eines SMGW Admin unabdingbar sind und jeweils schutzbedürftige Informationen beziehen, generieren, transportieren, speichern und verarbeiten. Dem Schutzbedarf dieser Informationen sowie der Anwendungsfälle selbst kann nur nachhaltig entsprochen werden, wenn sie nachhaltig in die konkretisierte Sicherheitskonzeption und Sicherheitsarchitektur des spezifischen SMGW Admin eingebettet und eingebunden wird.

Daher werden in diesem Dokument zu gewährleistende Mindestanforderungen in der Sicherheitskonzeption vorgegeben, deren konkretisierende Ausgestaltung jeweils spezifisch für einen SMGW Admin erfolgen muss.

Als Zielstellung wird durch ein Informationssicherheitsmanagementsystem[4] (ISMS) des konkreten SMGW Admin eine vollständige Sicherheitskonzeption erwartet, die die Mindestvorgaben aus diesem Dokument in der einsatzspezifischen Umgebung ausgestaltet und mittels wirksamer Maßnahmen potentiellen Bedrohungen und Risiken entgegenwirkt.

Die nachfolgenden Unterkapitel behandeln:

- Kapitel 4.1 („Informationssicherheitsmanagementsystem") stellt normativ Vorgaben an das ISMS und regelt insbesondere die Behandlung nachfolgender Kapitel.
- Kapitel 4.2 („Schutzziele") definiert die im ISMS mindestens zu behandelnden Schutzziele.
- Kapitel 4.3 („Mindestvorgaben zu den Schutzzielen") listet informationstechnische Objekte der in Kapitel 3 beschriebenen Anwendungsfälle, die einen schutzbedürftigen Wert aufweisen. Für jedes Objekt (Asset) werden Mindestvorgaben zum Schutzbedarf definiert.

  Die Reihenfolge der aufgeführten Assets orientiert sich an den in Kapitel 3 beschriebenen Anwendungsfällen.
- Kapitel 4.4 („Bedrohungen") gibt ein Mindestmaß an zu behandelnden Bedrohungen vor.
- Kapitel 4.5 („Mindest-Maßnahmen„) bestimmt Mindestvorgaben an die im ISMS zu bildenden Maßnahmen.

Die folgende Abbildung zeigt eine Übersicht der in diesen Kapitel beschriebenen Sicherheitsanforderungen:

4 ISMS nach ISO 27001 auf Basis von IT-Grundschutz oder nach ISO/IEC 27001

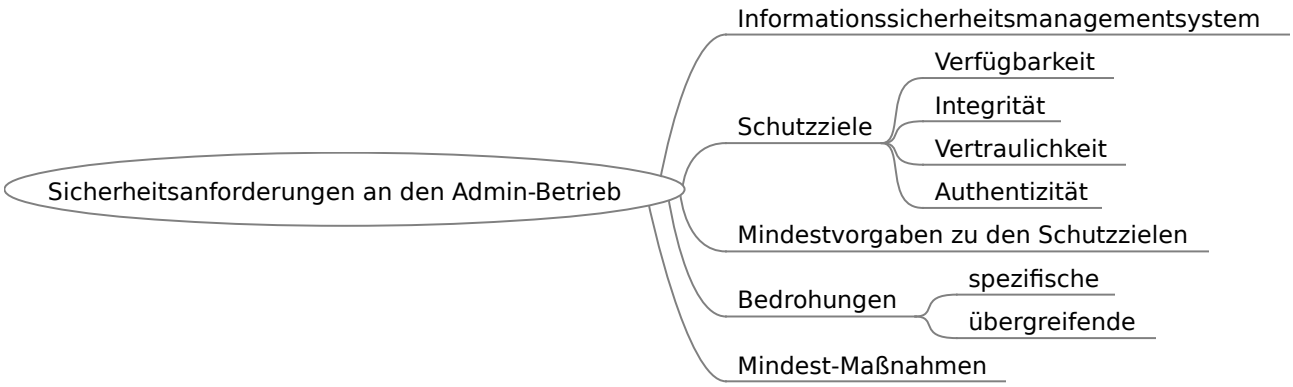

Abbildung 3: Übersicht der Sicherheitsanforderungen

4.1 Informationssicherheitsmanagementsystem

Ein verantwortlicher SMGW Admin MUSS ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 oder nach IT-Grundschutz gemäß BSI-Standard [100-2] planen, etablieren, nach Kapitel 5 („Auditierung und Zertifizierung“) zertifizieren lassen und nachhaltig betreiben.

Der Anwendungsbereich des ISMS MUSS sämtliche Betriebstätigkeiten des SMGW Admin abdecken, unabhängig von einer expliziten Erwähnung in Kapitel 3 („Anwendungsfälle des Smart Meter Gateway Admin“) und unabhängig von einer Auslagerung (Outsourcing) oder Teilauslagerung. Das ISMS MUSS die in diesem Kapitel 4 beschriebenen Schutzziele, Assets, die identifizierten Bedrohungen und resultierenden Maßnahmen als Mindestvorgaben behandeln und SMGW Admin spezifisch konkretisierend und vollständig ausgestalten.

Die Ausgestaltung MUSS im Risikomanagement, neben dem eigenen wirtschaftlichen Risiko, mögliche Risiken beinhalten, die aufgrund der Nichtbeachtung von Anforderungen Dritter entstehen können.

Ein ISMS Risikomanagement DARF NICHT Risiken akzeptieren, die sich aus der Nichtbeachtung von Mindestvorgaben aus diesem Dokument ergeben können. Demgegenüber DARF ein nach Maßnahmenauswahl verbleibendes und nachvollziehbar begründetes Restrisiko akzeptiert werden. Der verantwortliche SMGW Admin MUSS die Umsetzung und Einhaltung festgelegter Maßnahmen gewährleisten. Die Verantwortung bleibt von einer Auslagerung (Outsourcing) oder Teilauslagerung des SMGW Admin-Betriebs oder abgesetzten Arbeitsplätzen unberührt.

Das ISMS des SMGW Admin MUSS derart dokumentiert werden, dass zur Auditierung mindestens eine Prüfung der individuellen Rahmenbedingungen, Anzahl der SMGW, betrachteter Aspekte, Entscheidungen und resultierenden Maßnahmen möglich ist.

4.2 Schutzziele

Im ISMS des SMGW Admin MÜSSEN mindestens die nachfolgend aufgeführten Schutzziele behandelt werden.

- Verfügbarkeit (englisch: „availability“) von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
- Vertraulichkeit (englisch: „confidentiality“) ist der Schutz vor unbefugter Preisgabe von Informationen.

- Integrität (englisch: „integrity“) bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von IT-Systemen.
- Authentizität (englisch: „authenticity“) bezeichnet eine nachweisbare Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit.

Das ISMS MUSS weitere individuell geeignete Schutzziele prüfen und den Prüfvorgang, als auch das Prüfergebnis dokumentieren.

4.3 Mindestvorgaben zu den Schutzzielen

In der Beschreibung nach Anwendungsfällen (siehe Kapitel 3 „Anwendungsfälle des Smart Meter Gateway Admin“) wurden alle werthaltigen Objekte (Assets) eines SMGW Admin, die sich aus der Technischen Richtlinie ergeben, benannt.

Das ISMS des SMGW Admin MUSS die nachfolgend aufgeführten Assets mit den angegebenen Mindestvorgaben behandeln. Eine Mindestvorgabe DARF NICHT unterschritten werden. Das ISMS MUSS im Einzelfall eventuell geltende normative Vorgaben (z.B. der PTB, der BNetzA, des BSI, des Gesetzgebers) geeignet berücksichtigen.

Das ISMS MUSS die Assets in der konkreten Ausgestaltung um sämtliche werthaltigen individuellen Assets ergänzen bzw. vorhandene Assets angemessen erweitern.

Sollte das ISMS des SMGW Admin die IT-Grundschutz Methodik anwenden, MUSS mindestens ein Schutzbedarf von „hoch“ bei allen Zielobjekten angesetzt werden, die sich aus den aufgeführten Assets als auch aus individuellen Assets ergeben. Hieraus ergibt sich für alle diese Zielobjekte die Notwendigkeit einer erweiterten Sicherheitsanalyse sowie ggf. einer Risikoanalyse.

Interpretationshilfe zu den Mindestvorgaben:

- „Initiale Konfigurationsdatei“ (Kapitel 4.3.2.14):
  Aus den normativen Regelungen der [BSI TR-03109-1] als auch der Beschreibung des Anwendungsfalls „Bereitstellung der initialen Konfigurationsdatei“ (Kapitel 3.3.6) ergibt sich, dass dem Integrator die initiale Konfigurationsdatei übermittelt wird. Demgegenüber wird die Mindestanforderung zum Schutzbedarf im Schutzziel Vertraulichkeit als „Die Kenntnis um den Inhalt der initialen Konfigurationsdatei MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein“ vorgegeben. Diese normative Mindestvorgabe darf grundsätzlich nicht unterschritten werden, jedoch ist im Fall einer notwendigen Bereitstellung an den zuständigen Integrator die Übermittlung zulässig.
- „Betriebsinformationen zu einem SMGW“ (Kapitel 4.3.2.4):
  In diesem Kapitel wurden u.A. „Notwendige Parameter für das Regelwerk“ der Tarifstufen als Bestandteil der Betriebsinformationen zu einem SMGW genannt und die Mindestanforderungen zum Schutzbedarf im Schutzziel als „Die Kenntnis um den Dateninhalt sowie dessen Existenz in konkreter inhaltlicher Ausprägung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.“ definiert. Obwohl der auftraggebende EMT eine Tarifstufe festlegt und damit um die Tarifstufe weiß, liegt der EMT nicht im Geltungsbereich des ISMS des SMGW Admin und die Mindestvorgabe gilt für das ISMS des SMGW Admin wie definiert. Außer z.B. die normativen Regelungen von Marktkommunikation werden eine fallspezifische Ausnahme definieren.
- „Pseudonymisierte Netzzustandsdaten“ (Kapitel 4.3.2.22):
  Die Mindestvorgabe im Schutzziel Authentizität ist als „Die Authentizität der Daten MUSS mindestens in ihrer vertrauenswürdiger Echtheit gemäß Technischer Richtlinie gewährleistet werden.“ definiert. Die Mindestvorgabe kann z.B. erfüllt werden, wenn der SMGW Admin für die pseudonymisierten Netzzustandsdaten die Echtheit konzeptionell nachweisen kann und sich die technische/organisatorische Umsetzung der Konzeption prüfen lässt.
- „SMGW Firmware Update“ (Kapitel 4.3.2.5):
  Die Mindestvorgabe im Schutzziel Authentizität ist als „Die Authentizität der Daten MUSS in

vertrauenswürdiger und überprüfbarer Echtheit gemäß Technischer Richtlinie gewährleistet werden.“ definiert.
Die Mindestvorgabe kann z.B. erfüllt werden, wenn der SMGW Admin für das SMGW Firmware Update die Echtheit konzeptionell nachweisen kann und sich die technische/organisatorische Umsetzung der Konzeption prüfen lässt.
Eine überprüfbare Echtheit kann zusätzlich erreicht werden, wenn sich z.B. zu jedem SMGW Firmware Update jederzeit dessen konkrete Echtheit nachweisen lässt (z.B. anhand digitaler kryptographischer Signaturen nach anerkannten Sicherheitsstandards).

4.3.1 Übersicht

Dieses Kapitel fasst die im späteren Kapitel 4.3.2 („Mindestvorgaben zu den Assets“) angewandten Mindestvorgaben zu den Schutzzielen vorab zusammen. Die Übersicht untergliedert sich in Unterkapiteln nach Objekt Typ, wie in den Anwendungsfällen bestimmt, und behandelt jeweils die in Kapitel 4.2 vorgegebenen Schutzziele.

Aus der Übersicht lassen sich die möglichen unteren und oberen Schwellwerte normativer Mindestvorgaben ablesen.

4.3.1.1 Daten

Der aus bestehenden Mindestvorgaben zu den Schutzzielen von Daten[5] resultierende konkrete Schutzbedarf MUSS in Anweisungen, die diese Daten enthalten, sowie Diensten und Anbindungen, die diese Daten verarbeiten, gewährleistet werden.

5 Daten: Jede einzelne Information oder zusammengesetzte Information, die im Rahmen der Anwendungsfälle im SMGW oder im SMGW Admin-Betrieb verarbeitet wird (z.B. Profil, Letztverbraucher-ID, SMGW-ID, Schlüssel, Logeintrag)

Schutzziel	Mögliche Mindestvorgaben
Verfügbarkeit	• Keine Mindestvorgabe • Die Verfügbarkeit der Daten SOLL gewährleistet werden. • Die Verfügbarkeit der Daten MUSS gewährleistet sein, wenn sie benötigt werden. • Die Verfügbarkeit der Daten MUSS gewährleistet sein, wenn und so lange sie benötigt werden.
Vertraulichkeit	• Keine Mindestvorgabe • Die Kenntnis um den Dateninhalt SOLL auf den spezifischen SMGW Admin beschränkt sein. • Die Kenntnis um den Dateninhalt MUSS auf den spezifischen SMGW Admin beschränkt sein. • Die Kenntnis um den Dateninhalt MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein . • Die Kenntnis um den Dateninhalt MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein. • Die Kenntnis um den Dateninhalt sowie dessen Existenz in konkreter inhaltlicher Ausprägung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.
Integrität	• Keine Mindestvorgabe • Die Integrität der Daten SOLL gewährleistet werden. • Die Integrität der Daten MUSS gewährleistet werden.
Authentizität	• Keine Mindestvorgabe • Die Authentizität der Daten SOLL gewährleisten werden. • Die Authentizität der Daten MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden. • Die Authentizität der Daten MUSS in vertrauenswürdiger und überprüfbarer Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 61: Mögliche Mindestvorgaben zu den Schutzzielen von Daten

4.3.1.2 Anweisungen

Der Schutzbedarf einer Anweisung[6] MUSS in der konkreten Ausgestaltung mindestens den Schutzbedarf sämtlicher enthaltenen Daten gewährleisten.

6 Anweisung: Ein Befehl / Kommando vom SMGW Admin an das SMGW zur Auslösung einer Aktion.

Schutzziel	Mögliche Mindestvorgaben
Verfügbarkeit	• Keine Mindestvorgabe • Die Verfügbarkeit der Anweisung MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	• Keine Mindestvorgabe • Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung SOLL auf den spezifischen SMGW Admin beschränkt sein. • Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin beschränkt sein. • Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein. • Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.
Integrität	• Keine Mindestvorgabe • Die Integrität der Anweisung SOLL gewährleistet werden. • Die Integrität der Anweisung MUSS gewährleistet werden.
Authentizität	• Keine Mindestvorgabe • Die Authentizität der Anweisung SOLL gewährleisten werden. • Die Authentizität der Anweisung MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden. • Die Authentizität der Anweisung MUSS in vertrauenswürdiger und überprüfbarer Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 62: Mögliche Mindestvorgaben zu den Schutzzielen von Anweisungen

4.3.1.3 Dienste

Der Schutzbedarf eines Dienstes[7] MUSS in der konkreten Ausgestaltung mindestens den Schutzbedarf der verarbeiteten Daten gewährleisten.

Schutzziel	Mögliche Mindestvorgaben
Verfügbarkeit	• Keine Mindestvorgabe • Die Verfügbarkeit des Dienstes SOLL gewährleistet werden. • Die Verfügbarkeit des Dienstes MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	• Keine Mindestvorgabe
Integrität	• Die Integrität des Dienstes MUSS gewährleistet werden.
Authentizität	• Keine Mindestvorgabe

Tabelle 63: Mögliche Mindestvorgaben zu den Schutzzielen von Diensten

4.3.1.4 Anbindungen

Der Schutzbedarf einer Anbindung[8] MUSS in der konkreten Ausgestaltung mindestens den Schutzbedarf der übertragenen Daten gewährleisten.

Schutzziel	Mögliche Mindestvorgaben
Verfügbarkeit	• Keine Mindestvorgabe • Die Verfügbarkeit der Anbindung MUSS gewährleistet sein, wenn und so lange sie benötigt wird.
Vertraulichkeit	• Keine Mindestvorgabe
Integrität	• Keine Mindestvorgabe
Authentizität	• Keine Mindestvorgabe

Tabelle 64: Mögliche Mindestvorgaben zu den Schutzzielen von Anbindungen

4.3.2 Mindestvorgaben zu den Assets

In diesem Kapitel werden sämtliche werthaltigen Objekte aufgeführt, die unerlässlich zur Durchführung der in Kapitel 3 („Anwendungsfälle des Smart Meter Gateway Admin“) beschriebenen Anwendungsfällen sind und in diesen bereits beschrieben wurden. Die jeweils angegebenen Mindestvorgaben wurden nach Kapitel

7 Dienst: Die in Informationstechnik abgebildeten Dienste im SMGW Admin-Betrieb.

8 Anbindung: Alle technischen Objekte (Hardware und Software) im Einflussbereich des SMGW Admin, die für eine "Verbindung" zum EMT, Gateway Hersteller, PTB oder Sub-CA notwendig sind (z.B. Router, sonstige Netzkomponenten)

4.3.1 („Übersicht“) eingesetzt und ergaben sich subsumiert aus den Anwendungsfällen, gesetzlichen Vorgaben und der Technischen Richtlinie.

Eine Zusammenfassung der Mindestvorgaben zu den Schutzzielen für die hier aufgeführten Assets findet sich in Tabellenform im Anhang: Vereinfachte tabellarische Darstellung von Mindestvorgaben zu den Schutzzielen .

4.3.2.1 Gesetzliche Zeit

Dieses Asset bezieht sich auf die gesetzliche Zeit, wie im Kapitel 3.2.1 („Zeitsynchronisation“) behandelt.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der gesetzlichen Zeit MUSS gewährleistet sein, wenn sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität der gesetzlichen Zeit MUSS gewährleistet werden.
Authentizität	Die Authentizität der gesetzlichen Zeit MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 65: Mindestvorgaben zu den Schutzzielen von der gesetzlichen Zeit

4.3.2.2 SMGW Nachricht vom Typ Alarm

Dieses Asset bezieht sich sowohl auf eine, mehrere als auch auf alle SMGW Nachrichten vom Typ Alarm die gemäß Technischer Richtlinie in das SMGW Admin Log übernommen werden.

Die Mindestvorgaben entsprechen den Mindestvorgaben eines SMGW Admin Logeintrag (siehe Kapitel 4.3.2.17 („SMGW Admin Logeintrag“).

4.3.2.3 SMGW Nachricht vom Typ Benachrichtigung

Dieses Asset bezieht sich sowohl auf eine, mehrere als auch auf alle SMGW Nachrichten vom Typ Benachrichtigung gemäß Technischer Richtlinie.

Die Mindestvorgaben entsprechen den Mindestvorgaben eines SMGW Admin Logeintrag (siehe Kapitel 4.3.2.17 („SMGW Admin Logeintrag“).

4.3.2.4 Betriebsinformationen zu einem SMGW

Dieses Asset bezieht sich auf kumulierte Informationen zum Konfigurations-, Einsatz- und Betriebsstatus eines, mehrerer oder aller SMGW. Aus den in Kapitel 3 beschriebenen Anwendungsfällen sind diesem Asset mindestens die folgenden Objekte zugeordnet:

- SMGW-ID
- CLS-ID (nach Kapitel 3.2.3 „Empfang von SMGW Alarmierungen und Benachrichtigungen“)

- Profil-ID (nach Kapitel 3.3.2 „Profilverwaltung“)
- Letztverbraucher-ID (nach Kapitel 3.3.5 „Löschen von Teilen des Letztverbraucher Logs“)
- Speicherfrist vom Letztverbraucher (nach Kapitel 3.3.5 „Löschen von Teilen des Letztverbraucher Logs“)
- Notwendige Parameter für das Regelwerk (nach Kapitel 3.5.3 „Wechsel der Tarifstufen“)
- Zählpunkt-ID und Zähler-ID (nach Kapitel 3.5.4 „Abruf von Messwerten im Bedarfsfall“ sowie Kapitel 3.5.5 „Auslesen der Ist-Einspeiseleistung“)

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Daten MUSS gewährleistet sein, wenn und so lange sie benötigt werden.
Vertraulichkeit	Die Kenntnis um den Dateninhalt sowie dessen Existenz in konkreter inhaltlicher Ausprägung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.
Integrität	Die Integrität der Daten MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 66: Mindestvorgaben zu den Schutzzielen von Betriebsinformationen zu einem SMGW

4.3.2.5 SMGW Firmware Update

Dieses Asset bezieht sich auf ein, mehrere oder alle SMGW Firmware Updates.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des SMGW Firmware Updates MUSS gewährleistet sein, wenn und so lange es benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt des SMGW Firmware Update sowie dessen Existenz in konkreter inhaltlicher Ausprägung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.
Integrität	Die Integrität des SMGW Firmware Update MUSS gewährleistet werden.
Authentizität	Die Authentizität des SMGW Firmware Update MUSS in vertrauenswürdiger und überprüfbarer Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 67: Mindestvorgaben zu den Schutzzielen von SMGW Firmware Updates

4.3.2.6 Anweisung an SMGW zur Aktivierung eines Firmware-Update

Dieses Asset bezieht sich auf ein, mehrere oder alle Anweisungen an SMGW zur Aktivierung eines Firmware-Update. Aus dem Fachablauf eventuell resultierende fachliche Ablaufzustände werden unter einem eigenem Asset geführt (siehe Kapitel 4.3.2.32 „Fachlicher Ablaufzustand“).

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anweisung MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein.
Integrität	Die Integrität der Anweisung MUSS gewährleistet werden.
Authentizität	Die Authentizität der Anweisung MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 68: Mindestvorgaben zu den Schutzzielen von Anweisungen an SMGW zur Aktivierung eines Firmware-Update

4.3.2.7 Profile

Dieses Asset bezieht sich auf Inhaltsdaten eines, mehrerer oder aller Profile.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Profils MUSS gewährleistet sein, wenn und so lange es benötigt wird.
Vertraulichkeit	Die Kenntnis um den Profilinhalt sowie dessen Existenz in konkreter inhaltlichen Ausprägung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.
Integrität	Die Integrität des Profils MUSS gewährleistet werden.
Authentizität	Die Authentizität des Profils MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 69: Mindestvorgaben zu den Schutzzielen von Profilen

4.3.2.8 Private Schlüssel des SMGW Admin

Dieses Asset bezieht sich auf einen, mehrere oder alle privaten Schlüssel des SMGW Admin.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit seiner privaten Schlüssel MUSS gewährleistet sein, wenn und so lange sie benötigt werden.
Vertraulichkeit	Die Kenntnis seiner privaten Schlüssel MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.
Integrität	Die Integrität seiner privaten Schlüssel MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 70: Mindestvorgaben zu den Schutzzielen von Privaten Schlüsseln des SMGW Admin

4.3.2.9 Zertifikate

Dieses Asset bezieht sich auf ein, mehrere oder alle Zertifikate.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Zertifikate MUSS gewährleistet sein, wenn und so lange sie benötigt werden.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität der Zertifikate MUSS gewährleistet werden.
Authentizität	Die Authentizität der Zertifikate MUSS in vertrauenswürdiger und überprüfbarer Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 71: Mindestvorgaben zu den Schutzzielen von Zertifikaten

4.3.2.10 Zertifikatsrequest

Dieses Asset bezieht sich auf ein, mehrere oder alle Zertifikatsrequests.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Zertifikatsrequests MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität der Zertifikatsrequests MUSS gewährleistet werden.
Authentizität	Die Authentizität der Zertifikatsrequests MUSS in vertrauenswürdiger und überprüfbarer Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 72: Mindestvorgaben zu den Schutzzielen von Zertifikatsrequests

4.3.2.11 Anweisung an SMGW zur Generierung eines Zertifikatsrequest

Dieses Asset bezieht sich auf ein, mehrere oder alle Anweisungen an SMGW zur Generierung eines Zertifikatsrequests. Aus dem Fachablauf eventuell resultierende fachliche Ablaufzustände werden unter einem eigenem Asset geführt (siehe Kapitel 4.3.2.32 „Fachlicher Ablaufzustand“).

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anweisung MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin beschränkt sein.
Integrität	Die Integrität der Anweisung MUSS gewährleistet werden.
Authentizität	Die Authentizität der Anweisung SOLL gewährleisten werden.

Tabelle 73: Mindestvorgaben zu den Schutzzielen von Anweisungen an SMGW zur Generierung eines Zertifikatsrequest

4.3.2.12 Wake-Up-Paket

Dieses Asset bezieht sich auf ein, mehrere oder alle Wake-Up-Pakete.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anweisung MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität der Anweisung MUSS gewährleistet werden.
Authentizität	Die Authentizität der Anweisung SOLL gewährleisten werden.

Tabelle 74: Mindestvorgaben zu den Schutzzielen von Wake-Up-Paketen

4.3.2.13 Anweisung an SMGW zum Setzen der Speicherfrist für das Letztverbraucher-Log

Dieses Asset bezieht sich auf ein, mehrere oder alle Anweisungen an SMGW zur Speicherfrist im Letztverbraucher-Log.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anweisung MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein.
Integrität	Die Integrität der Anweisung MUSS gewährleistet werden
Authentizität	Die Authentizität der Anweisung MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 75: Mindestvorgaben zu den Schutzzielen von Anweisungen an SMGW zum Setzen der Speicherfrist für das Letztverbraucher-Log

4.3.2.14 Initiale Konfigurationsdatei

Dieses Asset bezieht sich auf ein, mehrere oder alle initialen Konfigurationsdateien.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der initialen Konfigurationsdatei MUSS gewährleistet sein, wenn und so lange sie benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt der initialen Konfigurationsdatei MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein. Hinweis: Der Integrator darf ebenfalls zweckgebunden die initiale Konfigurationsdatei im Auftrag des SMGW Admin berechtigt nutzen.
Integrität	Die Integrität der initialen Konfigurationsdatei MUSS gewährleistet werden.
Authentizität	Die Authentizität der initialen Konfigurationsdatei MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 76: Mindestvorgaben zu den Schutzzielen von Initiale Konfigurationsdateien

4.3.2.15 Logeintrag System-Log

Dieses Asset bezieht sich auf ein, mehrere oder alle Einträge aus dem System-Log eines SMGW.

Die Mindestvorgaben entsprechen den Mindestvorgaben eines SMGW Admin Logeintrag (siehe Kapitel 4.3.2.17 („SMGW Admin Logeintrag“).

4.3.2.16 Logeintrag eichtechn. Log

Dieses Asset bezieht sich auf ein, mehrere oder alle Einträge aus dem eichtechn. Log eines SMGW.

Die Mindestvorgaben entsprechen den Mindestvorgaben eines SMGW Admin Logeintrag (siehe Kapitel 4.3.2.17 („SMGW Admin Logeintrag“).

4.3.2.17 SMGW Admin Logeintrag

Dieses Asset bezieht sich sowohl auf einen, mehrere als auch auf alle Logeinträge im SMGW Admin-Log gemäß Technischer Richtlinie.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit eines Logeintrags MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt eines Logeintrags sowie dessen Existenz in konkreter inhaltlichen Ausprägung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.
Integrität	Die Integrität eines Logeintrags MUSS gewährleistet werden.
Authentizität	Die Authentizität eines Logeintrags MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 77: Mindestvorgaben zu den Schutzzielen von SMGW Admin Logeinträgen

4.3.2.18 Anweisung an SMGW zur Durchführung eines Selbsttests

Dieses Asset bezieht sich auf ein, mehrere oder alle Anweisungen an SMGW zur Durchführung eines Selbsttests.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anweisung MUSS gewährleistet werden wenn, und solange sie benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein.
Integrität	Die Integrität der Anweisung MUSS gewährleistet werden.
Authentizität	Die Authentizität der Anweisung MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 78: Mindestvorgaben zu den Schutzzielen von Anweisungen an SMGW zur Durchführung eines Selbsttests

4.3.2.19 Ergebnisdaten eines SMGW Selbsttests

Bis eine Spezifikation über Ergebnisdaten des Selbsttests in [BSI-TR-03109-1] definiert ist, verbleibt dieses Asset als nicht beschrieben.

Anmerkung: Die abschließende Anmerkung im Anwendungsfall „Selbsttest des SMGW anstoßen“ (siehe Kapitel 3.4.3) weist auf mögliche Mindestanforderungen dieses Asset.

4.3.2.20 Anweisung an SMGW zur Übermittlung von Logdaten

Dieses Asset bezieht sich auf ein, mehrere oder alle Anweisungen an SMGW zur Übermittlung von Logdaten.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anweisung MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein.
Integrität	Die Integrität der Anweisung MUSS gewährleistet werden.
Authentizität	Die Authentizität der Anweisung MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 79: Mindestvorgaben zu den Schutzzielen von Anweisungen an SMGW zur Übermittlung von Logdaten

4.3.2.21 Verschlüsselte und signierte Messwerte

Dieses Asset bezieht sich auf ein, mehrere oder alle verschlüsselten und signierten Messwerte.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Daten MUSS gewährleistet sein, wenn und so lange sie benötigt werden.
Vertraulichkeit	Die Kenntnis um den Dateninhalt SOLL auf den spezifischen SMGW Admin beschränkt sein.
Integrität	Die Integrität der Daten MUSS gewährleistet werden.
Authentizität	Die Authentizität der Daten MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 80: Mindestvorgaben zu den Schutzzielen von verschlüsselten und signierten Messwerten

4.3.2.22 Pseudonymisierte Netzzustandsdaten

Dieses Asset bezieht sich auf ein, mehrere oder alle pseudonymisierten Netzzustandsdaten.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Daten MUSS gewährleistet sein, wenn und so lange sie benötigt werden.
Vertraulichkeit	Die Kenntnis um den Dateninhalt SOLL auf den spezifischen SMGW Admin beschränkt sein.
Integrität	Die Integrität der Daten MUSS gewährleistet werden.
Authentizität	Die Authentizität der Daten MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 81: Mindestvorgaben zu den Schutzzielen von pseudonymisierten Netzzustandsdaten

4.3.2.23 Anweisung an SMGW zur Unterstützung der Messwertverarbeitung

Dieses Asset bezieht sich auf ein, mehrere oder alle Anweisungen an SMGW zur Unterstützung der Messwertverarbeitung.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anweisung MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	Die Kenntnis um den Inhalt und Übertragungsdetails der Anweisung MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein.
Integrität	Die Integrität der Anweisung MUSS gewährleistet werden.
Authentizität	Die Authentizität der Anweisung MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 82: Mindestvorgaben zu den Schutzzielen von Anweisungen an SMGW zur Unterstützung der Messwertverarbeitung

4.3.2.24 Log des SMGW Admin

Dieses Asset bezieht sich auf ein SMGW Admin-Log, das sämtliche SMGW Admin Logeinträge (gemäß Kapitel 4.3.2.17 („SMGW Admin Logeintrag“) hält.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Dienst MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität des Dienst MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 83: Mindestvorgaben zu den Schutzzielen vom Log des SMGW Admin

4.3.2.25 Dienst zum Empfang und Ausliefern von Messwerten

Dieses Asset bezieht sich auf einen Dienst, der zum Empfang und Ausliefern von Messwerten beim SMGW Admin betrieben wird.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Dienst MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität des Dienst MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 84: Mindestvorgaben zu den Schutzzielen vom Dienst zum Empfang und Ausliefern von Messwerten

4.3.2.26 Zeitserver SMGW Admin

Dieses Asset bezieht sich auf den Zeitserver des SMGW Admin der die gesetzliche Zeit (gemäß Kapitel 4.3.2.1 „Gesetzliche Zeit“) hält.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Dienst MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität des Dienst MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 85: Mindestvorgaben zu den Schutzzielen vom Zeitserver SMGW Admin

4.3.2.27 PTB Anbindung

Dieses Asset bezieht sich auf die Anbindung des SMGW Admin zur PTB zwecks Synchronisation der Zeitserver des SMGW Admin mit den Zeitservern der PTB.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anbindung MUSS gewährleistet sein, wenn und so lange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Keine Mindestvorgabe
Authentizität	Keine Mindestvorgabe

Tabelle 86: Mindestvorgaben zu den Schutzzielen von der PTB Anbindung

4.3.2.28 Zeitsynchronisation-Webservice des SMGW Admin

Dieses Asset bezieht sich auf den Zeitsynchronisation-Webservice des SMGW Admin der SMGW Anfragen zur gesetzlichen Zeit (siehe Kapitel 4.3.2.1 „Gesetzliche Zeit“) vom SMGW Admin Zeitserver (siehe Kapitel 4.3.2.26 („Zeitserver SMGW Admin“) bezieht und beantwortet.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Dienst MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität des Dienst MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 87: Mindestvorgaben zu den Schutzzielen vom Zeitsynchronisation-Webservice des SMGW Admin

4.3.2.29 WAN Anbindung

Dieses Asset bezieht sich auf die Anbindung des SMGW Admin an ein WAN zwecks Kommunikation mit den SMGW.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anbindung MUSS gewährleistet sein, wenn und so lange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Keine Mindestvorgabe
Authentizität	Keine Mindestvorgabe

Tabelle 88: Mindestvorgaben zu den Schutzzielen von der WAN Anbindung

4.3.2.30 Nachrichten Empfangsservice des SMGW Admin

Dieses Asset bezieht sich auf den Nachrichten Empfangsservice des SMGW Admin, der SMGW Nachrichten vom Typ Alarm (siehe Kapitel 4.3.2.2 „SMGW Nachricht vom Typ Alarm“) und vom Typ Benachrichtigung (siehe Kapitel 4.3.2.3 „SMGW Nachricht vom Typ Benachrichtigung“) empfängt.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Dienst MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität des Dienst MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 89: Mindestvorgaben zu den Schutzzielen vom Nachrichten Empfangsservice des SMGW Admin

4.3.2.31 EMT Anbindung

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anbindung MUSS gewährleistet sein, wenn und so lange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Keine Mindestvorgabe
Authentizität	Keine Mindestvorgabe

Tabelle 90: Mindestvorgaben zu den Schutzzielen von der EMT Anbindung

4.3.2.32 Fachlicher Ablaufzustand

Dieses Asset bezieht sich auf einen, mehrere oder alle fachlichen Ablaufzustände, die aus einem Zwischenstand von Anwendungsfällen nach Kapitel 3 ("Anwendungsfälle des Smart Meter Gateway Admin") resultieren.

Beispiel für einen fachlichen Ablaufzustand: Nachdem der GWA ein Wake-Up-Paket an ein SMGW gesendet hat, wird die Erwartung eines zeitnahen Verbindungsaufbau von diesem SMGW als fachlicher Ablaufzustand am GWA vorgehalten.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit eines fachlichen Ablaufzustands MUSS gewährleistet sein, wenn und so lange er benötigt werden.
Vertraulichkeit	Die Kenntnis um den Dateninhalt sowie dessen Existenz in konkreter inhaltlichen Ausprägung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.
Integrität	Die Integrität der Daten MUSS gewährleistet werden.
Authentizität	Die Authentizität der Daten SOLL gewährleisten werden.

Tabelle 91: Mindestvorgaben zu den Schutzzielen vom Fachlichen Ablaufzustand

4.3.2.33 Bestätigung oder Fehlermeldung eines SMGW

Dieses Asset bezieht sich auf ein, mehrere oder alle Bestätigungen / Fehlermeldungen des SMGW.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Daten MUSS gewährleistet sein, wenn und so lange sie benötigt werden.
Vertraulichkeit	Die Kenntnis um den Dateninhalt MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein.
Integrität	Die Integrität der Daten MUSS gewährleistet werden.
Authentizität	Die Authentizität der Daten MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 92: Mindestvorgaben zu den Schutzzielen von Bestätigungen oder Fehlermeldungen eines SMGW

4.3.2.34 SMGW Admin Update Dienst

Dieses Asset bezieht sich auf einen Dienst, der auf Anfrage eines SMGW ein passendes Firmware-Update (siehe Kapitel 4.3.2.5 „SMGW Firmware Update“) bereitstellt.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Dienst MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität des Dienst MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 93: Mindestvorgaben zu den Schutzzielen vom SMGW Admin Update Dienst

4.3.2.35 Anbindung zur Sub-CA

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anbindung MUSS gewährleistet sein, wenn und so lange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Keine Mindestvorgabe
Authentizität	Keine Mindestvorgabe

Tabelle 94: Mindestvorgaben zu den Schutzzielen von der Anbindung zur Sub-CA

4.3.2.36 SMGW Admin Software

Obwohl in Kapitel 3 („Anwendungsfälle des Smart Meter Gateway Admin“) keine SMGW Admin Software explizit beschrieben und definiert wurde, versteht dieses Dokument eine SMGW Admin Software als Oberbegriff für eine technische Steuereinheit und Infrastruktur zur unterstützenden und teilautomatisierten Durchführung der beschriebenen Anwendungsfälle sowie sonstige Funktionen und Dienste die zur Aufgabenerfüllung eines SMGW Admin erforderlich sind.

Die funktionale und technische Ausgestaltung kann im Einzelfall unterschiedlich ausfallen.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Dienst MUSS gewährleistet sein, wenn und so lange er benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität der SMGW Admin Software MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 95: Mindestvorgaben zu den Schutzzielen von der SMGW Admin Software

4.3.2.37 Frontend SMGW Admin Software

Dieses Asset ergänzt die in Kapitel 4.3.2.36 („SMGW Admin Software“) bereits beschriebene SMGW Admin Software und bezieht sich auf eine funktionale Zugriffseinheit gegenüber der SMGW Admin Software.

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit des Frontend SMGW Admin Software MUSS gewährleistet sein, wenn und so lange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität des Frontend SMGW Admin Software MUSS gewährleistet werden.
Authentizität	Keine Mindestvorgabe

Tabelle 96: Mindestvorgaben zu den Schutzzielen vom Frontend SMGW Admin Software

4.3.2.38 SMGW Hersteller Anbindung

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Anbindung MUSS gewährleistet sein, wenn und so lange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Keine Mindestvorgabe
Authentizität	Keine Mindestvorgabe

Tabelle 97: Mindestvorgaben zu den Schutzzielen von der SMGW Hersteller Anbindung

4.3.2.39 Sperrliste

Schutzziel	Mindestvorgaben
Verfügbarkeit	Die Verfügbarkeit der Sperrliste MUSS gewährleistet werden, wenn und solange sie benötigt wird.
Vertraulichkeit	Keine Mindestvorgabe
Integrität	Die Integrität der Sperrliste MUSS gewährleistet werden.
Authentizität	Die Authentizität der Sperrliste MUSS in vertrauenswürdiger und überprüfbarer Echtheit gemäß Technischer Richtlinie gewährleistet werden.

Tabelle 98: Mindestvorgaben zu den Schutzzielen von der Sperrliste

4.4 Bedrohungen

In den nachfolgenden Unterkapiteln werden relevante Bedrohungen für einen SMGW Admin Betrieb aufgeführt, bei denen das mit einem Eintritt verbundene Risiko als nicht tragbar eingeschätzt wird und eine Technologie neutrale Bedrohung bestimmt werden kann.

Die meisten Bedrohungen wurden zudem bewusst in ihrem Abdeckungsbereich großzügig formuliert, um die geforderte Betrachtung im ISMS eines verantwortlichen SMGW Admin zu zielgerichteten und einsatzspezifischen Maßnahmen zu führen. Die vollständige Ableitung dieser Bedrohungen als auch seiner individuell identifizierten Bedrohungen obliegt dem verantwortlichen SMGW Admin in seinem ISMS.

4.4.1 Spezifische Bedrohungen

Aus den in Kapitel 3 („Anwendungsfälle des Smart Meter Gateway Admin“) aufgeführten Anwendungsfällen des SMGW Admin wurden die in den nachfolgenden Unterkapiteln beschriebenen Bedrohungen abgeleitet.

4.4.1.1 Verbindungsaufbau vom SMGW zum SMGW Admin

B.VA.1	Angreifer gibt vor, ein (bekanntes) SMGW zu sein
	Ein Angreifer versucht, unter Verwendung einer nicht registrierten Kennung (SMGW, das bisher nicht existiert) oder einer beim SMGW Admin bereits bekannten Kennung (z.B. ausgelesen aus übertragenen Zertifikat), eine Verbindung zum SMGW Admin aufzubauen.

Tabelle 99: Bedrohungen beim Verbindungsaufbau

4.4.1.2 Zeitsynchronisation mit PTB

B.PTB.1	Zeitsynchronisation mit der PTB schlägt fehl
	Bei der Zeitsynchronisation mit der PTB kann es zu vielfältigen Fehlersituationen kommen. Hierzu zählen u.a.: – Verbindung zum Zeitserver der PTB ist gestört (Netzprobleme, Überlastung vom Zeitserver der PTB, ...) – Zeitangaben der PTB sind offensichtlich falsch (plötzliche ungewöhnliche Abweichung)
B.PTB.2	Manipulation der Kommunikation zur Zeitsynchronisation mit der PTB
	Ein Angreifer kann versuchen, die Kommunikation zur Zeitsynchronisation mit der PTB so zu manipulieren, dass die resultierenden Zeitinformationen beim SMGW Admin von der wirklichen Zeit abweichen. Dies hätte auch eine Abweichung in den SMGW zur Folge, die ihre Zeit vom SMGW Admin beziehen.
B.PTB.3	Überlastung der PTB Infrastruktur durch häufige Zeitsynchronisation
	Durch unangemessen häufige Zeitsynchronisationen zahlreicher SMGW Admin könnte die PTB Infrastruktur in einem Ausmaß belastet werden, die einen regulären Bezug der gesetzlichen Zeit durch den PTB Zeitserver behindert oder gänzlich verhindert.

Tabelle 100: Bedrohungen bei der Zeitsynchronisation mit der PTB

4.4.1.3 Zeitsynchronisation mit SMGW

B.ZS.1	Manipulation der Kommunikation zur Zeitsynchronisation zwischen SMGW und SMGW Admin
	Ein Angreifer kann versuchen, die Kommunikation zur Zeitsynchronisation zwischen SMGW und SMGW Admin so zu manipulieren, dass die resultierenden Zeitinformationen beim SMGW von der wirklichen Zeit abweichen.

Tabelle 101: Bedrohungen bei der Zeitsynchronisation mit dem SMGW

4.4.1.4 Empfang von SMGW Alarmierungen und Benachrichtigungen

B.AB.1	Fehlerhafte Zuordnung von Alarmierungen und Benachrichtigungen zu einem SMGW
	Eine fehlerhafte Zuordnung von Alarmierungen und Benachrichtigungen kann aus unterschiedlichsten Gründen passieren, z.B.: – Die Manipulation der Zuordnung von Alarmierungen und Benachrichtigungen zu einem SMGW, so dass diese fälschlicherweise einem anderem SMGW zugeordnet werden. – Die Erzeugung zusätzlicher Alarmierungen und Benachrichtigungen durch einen Angreifer, die dann einem SMGW zugeordnet werden. – Eine fehlerhafte Zuordnung aufgrund von Fehlern in der verarbeitenden Software.

Tabelle 102: Bedrohungen beim Empfang von SMGW Alarmierungen und Benachrichtigungen

4.4.1.5 Kommunikation zwischen EMT und CLS

Die Bedrohungen der Kommunikation zwischen EMT und CLS lassen sich aus Sicht des SMGW Admin auf folgende „Teil-Bedrohungen“ abbilden (siehe hierzu auch Anwendungsfall 3.2.4):

- Bedrohung der Kommunikation zwischen EMT und SMGW Admin

- Bedrohung der Kommunikation zwischen SMGW Admin und SMGW

- Bedrohungen im Bereich des SMGW Admin Betriebs.

Damit lassen sich diese Bedrohungen durch die in Kapitel 4.4.2 erläuterten allgemeinen Bedrohungen ersetzen (vgl. insbesondere Kapitel 4.4.2.9 und 4.4.2.10).

4.4.1.6 Aktualisierung der Firmware des SMGW

In diesem Abschnitt werden spezifische Bedrohungen bezogen auf die Aktualisierung der Firmware des SMGW aufgeführt. Diese beziehen sich auf die Anwendungsfälle

– „Firmware-Download“,

– „Bereitstellung von SMGW Firmware-Updates“

Da sich die Bedrohungen oft auf mehr als einen Anwendungsfall beziehen und somit nicht eindeutig zugeordnet werden können, wurden diese in einem Abschnitt zusammengefasst.

B.SU.1	Manipulation von Firmware-Updates bei der Übertragung vom SMGW-Hersteller zum SMGW Admin
	Ein Angreifer kann versuchen, das Firmware-Update bereits bei der Übertragung vom SMGW-Hersteller zum SMGW Admin zu manipulieren oder durch eine falsche Version zu ersetzen. Damit wären alle SMGW betroffen, für die das echte Update bestimmt ist.
B.SU.2	Manipulation von Firmware-Updates in der Infrastruktur des SMGW Admin
	Ein Angreifer kann versuchen, das Firmware-Update in der Infrastruktur des SMGW Admin zu manipulieren oder durch eine falsche Version zu ersetzen. Damit wären alle SMGW betroffen, für die das echte Update bestimmt ist.
B.SU.3	Unterdrückung der Aufforderung des SMGW Admin zum Laden eines Firmware-Updates
	Ein Angreifer kann versuchen, die an ein SMGW gerichtete Aufforderung des SMGW Admin zum Laden eines Firmware-Updates zu unterdrücken. Damit kann z.B. erreicht werden, dass die Behebung eines Fehlers auf dem SMGW nicht vollzogen wird.
B.SU.4	Manipulation von Firmware-Updates bei der Übertragung vom SMGW Admin zum SMGW
	Ein Angreifer kann versuchen, das Firmware-Update erst bei der Übertragung vom SMGW Admin zum SMGW zu manipulieren oder durch eine falsche Version zu ersetzen. Damit könnten gezielt einzelne SMGW mit einem gefälschtem Update versorgt werden.
B.SU.5	Informationsstand des SMGW Admin über die Firmware-Version weicht von tatsächlichem Stand im SMGW ab
	Wenn der Informationsstand des SMGW Admin über die Firmware-Version eines SMGW vom tatsächlichen Stand im SMGW abweicht, kann dies dazu führen, dass notwendige Updates nicht durchgeführt werden.
B.SU.6	Bandbreitenverbrauch bei Massenupdates behindert den Betrieb des SMGW Admin
	Wenn viele SMGW auf einmal ihr Firmware-Update laden, kann es aufgrund des Bandbreitenverbrauchs beim Download zu Behinderungen im Betrieb des SMGW Admin kommen.
B.SU.7	Wichtige Updates werden (organisatorisch) nicht zeitnah eingespielt
	Zwischen Lieferung eines Firmware-Updates durch den SMGW-Hersteller und Einspielung auf den SMGW durch den SMGW Admin kann eine zu große Zeitspanne liegen. Dies wird insbesondere dadurch begünstigt, dass der SMGW Admin alle entsprechenden SMGW über das Vorliegen eines Firmware-Updates informieren muss, sofern diese nicht eigenständig regelmäßig prüfen, ob ein Firmware-Update vorliegt.

Tabelle 103: Bedrohungen bei der Aktualisierung der Firmware des SMGW

Anmerkung:

Die Bedrohung „Firmware-Update wird bereits fehlerhaft vom Hersteller ausgeliefert“ betrifft nicht den SMGW Admin sondern den SMGW-Hersteller.

Die Bedrohung „Versuch, ein falsches Update auf ein SMGW einzuspielen“ betrifft nicht den SMGW Admin sondern das SMGW.

4.4.1.7 Profilverwaltung

B.PV.1	Einspielen eines Profils in ein falsches SMGW
	Wird ein Profil in ein falsches SMGW eingespielt, so kann dies je nach Profil unterschiedliche Folgen haben, z.B.: – Messdaten werden dem falschen Letztverbraucher zugeordnet. – Geräte können nicht angesprochen werden. – Das SMGW kann keine Daten liefern. – Das SMGW kann funktionsunfähig werden.
B.PV.2	Einspielen eines fehlerhaften Profils in ein SMGW
	Das Einspielen fehlerhafter Profile in SMGW kann zur Folge haben, dass die Profile den vorgesehenen Zweck nicht erfüllen und somit z.B. eine Kommunikation nicht möglich ist (im Extremfall ist z.B. bei einem fehlerhaften WAN-Kommunikationsprofil keine Kommunikation zwischen SMGW und SMGW Admin mehr möglich) oder die gelieferten Daten nicht den erwarteten entsprechen. Ein Profil kann z.B. fehlerhaft sein, weil bereits die vom EMT für das Profil gelieferten Daten falsch sind.
B.PV.3	Informationsstand des SMGW Admin über Profile weicht vom tatsächlichen Stand im SMGW ab
	Wenn der Informationsstand des SMGW Admin über Profile vom tatsächlichen Stand im SMGW abweicht, kann dies zur Folge haben, dass notwendige Änderungen nicht durchgeführt werden. Dies kann z.B. der Fall sein, wenn angenommen wird, dass die Änderungen bereits aktiv sind.
B.PV.4	SMGW Admin erstellt Auswertungsprofil mit falschem Empfänger der Daten
	In den Auswertungsprofilen werden Kommunikationsprofile für die Empfänger der Daten referenziert. Dabei können in einem Auswertungsprofil auch mehrere Empfänger eingetragen werden. Wird dort ein nicht vorgesehenes Kommunikationsprofil referenziert, so werden die Daten an den dort eingetragenen Empfänger gesendet. Auf diese Weise können Daten z.B. zusätzlich an einen nicht zuständigen EMT oder an den SMGW Admin selbst versendet werden.

Tabelle 104: Bedrohungen bei der Profilverwaltung

Anmerkung:

In bestimmten Profilen sind sensible Informationen enthalten, die nicht offen gelegt werden dürfen, z.B. Kennung + Passwort im HAN-Kommunikationsprofil oder symmetrische Schlüssel im Zählerprofil. Die Bedrohung der Offenlegung von Profilen wird in Kapitel 4.4.2.8 („Ungesicherte Betriebsdaten“) behandelt.

Die Bedrohung „Unberechtigter spielt Profil in SMGW ein“ betrifft nicht den SMGW Admin, sondern das SMGW.

4.4.1.8 Schlüssel-/Zertifikatsmanagement

B.SZ.1	Private Schlüssel des SMGW Admin sind nicht verfügbar (organisatorisch/technisch)
	Die privaten Schlüssel des SMGW Admin sind zwingend notwendig für den Aufbau verschlüsselter Verbindungen, die Entschlüsselung empfangener verschlüsselter Nachrichten und die Erstellung von Signaturen.
B.SZ.2	Private Schlüssel des SMGW Admin werden offen gelegt
	Werden private Schlüssel des SMGW Admin offen gelegt, sind damit verschlüsselte Daten bzw. erstellte Signaturen nicht mehr sicher.
B.SZ.3	Zertifikate sind nicht verfügbar (organisatorisch/technisch)
	Bei nicht verfügbaren Zertifikaten ist es nicht möglich, die Nachrichten für den entsprechenden Empfänger zu verschlüsseln. Außerdem werden die Zertifikate beim Erstellen/Anpassen von Profilen benötigt.
B.SZ.4	Zertifikate werden nicht rechtzeitig ersetzt bzw. sind abgelaufen
	Wenn Zertifikate nicht rechtzeitig ersetzt werden bzw. abgelaufen sind, führt dies dazu, dass die Ausstellung eines Folgezertifikats nicht mehr möglich ist. Somit müsste eine erneute Registrierung des Nutzers bei der Sub-CA durchgeführt werden. Bei den SMGW ist dies allerdings nicht möglich, da diese keinen gültigen Zertifikatsrequest mehr erstellen können, so dass ein SMGW in diesem Fall nicht mehr verwendet werden kann. Noch drastischer gestaltet es sich, wenn das Zertifikat des SMGW Admin nicht rechtzeitig ersetzt wird (sowohl beim SMGW Admin selbst als auch in den verwalteten SMGW). In diesem Fall verweigern nämlich alle vom betroffenen SMGW Admin verwalteten SMGW die weitere Kommunikation mit dem SMGW Admin, so dass die SMGW alle ersetzt werden müssen.
B.SZ.5	Schlüssel/Zertifikate werden an falscher Stelle eingespielt
	Werden Schlüssel/Zertifikate an falscher Stelle eingespielt, so kann dies dazu führen, dass eine vorgesehene Kommunikation nicht möglich ist oder dass Informationen an der falschen Stelle entschlüsselt werden können bzw. die Kommunikation mit der falschen Stelle durchgeführt wird.
B.SZ.6	Kommunikation des SMGW Admin mit der Sub-CA wird durch Angreifer manipuliert bzw. gestört
	Wird die Kommunikation des SMGW Admin mit der Sub-CA gestört, so kann ein Angreifer damit erreichen, dass die Prüfung von Zertifikaten nicht möglich ist sowie Zertifikate nicht rechtzeitig ersetzt werden können. Mit einer Manipulation der Kommunikation des SMGW Admin mit der Sub-CA wären z.B. die Fälschung von Prüfungsergebnissen oder das Unterschieben falscher Zertifikate denkbar.

Tabelle 105: Bedrohungen beim Schlüssel-/Zertifikatsmanagement (Teil 1)

B.SZ.7	Die Sperrliste ist nicht aktuell
	Wird die Sperrliste nicht regelmäßig aktualisiert, könnten bereits kompromittierte Zertifikate weiter genutzt werden.
B.SZ.8	Ausliefern der Sperrliste wird verhindert
	Kann die angeforderte Sperrliste von der Sub-CA nicht empfangen werden, liegen beim SMGW Admin veraltete Sperrlisten vor (siehe B.SZ.7).
B.SZ.9	Sperrliste wird im Betrieb nicht umgesetzt
	Eine Nichtbeachtung der vorliegenden Sperrliste beim Zertifikatsmanagement kann z.B. dazu führen, dass kompromittierte Zertifikate weiter genutzt werden.

Tabelle 106: Bedrohungen beim Schlüssel-/Zertifikatsmanagement (Teil 2)

Anmerkung:

Ein in seiner Integrität verletztes Zertifikat muss als nicht verfügbar betrachtet werden.

4.4.1.9 Senden eines Wake-Up Paketes

B.WU.1	Wake-Up Paket wird durch Angreifer unterdrückt
	Indem ein Angreifer Wake-Up Pakete an ein SMGW unterdrückt, kann dieser die Administration des SMGW verhindern, bis dieses von sich aus eine Verbindung zum SMGW Admin aufbaut.
B.WU.2	Wake-Up Paket wird durch Angreifer erneut eingespielt
	Wird ein Wake-Up Paket erneut einspielt und das SMGW baut daraufhin eine Verbindung zum SMGW Admin auf, so kann dies eine Vorbereitung für einen Angriff auf die dann bestehende Verbindung sein. Spielt ein Angreifer sehr viele Wake-Up Pakete wieder ein und die angesprochenen SMGW versuchen dann alle eine Verbindung zum SMGW Admin aufzubauen, so kann dies den Betrieb des SMGW Admin durch Überlastung beeinträchtigen.
B.WU.3	Wake-Up Paket wird durch Angreifer manipuliert
	Eine Manipulation des Wake-Up Pakets kann dafür sorgen, dass das adressierte SMGW nicht wie vorgesehen reagiert, d.h. es wird keine Verbindung zum SMGW Admin aufgebaut.
B.WU.4	Wake-Up Pakete werden durch Angreifer verzögert
	Ein Angreifer könnte Wake-Up-Pakete an mehrere Gateways verzögern und später an alle gleichzeitig weiterleiten. Dann bauen alle Gateways gleichzeitig eine Management-Verbindung zum SMGW Admin auf und könnten die Infrastruktur überlasten.

Tabelle 107: Bedrohungen beim Senden eines Wake-Up Paketes

4.4.1.10 Löschen von Teilen des Letztverbraucher Logs

B.LL.1	SMGW Admin sendet Frist/Letztverbraucher-ID an falsches SMGW
	Sendet der SMGW Admin die Frist/Letztverbraucher-ID an ein falsches SMGW, so wird der intendierte Auftrag nicht ausgeführt und eventuell eine aufwändige Fehlersuche eingeleitet. Außerdem könnte es sein, dass auf dem falschen SMGW Teile des Letztverbraucher Logs gelöscht werden.
B.LL.2	Fehlende organisatorische Regelung, wann das Letztverbraucher Log gelöscht werden soll/muss/darf
	Fehlen entsprechende organisatorische Regelungen, so kann dies darin resultieren, dass Teile des Letztverbraucher Logs zu früh/spät gelöscht werden oder aber der Log Speicher überläuft.

Tabelle 108: Bedrohungen beim Löschen von Teilen des Letztverbraucher Logs

4.4.1.11 Bereitstellung der initialen Konfigurationsdatei

B.IK.1	Die Integrität, Vertraulichkeit und Authentizität der Daten ist auf dem Kommunikationsweg zum Integrator nicht gewährleistet
	Kann die Integrität, Vertraulichkeit und Authentizität der Daten auf dem Kommunikationsweg zum Integrator nicht gewährleistet werden, so ist der ordnungsgemäße Betrieb des/der SMGW gefährdet.

Tabelle 109: Bedrohungen bei der Bereitstellung der initialen Konfigurationsdatei

4.4.1.12 Monitoring

Das Monitoring bezieht sich auf die Anwendungsfälle

- „Auswerten der SMGW Nachrichten“,
- „Lesen der SMGW-Logs“,
- „Selbsttest des SMGW anstoßen“
- „Führen eines SMGW Admin-Logs“.

Das Monitoring umfasst damit das Austauschen von Nachrichten über Kommunikationsverbindungen (siehe 4.4.2.9, „Ungesicherte Kommunikationsverbindungen“) und die Speicherung und Verwaltung von Betriebsdaten (siehe 4.4.2.8, „Ungesicherte Betriebsdaten“). Als Bedrohungen für die hier genannten Anwendungsfälle lassen sich somit die unter 4.4.2.9 und 4.4.2.8 aufgeführten allgemeinen Bedrohungen nennen.

Zu den Betriebsdaten zählen insbesondere:

- Alarmierungen
- Benachrichtigungen

– SMGW-Logs
– Ergebnisdaten des Selbsttests
– Einträge des SMGW Admin-Logs

Anmerkung:

Die Bedrohung „Erneutes Anstoßen des Selbsttest durch Wiedereinspielen von Nachrichten“ betrifft nicht den SMGW Admin sondern das SMGW.

4.4.1.13 Unterstützung der Messwertverarbeitung

In diesem Abschnitt werden spezielle Bedrohungen bezogen auf die Unterstützung der Messwertverarbeitung aufgeführt. Diese beziehen sich auf die Anwendungsfälle

– „Tarifierte Messwerte“,
– „Netzzustandsdaten“,
– „Wechsel der Tarifstufen“,
– „Abruf von Messwerten im Bedarfsfall“ und
– „Auslesen der Ist-Einspeiseleistung“.

Da sich die Bedrohungen oft auf mehr als einen Anwendungsfall beziehen und somit nicht eindeutig zugeordnet werden können, wurden diese in einem Abschnitt zusammengefasst.

B.MB.1	Daten werden nicht weitergeleitet
	Werden Daten der Messwertverarbeitung nicht weitergeleitet, so kann dies zu fehlerhaften Verbrauchsabrechnungen führen.
B.MB.2	Netzzustandsdaten werden nicht pseudonymisiert
	Bei fehlender Pseudonymisierung von Netzzustandsdaten werden Vorgaben des Datenschutzes missachtet.
B.MB.3	Profilbildung beim SMGW Admin mittels Klartextdaten, die sich einzelnen Letztverbrauchern zuordnen lassen
	Die Profilbildung beim SMGW Admin widerspricht Vorgaben des Datenschutzes.
B.MB.4	Wechsel der Tarifstufe kann nicht vollzogen werden bzw. ist fehlerhaft
	Kann ein Wechsel der Tarifstufe nicht vollzogen werden bzw. ist dieser fehlerhaft, so hat dies ggf. falsche Abrechnungen zur Folge.

Tabelle 110: Bedrohungen bei der Unterstützung der Messwertverarbeitung

Anmerkung:

Grundsätzlich besteht noch die Bedrohung, dass Daten der Messwertverarbeitung bei der Übertragung oder in der Infrastruktur des SMGW Admin manipuliert werden. Dies kann unterschiedlich gravierende

Auswirkungen haben, z.B. falsche Entscheidungsfindung des VNB aufgrund manipulierter Netzzustandsdaten. Die Bedrohung der Manipulation von Daten wird in den übergreifenden Bedrohungen behandelt, in diesem Fall die Bedrohungen in den Kapiteln 4.4.2.8 („Ungesicherte Betriebsdaten“) und 4.4.2.9 („Ungesicherte Kommunikationsverbindungen“).

4.4.2 Übergreifende Bedrohungen

Ergänzend zu den in Kapitel 4.4.1 („Spezifische Bedrohungen“) aufgeführten spezifischen Bedrohungen können die in diesem Kapitel beschriebenen Bedrohungen Anwendungsfall übergreifend wirken.

4.4.2.1 Mangelhafte Konformität gegenüber Technischer Richtlinie

Der SMGW Admin kann die ihm zugedachten Aufgaben ausschließlich erfüllen, wenn alle beteiligten Stellen und technischen Komponenten konform zur Technischen Richtlinie agieren. Aus der zentralen Einbettung des SMGW Admin in Kommunikations-, Verwaltungs- und Steueraufgaben resultiert wiederum die Erfordernis, dass der SMGW Admin in seinen Aufgaben und technischen Hilfsmitteln ebenfalls Konformität zur Technischen Richtlinie gewährleisten muss. Die Rahmenbedingung, dass die Technische Richtlinie bedarfsgerecht fortgeschrieben wird, verlangt besondere Aufmerksamkeit.

Jede Abweichung von der Technischen Richtlinie kann für den SMGW Admin und/oder für Dritte zu ggf. weitreichenden Betriebsstörungen führen.

Beispiele für mangelhafte Konformität gegenüber Technischer Richtlinie sind:

- Vorgaben der Technischen Richtlinie werden nicht umgesetzt.
- Konformität der eingesetzten technischen Hilfsmittel nicht zertifiziert.

4.4.2.2 Implementierungsfehler und Sicherheitslücken in SMGW Admin Software oder Frontend SMGW Admin Software

Konzeptionelle und Implementierungsfehler in einer die Anwendungsfälle unterstützenden Software (SMGW Admin Software) können zu weitreichenden und vorab schwer bestimmbaren Folgen führen. Diese Bedrohung bezieht sich sowohl auf durch Dritthersteller entwickelte Software, Eigenentwicklungen sowie Softwarekomponenten zur Interoperabilität zwischen technischen Komponenten.

Beispiele:

- Technische Sicherheitslücken in relevanten OSI-Layer.
- Rollentrennung in SMGW Admin Software nicht gewährleistet.
- Eventuell erforderliche Mandantenfähigkeit nicht gewährleistet.
- Unzureichende Behandlung von SMGW Nachrichten die Abweichungen gegenüber der Technischen Richtlinie aufweisen.
- Fehlerhafte Generierung von SMGW Nachrichten.
- Fehlerhafte Generierung und/oder Verarbeitung herstellerspezifischer Erweiterungen.
- Fehlerhafte oder unzureichende Behandlung von Ereignissen die konzeptionell nicht eintreten sollten, jedoch eintreten können.

- Technisches Verhalten abweichend gegenüber Software Einstellungen.
- Technisches Verhalten abweichend gegenüber Steueranweisungen durch SMGW Admin Fachpersonal.
- Unzureichende Berücksichtigung eingestellter Berechtigungen.
- Fehlerhafte Datenzuordnung.
- Anerkennung unbekannter Zertifikate.
- Mandantenfähigkeit nicht über alle Komponenten gewährleistet; wenn Mandantenfähigkeit erforderlich.

4.4.2.3 Keine oder unzureichende Nachvollziehbarkeit

In den komplexen Betriebsprozessen eines SMGW Admin werden eine Vielzahl manueller oder technisch unterstützter Handlungen durch Ereignisse ausgelöst. Die jeweils konkrete Ausprägung der erforderlichen Handlung wird auf Basis vorliegender Informationen getroffen werden müssen.

Sollte sich dem SMGW Admin nicht nachvollziehbar darstellen, welche ereignisorientierte Handlungen anstehen, besteht die Gefahr, das Handlungen nicht veranlasst werden.

Sollten dem SMGW Admin zum Zeitpunkt einer Handlung nicht sämtliche erforderlichen Informationen nachvollziehbar vorliegen, besteht die Gefahr inkorrekt zu handeln.

Sollten bereits getätigte Handlungen und sämtliche zu diesem Zeitpunkt im Zusammenhang stehenden Informationen nicht abrufbar sein, ist keine Handlung in der Vergangenheit nachvollziehbar.

Beispiele für unzureichende Nachvollziehbarkeit sind:

- Keine dokumentierten Arbeitsanweisungen.
- Keine Protokollierung gesendeter Nachrichten ohne Angabe „wer“, „wann“ und „warum“ die Nachricht generiert und gesendet hat.
- Keine Protokollierung empfangener Nachrichten.
- Keine organisatorischen Handlungen die in Art und Umfang an eine Protokollierung angelehnt sind.
- Technische Protokollierung ohne zuverlässigen Zeitstempel.

4.4.2.4 Betriebsinfrastruktur unzureichend vor unberechtigtem Zutritt, Zugang und/oder Zugriff geschützt

Die Aufgabenerfüllung des SMGW Admin erfolgt innerhalb einer betrieblichen Infrastruktur, bestehend aus einer individuellen Gebäude- und technischen Infrastruktur. Im Ergebnis bedroht jede Schwachstelle der betrieblichen Infrastruktur direkt oder indirekt die vom SMGW Admin verarbeiteten Informationen vollständig oder in Teilen ihres Schutzbedarfs.

Beispiele:

- Mängel im Zutrittsschutz eines SMGW Admin Betriebsraum gefährden die im oder über den Betriebsraum verarbeiteten Informationen.
- Netzwerke des SMGW Admin ohne Zugangs- und/oder Zugriffsschutz gefährden die über das Netzwerk übermittelten Informationen.
- Datenhaltung und Datenverarbeitung in einer „Cloud“ können die Daten in Ihrem Schutzbedarf auf dem Übertragungsweg oder an ihrem Speicherort gefährden.

– Arbeitsplätze ohne wirksamen Integritätsschutz bedrohen den Schutzbedarf der über sie erreichbaren Informationen durch Schadsoftware und physischen Manipulationen.
– Serversysteme des SMGW Admin sind bei mangelhaften Zugangs- und Zugriffsschutz gegenüber unberechtigten Änderungen gefährdet.
– SMGW Admin Tätigkeiten im Homeoffice gefährden bei mangelhaften Zugangs- und Zugriffsschutz auf dem Übertragungsweg als auch dem Homeoffice selbst die erreichbaren Informationen.

4.4.2.5 Unzureichende Beachtung von Datenschutzrecht

Aufgabe des Datenschutzes ist es nach § 1 Bundesdatenschutzgesetz (BDSG), "den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird". In den Datenschutzgesetzen der Länder finden sich ähnliche Aufgabenumschreibungen zum Schutz des "Rechts auf informationelle Selbstbestimmung". Das gesamte Datenschutzrecht bezieht sich nur auf personenbezogene Daten. Darunter sind "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" zu verstehen. Juristische Personen werden nicht erfasst.

Aus dem Verbotsprinzip mit Erlaubnisvorbehalt muss für den SMGW Admin die Konformität zur Rechtsnorm gewährleistet werden, die u.A. umfasst:

- Grundsatz der Datensparsamkeit und Datenvermeidung (BDSG §3a)
- Ggf. Bestellung eines Beauftragten für den Datenschutz (BDSG §4f)
- Technische und organisatorische Maßnahmen (BDSG §9 und Anlage zu §9 Satz 1)
- Transparente und dokumentierte EDV (Verfahrensverzeichnis nach BDSG §4d und BDSG §4e)
- Vorgaben und Rahmenbedingungen zur Auftragsdatenverarbeitung (BDSG §11)[9]
- Erheben, Speichern, Verändern, Übermitteln oder Nutzung personenbezogener Daten für eigene Geschäftszwecke sowie Übermittlung oder Nutzung für einen anderen Zweck (BDSG §28)

Beispiele für unzureichende Beachtung des Datenschutzrechts:

– Verarbeitung personenbezogener Daten (nach Definition des BDSG) im Ausland mit einem geringeren Datenschutzniveau als in der Bundesrepublik Deutschland.
– Zusammenführung von getrennten Informationen die zur Bestimmbarkeit einer natürliche Person führen können.
– Unzureichende Prüfung und Einhaltung von Rechtsvorschriften.
– Verzicht auf die Bestellung eines betrieblichen Datenschutzbeauftragten in Unternehmen mit mehr als 5 festangestellten Mitarbeitern.
– Auftragsdatenverarbeitung ohne juristisch Prüfung und rechtskonforme Regelung.
– Verstoß gegen Prüfpflichten bei Auftragsdatenverarbeitung.

9 In der juristischen Interpretation wird Cloud Computing primär als klassische Auftragsverarbeitung nach BDSG §11 eingestuft.

4.4.2.6 Keine oder unzureichende Regelung zu Aufbewahrungsdauer, -umfang, -methoden und Zugriffsregelungen von Informationen

Im Betrieb des SMGW Admin werden zahlreiche Informationen bezogen, erhoben, generiert und verarbeitet. Zur Gewährleistung eines geregelten Geschäftsbetriebs muss eine Teilmenge dieser Informationen über eine zu bestimmende Dauer mittels einer dem Schutzbedarf der Informationen gerechten Methode aufbewahrt werden. Die Technische Richtlinie bestimmt lediglich implizit für einige Detailinformationen eine Aufbewahrungsdauer.

Wenn dem SMGW Admin im Geschäftsbetrieb notwendige Informationen im erforderlichen Umfang nicht mehr zur Verfügung stehen, kann der ordnungsgemäße Betrieb nicht mehr gewährleistet werden.

Sollten die Aufbewahrungsmethoden nicht ausreichend auf Aufbewahrungsdauer, -umfang und informationsspezifische Verfügbarkeitsanforderungen abgestimmt sein, ist der ordnungsgemäße Betrieb ebenfalls gefährdet.

Sind Zugriffsregelungen gegenüber aufbewahrten Informationen nicht ausreichend restriktiv umgesetzt, sind die aufbewahrten Informationen mindestens im Schutzziel Vertraulichkeit gefährdet. Fallspezifisch kann zusätzlich das Schutzziel Integrität und Verfügbarkeit gefährdet sein.

Beispiele relevanter Informationen:

- Zertifikate
- Empfangene / Gesendete Nachrichten
- Änderungshistorie
- Profilinformationen
- Bekannte SMGW Zustände
- E-Mails

4.4.2.7 Keine oder unzureichende Regelungen zur Löschung und Vernichtung von Daten

Sollte die in der Bedrohung „Keine oder unzureichende Regelung zu Aufbewahrungsdauer, -umfang, -methoden und Zugriffsregelungen von Informationen“ (Kapitel 4.4.2.6) behandelte Aufbewahrungsdauer von Informationen überschritten werden ohne diese restriktiv zu löschen, ist die Vertraulichkeit unnötig gefährdet. Zudem werden unnötig technische und personelle Ressourcen an die Aufbewahrung gebunden.

Sobald die Aufbewahrungsdauer überschritten wurde und damit einhergehend das Schutzziel der Verfügbarkeit und Integrität entfällt, verbleibt das Schutzziel der Vertraulichkeit. Sollten die Daten nicht angemessen geregelt vernichtet werden ist die Vertraulichkeit verbleibender oder rekonstruierbarer Informationen gefährdet.

4.4.2.8 Ungesicherte Betriebsdaten

Gemäß der Technischen Richtlinie müssen vom SMGW Admin alle für den Betrieb erforderliche Daten (Betriebsdaten[10]) vorgehalten werden. Die Betriebsdaten sind den nachfolgend aufgeführten generischen Bedrohungen ausgesetzt und müssen entsprechend ihres bestimmten Schutzbedarfs angemessen geschützt werden:

- Betriebsdaten werden unberechtigt oder unbeabsichtigt offen gelegt
- Betriebsdaten werden unberechtigt oder unbeabsichtigt gelöscht

10 Hierzu zählen mindestens die Betriebsinformationen zu den SMGW (siehe 4.3.2.4), sämtliche Log-Daten beim SMGW Admin und alle weiteren Assets vom Objekt Typ „Daten“.

– Betriebsdaten werden unberechtigt oder unbeabsichtigt verändert

4.4.2.9 Ungesicherte Kommunikationsverbindungen

Gemäß der Technischen Richtlinie werden vom SMGW Admin Kommunikationsverbindungen zu berechtigen EMT, SMGW und der PTB gehalten. In konkretisierter Ausgestaltung der Funktion SMGW Admin sind, neben den in den Anwendungsfällen benannten, weitere Kommunikationsverbindungen denkbar.

Beispielsweise:

– SMGW Admin interne Kommunikationsverbindungen
– E-Mail Kommunikationsverbindungen
– Kommunikationsverbindungen mit Hersteller der SMGW Admin Software
– Kommunikationsverbindungen mit Support Unternehmen

Alle über diese Kommunikationsverbindungen transportierten Daten sind den nachfolgend aufgeführten generischen Bedrohungen ausgesetzt und müssen entsprechend ihres bestimmten Schutzbedarfs angemessen geschützt werden:

– Auslesen der transportieren Daten
– Manipulation der transportierten Daten
– Unterdrückung der transportierten Daten
– Einschleusen von Daten in die transportierten Daten (inklusive der besonderen Ausprägung „Replay-Attacken“)

4.4.2.10 Fehlplanung und/oder mangelhafte Anpassung der Planung im Betrieb

Wenn organisatorische Abläufe, die direkt oder indirekt der Informationsverarbeitung dienen, nicht sachgerecht gestaltet sind, kann dies zu Sicherheitsproblemen führen. Obwohl jeder einzelne Prozessschritt korrekt durchgeführt wird, kommt es oft zu Schäden, weil Prozesse insgesamt fehlerhaft definiert sind.

Eine weitere mögliche Ursache für Sicherheitsprobleme sind Abhängigkeiten mit anderen Prozessen, die selbst keinen offensichtlichen Bezug zur Informationsverarbeitung haben. Solche Abhängigkeiten können bei der Planung leicht übersehen werden und dadurch Beeinträchtigungen während des Betriebes auslösen.

Sicherheitsprobleme können außerdem dadurch entstehen, dass Aufgaben, Rollen oder Verantwortung nicht eindeutig zugewiesen sind. Unter anderem kann es dadurch passieren, dass Abläufe verzögert, Sicherheitsmaßnahmen vernachlässigt oder Regelungen missachtet werden.

Gefahr besteht auch, wenn Geräte, Produkte, Verfahren oder andere Mittel zur Realisierung der Informationsverarbeitung nicht sachgerecht eingesetzt werden. Die Auswahl eines ungeeigneten Produktes oder Schwachstellen beispielsweise in der Anwendungsarchitektur oder im Netzdesign können zu Sicherheitsproblemen führen.

Beispiele für Fehlplanung oder fehlende Anpassungen sind:

– Mangelhafte Einsatzplanung SMGW Admin Fachpersonal.

- Betriebsausfall durch Ausfall WAN Anbindung, Kommunikationsverbindung zwischen EMT und SMGW Admin oder Kommunikationsverbindung zwischen SMGW Admin und PTB ohne geplante Handlungsalternativen.
- Betriebsausfall durch Wartungsfenster.
- Betriebsausfall durch fehlerhaftes Update einer Softwarekomponente.
- Engpässe in SMGW Software-Aktualisierung durch Fehlplanung erforderlicher WAN Bandbreite .
- Betriebsbehinderungen durch Fehlplanung in erforderlicher System und Application Performance.
- Betriebsausfälle durch unzureichende Skalierfähigkeit der SMGW Admin Software.
- Betriebsausfälle ohne Wiederanlaufplan.
- Die PTB Anbindung muss mit ausreichend Bandbreite während der Geschäftstätigkeit des SMGW Admin verfügbar sein. Ein Ausfall der PTB Anbindung während der zyklisch oder termingesteuerten Zeitsynchronisation kann zu einer Abweichung gegenüber der gesetzlichen Zeit führen die außerhalb der in [BSI TR-03109-1] Kapitel 3.2.6 definierten Grenzen liegt.
- Die WAN Anbindung muss mit ausreichend Bandbreite während der Geschäftstätigkeit des SMGW Admin verfügbar sein. Ein Ausfall der WAN Anbindung würde sämtliche Kommunikationsverbindungen mit SMGW verhindern und daraus resultierend für die Dauer des Ausfalls keinen Betrieb des Kerngeschäfts ermöglichen. Sollte die Bandbreite gegenüber der zur Übertragung anstehenden Datenmenge nicht ausreichend dimensioniert sein, sind Engpässe in der Datenübertragung zu erwarten. Abhängig vom Ausmaß der Engpässe können bestehende Verbindungen ein Timeout erfahren und terminieren. Anstehende Verbindungen und Datenübertragungen können nur über Warteschlangen abgearbeitet werden und der Betrieb des Kerngeschäfts behindern. Wenn das Datenvolumen in Warteschlangen der SMGW und des SMGW Admin über einen längeren Zeitraum die verfügbare Bandbreite überschreiten, ist ein Betrieb des Kerngeschäfts bis zum Abbau der Warteschlangen nur partiell oder gar nicht möglich.

4.4.2.11 Qualifikation des eingesetzten Personals nicht ausreichend

Fehlende Qualifikationen des eingesetzten Personals kann die Schutzziele der verarbeiteten Informationen gefährden. Neben dem SMGW Admin Fachpersonal, dass die Anwendungsfälle umsetzt, umfasst die Bedrohung auch Personal das zur Einrichtung und Aufrechterhaltung der erforderlichen Infrastruktur beiträgt.

Beispiele für ein von der Bedrohung gefährdetes Personal sind:

- Fachpersonal SMGW Admin
- IT Fachkräfte
- Reinigungskräfte
- Personal von Wartungsfirmen
- usw.

Beispiele für unzureichende Qualifikationen sind:

- Vertrauenswürdigkeit nicht gewährleistet.
- Mangelhafte Akzeptanz von Informationssicherheit.
- Informationssicherheit gefährdender Umgang mit Infrastrukturen oder Informationen.
- Fachliche Kenntnisse zur Erfüllung der Arbeitsaufgabe ist nicht ausreichend.

4.5 Mindest-Maßnahmen

Ausgehend von den spezifischen Bedrohungen als auch den übergreifenden Bedrohungen des Kapitel 4.4 „Bedrohungen“, werden in diesem Kapitel mehrere Mindest-Maßnahmen definiert, die Vorgaben für die individuelle und ganzheitliche Sicherheitskonzeption bestimmen.

Die vorgegebenen Mindest-Maßnahmen sind primär auf eine breite Abdeckung zu erwartender IT-Landschaften ausgerichtet, sollen ein vergleichbares Sicherheitsniveau garantieren und bereits die Mindestvorgaben zu den Schutzzielen (gemäß Kapitel 4.3) stützen, indem den meisten Bedrohungen (gemäß Kapitel 4.4) reduzierend entgegengewirkt wird. Die Vorgaben sind an einer Kompatibilität gegenüber IT-Grundschutz und ISO/IEC 27001 ausgerichtet.

Gemäß normativer Regelungen des Kapitel 4.1 („Informationssicherheitsmanagementsystem“) muss das ISMS eines SMGW Admin die vollständige Ausgestaltung individuell geeigneter Maßnahmen übernehmen. Dazu gehört sowohl die Konkretisierung der hier definierten Mindest-Maßnahmen als auch ggf. die Einführung zusätzlicher Maßnahmen (z.B. gemäß ISO/IEC 27019).

4.5.1 Dokumentation von Prozessabläufen und Verantwortlichkeiten

In der Ausgestaltung eines SMGW Admin werden, neben den Anwendungsfällen und Betriebsprozessen eines SMGW Admin nach Technischer Richtlinie, eine Vielzahl individueller und konkretere Prozessabläufe eingeführt werden.

Alle Prozessabläufe müssen mit definierten Verantwortlichkeiten in ihrer konkreten Ausgestaltung vollständig dokumentiert und den Mitarbeitern als verbindlich einzuhaltende Handlungsanweisung deklariert werden.

Die Dokumentation muss in Art und Umfang mindestens geeignet sein:

- Eine verbindliche Handlungsanweisung an die jeweiligen Prozessverantwortlichen vorzugeben.
- Einem Auditor nach Kapitel 5 („Auditierung und Zertifizierung“) die Prozesssicherheit nachzuweisen.
- Die Aufrechterhaltung der Informationssicherheit (nach Kapitel 4.5.16) zu stärken.

Die Dokumentation ist regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu vermeiden und, soweit möglich, aufzulösen. Die Dokumentation und seine ggf. vorhandenen Teildokumente muss ein Erstellungsdatum (oder eine Versionsnummer) sowie eine Änderungshistorie enthalten.

4.5.2 Sensibilisierung der Mitarbeiter

In einem Sensibilisierungskonzept müssen Maßnahmen bestimmt werden, die geeignet sind, die Akzeptanz von Sicherheitsmaßnahmen zu steigern. Allen Mitarbeitern ist das Kernverständnis zu vermitteln, dass geltende Sicherheitsmaßnahmen Bestandteil der Arbeit und Arbeitsabläufen sind, da dem SMGW Admin eine wichtige und zugleich sensible Rolle im intelligenten Messsystem zufällt.

Das Sensibilisierungskonzept muss schriftlich dokumentiert sein und geeignete fortwährende als auch regelmäßige Sensibilisierungsmaßnahmen benennen.

4.5.3 Inferenzprävention

Zum Schutz personenbezogener und anderer vertraulicher Daten eines SMGW Admin ist grundsätzlich jedem Benutzer maximal nur der Zugriff auf diejenigen Daten zu gestatten, die für seine Tätigkeiten

notwendig sind (siehe auch Kapitel 4.5.4 „Rollen- und Rechtekonzept“). Alle anderen Informationen sind ihm nachhaltig zu verbergen.

Bei statistischen und pseudonymisierten Daten gilt es zu verhindern, dass aus Kenntnis über die Daten selbst und ggf. ergänzenden Daten auf spezifische vertrauliche Eigenschaften geschlossen werden kann.

Geeignete Techniken der Inferenzprävention inklusive unterdrückter[11] und verzerrender Inferenzprävention[12] sind anzuwenden.

4.5.4 Rollen- und Rechtekonzept

Es muss ein Rollen- und Rechtekonzept entwickelt und dokumentiert werden, das den Grundsätzen einer Funktionstrennung genügt und nur berechtigten Personen einen Zugriff erlaubt. Das Konzept muss des Weiteren bestimmen, welche Rollen in einer konkreten Abbildung nicht in einer Person und/oder in einem Bereich vereint werden dürfen (Rollenausschlüsse). Das Konzept muss mindestens Zutritts-, Zugangs- und Zugriffsberechtigungen abdecken.

Im Konzept muss die signifikant reduzierende Wirkung gegenüber Missbrauchsmöglichkeiten mindestens in den folgenden Bereichen nachgewiesen werden:

- Fachanwender in SMGW Admin Software Frontend
- Administratoren und Datenbankadministratoren der SMGW Admin Software
- Systemadministration in segmentierten Netzen (gemäß Kapitel 4.5.10 „Netzsegmentierung und -trennung“)

4.5.5 Regelungen zur Vorhaltezeit und Aufbewahrungsdauer von Daten

Zu jeder Datenart muss deren typisierte Datenquelle sowie sämtliche Aufbewahrungsgründe analysiert und dokumentiert werden. Anhand der Aufbewahrungsgründe sind erforderliche Vorhaltezeiten (in produktiver Betriebsumgebung) sowie Aufbewahrungsdauer (in Archivierung) begründet abzuleiten und in der Dokumentation zu ergänzen. Die Vorhaltezeit sowie Aufbewahrungsdauer muss sich an dem Grundsatz der Datensparsamkeit und Datenvermeidung orientieren.

Eventuell bestehende Vorgaben zur Aufbewahrungsdauer sind zu dokumentieren und zu beachten.

4.5.6 SMGW Admin Software und Frontend SMGW Admin Software

4.5.6.1 Produktauswahl

Die Produktauswahl muss nach einer strukturierten, rationalen und systematischen Vorgehensweise erfolgen. Im IT-Ressourcen-Management, als Teilgebiet der Softwaretechnik, sind geeignete internationale Standards[13] bekannt.

Die funktionalen Anforderungen müssen mindestens die sich aus der Technischen Richtlinie ergebenden Leistungsmerkmale abdecken und sollten um spezifische Anforderungen des SMGW Admin ergänzt werden.

Die nichtfunktionalen Anforderungen müssen mindestens in den nachfolgend aufgeführten Klassen angemessen bestimmt werden und sollten um spezifische Anforderungen des SMGW Admin ergänzt werden:

11 Unterdrückte Inferenzprävention bezeichnet den Zugriff auf Informationen zu verhindern, aus deren Zusammenführung mit anderen verfügbaren Informationen, eine Rekonstruktion schutzbedürftiger Informationen möglich wäre.

12 Verzerrende Inferenzprävention bezeichnet eine einheitlich kontrollierte Verzerrung verfügbarer Informationen (z.B. kontrolliertes Runden von Werten in Statistiken).

13 Beispielsweise ISO/IEC 25000

- Sicherheit (inkl. Sicherheit im Umgang mit Kryptomaterial)
- Korrektheit
- Skalierbarkeit
- Zuverlässigkeit (insbesondere in Systemreife, Wiederherstellbarkeit und Fehlertoleranz)
- Leistung und Effizienz
- Wartbarkeit
- Aktualisierbarkeit
- Testbarkeit während Software-Abnahme und Freigabe-Verfahren (siehe Kapitel 4.5.6.2 „Software Abnahme- und Freigabeverfahren“)

Die Anwendung nach Vorgehensmodell muss derart dokumentiert werden, dass die Produktauswahl auch nachträglich im Rahmen eines Audit methodisch und im Entscheidungsergebnis verifiziert werden kann.

4.5.6.2 Software Abnahme- und Freigabeverfahren

Es muss ein dokumentiertes Software Abnahme- und Freigabeverfahren etabliert werden, welches nach der Erstbeschaffung als auch bei jeder Softwareaktualisierung anzuwenden ist. Die Software darf in der Produktionsumgebung nur nach bestandenem Abnahme- und Freigabeverfahren installiert und genutzt werden.

Die Dokumentation des Verfahrens muss mindestens die folgenden Aspekte regeln:

- Welche Testinfrastruktur jeweils genutzt wird,
- Welche Testdatensätze, die keinen Produktivdaten entsprechen dürfen, genutzt werden,
- Welche Test und Testfälle funktionaler Art angewandt werden,
- Welche Integrationstests, sofern jeweils möglich, angewandt werden,
- Wie die Durchführung des Abnahme und Freigabeverfahrens erfolgt,
- Wie die Dokumentation der Durchführung erfolgt,
- Nach welchen Erfüllungskriterien die Software in den Betrieb übernommen werden darf.

Des Weiteren muss das Verfahren die Behandlung von Sicherheitsupdates berücksichtigen. Sicherheitsupdates sollen einerseits bestehende Sicherheitslücken in genutzter Software schließen, andererseits dürfen Softwarefehler in Sicherheitsupdates nicht zu einem höheren Schaden führen. Zu diesem Detailaspekt muss die Dokumentation die folgenden Aspekte regeln:

- Wann eine Softwareaktualisierung einem Sicherheitsupdate entspricht,
- Wann eine Softwareaktualisierung einem kritischen Sicherheitsupdate entspricht[14],
- Welche verkürzten Software Abnahme- und Freigabeverfahren existieren und wann sowie wie diese jeweils angewandt werden,
- Welche Rolle(n) des SMGW Admin in individuelle Entscheidungen eingebunden werden und wie deren Entscheidung dokumentiert wird.

14 Gemeinhin, wenn der Schutzbedarf mindestens eines als 'höher' klassifizierten Assets - durch verzögerte Übernahme der Softwareaktualisierung – erheblich gefährdet wäre und das resultierende Risiko gemäß individuellen Risikomanagement als nicht tragbar eingestuft wurde.

4.5.6.3 Nutzungsort der SMGW Admin Software Frontend

Die Benutzeroberfläche der SMGW Admin Software darf ausschließlich auf/von IT-Systemen genutzt werden, die sich seit ihrer Installation unterbrechungsfrei an einem Betriebsort des SMGW Admin befinden, fortwährend einem Zugangs- und Zutrittsschutz gegenüber Unberechtigten erfuhren und ausschließlich am zu diesem Zweck bestimmten Teilnetz (Definition gemäß Kapitel 4.5.10 „Netzsegmentierung und -trennung“) angeschlossen waren und sind.

Die Nutzung der Benutzeroberfläche einer SMGW Admin Software an einem häuslichen Arbeitsplatz ist zu untersagen. Mobile Geräte dürfen ausschließlich stationär innerhalb der vom ISMS erfassten Betriebsorte des SMGW Admin genutzt werden.

4.5.6.4 Erstellung eines Datenbanksicherheitskonzeptes

Zur Gewährleistung der Schutzziele der am SMGW Admin verarbeiteten Daten muss ein Datenbanksicherheitskonzept erstellt werden, in dem Sicherheitsaspekte bei der Planung, Installation, Konfiguration, Betrieb, Migration und Deinstallation beschrieben sind.

Im Konzept müssen mindestens Aussagen darüber getroffen werden,

- wie unberechtigte Zugänge und Zugriffe ausgeschlossen werden,
- wie die Abgrenzung der Zugangs- und Zugriffsrechte zwischen Datenbankadministration und Anwendungsadministration erfolgt (siehe auch Kapitel 4.5.4 „Rollen- und Rechtekonzept“),
- wie eine Umgehung der Zugangs- und Zugriffsrechte verhindert wird,
- wie die Speicherung der Daten und gegebenenfalls Spiegelung der Datenbank erfolgt,
- wann und wie die Datensicherung erfolgt (siehe auch Kapitel 4.5.1 „Dokumentation von Prozessabläufen und Verantwortlichkeiten“),
- wie der Schutzbedarf der Daten in Datenbank und Datensicherung gewährleistet wird,
- welche Mechanismen zur Überwachung und Kontrolle der Datenbankaktivitäten eingesetzt werden und
- wie die Datenbankkapazität überwacht wird.

4.5.6.5 Sicherstellung der Integrität

Der SMGW Admin muss die Integrität der SMGW Admin Software und seiner Komponenten sicherstellen.

Dem SMGW Admin wird empfohlen die fortwährende Prüfung auf Integrität bereits als funktionale Anforderung während der Produktauswahl (siehe Kapitel 4.5.6.1 „Produktauswahl“) aufzunehmen. Andernfalls muss der SMGW Admin durch geeignete Maßnahmen die Integrität fortwährend prüfen.

Die Integrität der SMGW Admin Software und seiner Komponenten muss der SMGW Admin jederzeit nachweisen können. Die Behandlung von Integritätsverletzungen sind in den Prozessabläufen nach Kapitel 4.5.1 „Dokumentation von Prozessabläufen und Verantwortlichkeiten“ zu dokumentieren.

4.5.6.6 Prozessfreigabe

Der SMGW Admin muss in seiner Sicherheitskonzeption berücksichtigen, dass eine Vielzahl an Prozessen, zum Teil mit Abhängigkeit von der Anzahl betroffener SMGW, eine beträchtliche Schadwirkung entfalten können.

In einem Dokument, empfohlen wird die Sicherheitskonzeption, muss bestimmt und plausibel begründet werden, in welchen Prozessen eine Prozessfreigabe nach einem 4 Augen Prinzip erfolgen muss und welche Prozessfreigaben weitere, darüber hinausgehende Maßnahmen verlangen.

Die getroffene Regelung muss in die Prozessdokumentation (siehe Kapitel 4.5.1 „Dokumentation von Prozessabläufen und Verantwortlichkeiten“) eingearbeitet sein und umgesetzt werden. Die getroffene Regelung muss konform zum Rollen- und Rechtemodell (siehe Kapitel 4.5.4 „Rollen- und Rechtekonzept“) ausgearbeitet sein. Jede Prozessauslösung sowie -freigabe nach dieser Regelung muss im SMGW Admin-Log protokolliert werden.

4.5.6.7 Protokollierung von Zugriffen, Aktivitäten und Ereignissen

Ergänzend zum SMGW Admin-Log (siehe Kapitel 3.4.4 „Führen eines SMGW Admin-Logs“) müssen Zugriffe auf Daten, Aktivitäten sowie Ereignisse protokolliert werden.

Mit der Protokollierung wird eine nachträgliche Erkennung z.B. der folgenden Ereignisse ermöglicht :

- Vertraulichkeits- bzw. Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer,
- fehlerhafte Administration von Zugangs- und Zugriffsrechten,
- Ausschalten des Servers im laufenden Betrieb,
- Verstoß gegen rechtliche Rahmenbedingungen,
- defekte Datenträger,
- Verlust gespeicherter Daten,
- unerwarteter Verbindungsabbruch,
- Datenverlust bei erschöpftem Speichermedium,
- Manipulation an Daten oder Software,
- unberechtigtes Kopieren von Daten,
- Manipulation eines Kryptomoduls,
- Kompromittierung kryptographischer Schlüssel und
- unberechtigtes Überschreiben oder Löschen von Daten.

Der Umfang der Protokollierung richtet sich einerseits nach den Anforderungen an die Nachvollziehbarkeit von Ereignissen/Änderungen und Authentizität der gespeicherten Daten. Andererseits müssen sowohl Vorgaben der Technischen Richtlinie als auch die organisationsintern abgestimmten Regelungen, z. B. zum Datenschutz, beachtet werden.

Sofern möglich, sollten mindestens folgende Daten protokolliert werden:

- Datum und Uhrzeit des Zugriffs in einer einheitlichen Zeitzone,
- Clientsystem, von dem aus zugegriffen wurde,
- Benutzer und ausgeübte Benutzerrolle,
- eingesehene Daten,
- ausgeführte Aktionen sowie
- eventuelle Fehlermeldungen und -codes.

Die Zeitdauer der Aufbewahrung der Protokolldaten ist im Sicherheitskonzept festzulegen und muss mindestens 6 Monate umfassen.

Die Protokolldaten müssen unter Beachtung organisationsinterner Vorgaben regelmäßig ausgewertet werden, um Missbrauch und Systemfehler zu erkennen. Die Auswertung kann manuell oder mit Unterstützung eines Tools erfolgen. Im Vorfeld sollten kritische Ereignisse definiert werden, also solche, bei

deren Auftreten eine Rolle gemäß Rollenkonzept (siehe Kapitel 4.5.4 „Rollen- und Rechtekonzept“) zu benachrichtigen ist. Solche Vorfälle sollten umgehend signalisiert werden, z. B. unter Nutzung vorhandener Systemmanagement-Umgebungen. Außerdem ist es wichtig, dass die Benachrichtigung rollenbezogen, nicht personenbezogen erfolgt.

Folgende Ereignisse weisen beim SMGW Admin typischerweise eine hohe Kritikalität auf und sollten daher permanent protokolliert, überwacht und bei Auftreten umgehend signalisiert werden:

- Unberechtigte Anmelde- und Zugriffsversuche,
- Manipulationsversuche gegenüber Daten, Software oder funktionalen Prozessabläufen,
- Zugriffsversuche auf private Schlüssel,
- Fehler oder Probleme in funktionalen Prozessabläufen (inkl. den Anwendungsfällen und Betriebsprozessen eines SMGW Admin nach Technischer Richtlinie),
- Ausfall von Anbindungen,
- Ausfall von Diensten,
- Systemfehler und Timeouts,
- Katastrophenszenarien (Brand, unzulässige Temperatur, Wasser etc.), die in der Regel durch externe Sensorik gemeldet werden.

Nach der Signalisierung muss das Ereignis sofort geprüft und gegebenenfalls weiter eskaliert werden.

4.5.7 Regelungen für Wartungs- und Reparaturarbeiten

4.5.7.1 Wartungs- und Reparaturarbeiten im Haus

Für Wartungs- und Reparaturarbeiten im Hause, vor allem wenn sie durch Externe durchgeführt werden, sind Regelungen über deren Beaufsichtigung zu treffen: während der Arbeiten muss eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit keine unautorisierten Handlungen vollzogen wurden und der Wartungsauftrag im vereinbarten Umfang ausgeführt wurde.

Als Maßnahmen vor und nach Wartungs- und Reparaturarbeiten sind mindestens vorzusehen:

- Wartungs- und Reparaturarbeiten sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden. Falls erforderlich, sind Speichermedien vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung), insbesondere wenn die Arbeiten extern durchgeführt werden müssen. Falls das Löschen nicht möglich ist (z. B. aufgrund eines Defektes), sind die Arbeiten auch extern zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen und vertrauenswürdige Firmen auszuwählen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind, je nach "Eindringtiefe" des Wartungspersonals, ggf. Passwortänderungen sowie weitere einsatzspezifisch risikomindernde Maßnahmen erforderlich.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (mindestens in Umfang, Ergebnisse, Zeitpunkt, Firmenname sowie eventuell Name des Wartungstechnikers).

- Beauftragte Firmen müssen schriftlich zusichern, dass sie einschlägige Sicherheitsvorschriften und Richtlinien beachten.

Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Komponente zu überprüfen. Eventuell sind zu Testzwecken vorgenommenen Eingriffe zurückzunehmen.

4.5.7.2 Externe Wartungs- und Reparaturarbeiten

Werden IT-Systeme zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher physikalisch zu löschen. Ist dies nicht möglich, weil aufgrund eines Defekts nicht mehr auf die Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen Informationssicherheitsmaßnahmen zu verpflichten.

Mittels einer Vertraulichkeitsvereinbarung, als Vertragsbestandteil, sind wirksame Vereinbarungen zur Gewährleistung der Geheimhaltung eventuell zugreifbarer Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden.

Bei der Durchführung externer Wartungsarbeiten muss protokolliert werden, welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden, wer dies veranlasst hat, was der Wartungs- bzw. Reparaturauftrag umfasst, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann ein Gerät wieder zurückgebracht wurde.

Beim Versand oder Transport der zu reparierenden Komponenten muss darauf geachtet werden, dass Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf den IT-Systemen noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z. B. in verschlossenen Behältnissen und/oder durch Kuriere. Weiterhin müssen Nachweise über den Versand (Reparaturauftrag, Begleitzettel, Versandscheine) und den Eingang beim Empfänger (Empfangsbestätigung) geführt und archiviert werden.

Komponenten, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung, alle oder einige Passwörter entweder bekannt gegeben oder auf festgelegte Einstellungen wie "REPARATUR" gesetzt werden, damit die Wartungstechniker auf die Komponenten zugreifen können.

Nach der Rückgabe der IT-Systeme oder Komponenten sind diese auf Vollständigkeit und – soweit möglich – auf Integrität zu überprüfen. Alle Passwörter sind zu ändern. Alle Dateien oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

4.5.7.3 Wartungs- und Reparaturarbeiten durch Remote Zugriff

Wartungs- und Reparaturarbeiten durch Remote Zugriff externer Dritte müssen auf das minimal erforderliche Maß reduziert werden und sind zeitlich zu begrenzen.

In einem Dokument, empfohlen wird die Sicherheitskonzeption, muss bestimmt und plausibel begründet werden, in welcher Situation Wartungs- und Reparaturarbeiten durch Remote Zugriff mit welcher Zielstellung und unter welchen risikominimierenden Rahmenbedingungen erfolgen dürfen.

Ferner sind in diesem Dokument für die genannten Situationen mindestens die nachfolgend aufgeführten Aspekte zur Realisierung zu beantworten:

- Welche Firmen sind zulässig?
- Wie werden die vergleichbaren Ansprüche an eine Wartung im Haus (siehe Kapitel 4.5.7.1 „Wartungs- und Reparaturarbeiten im Haus“) erfüllt?
- Wie wird die Authentizität der fernwartenden Personen/Beteiligten gewährleistet?

- Wie erfolgt eine Beaufsichtigung und Protokollierung der Tätigkeiten?
- Wie wird die Vertraulichkeit vertraulicher Daten gewährleistet?
- Wie wird die Integrität von Daten und Komponenten gewährleistet?
- Wie wird ein Zugriff außerhalb der vereinbarten Dauer durch physikalische Trennung unterbunden?
- Welche ergänzenden Sicherheitsmaßnahmen werden ergriffen?
- Welches Restrisiko besteht?

Die getroffene Regelung muss in die Prozessdokumentation (siehe Kapitel 4.5.1 „Dokumentation von Prozessabläufen und Verantwortlichkeiten“) eingearbeitet sein und umgesetzt werden.

4.5.8 Entwicklung und Umsetzung eines Anbindungskonzeptes

Um den Anforderungen bezüglich Verfügbarkeit (auch Bandbreite und Performance), Vertraulichkeit und Integrität zu genügen, muss der Aufbau, die Änderung bzw. die Erweiterung einer Netzanbindung des SMGW Admin sorgfältig geplant und mit Produktivbetrieb umgesetzt werden. Hierzu dient die Erstellung eines Anbindungskonzeptes für die Anbindung an externe Netze sowie deren anschließende Umsetzung.

Im Konzept müssen mindestens Aussagen darüber gemacht werden,

- welche Kommunikationsbeziehungen zu welchen Zweck benötigt werden,
- welchen Einschränkungen benötigte Kommunikationsbeziehungen aus der Anbindung unterliegen können und wie das resultierende Risiko in Schaden und Eintrittswahrscheinlichkeit im Betrieb minimiert wird,
- wie die Schutzziele der Anbindung gewährleistet werden,
- wie ein Verlust des Schutzziel „Verfügbarkeit“ zeitnahe identifiziert werden kann,
- ob und - wenn ja - wie eine redundante Anbindung erzielt wird,
- wie unerwünschte Kommunikationsbeziehungen über die Netzanbindung wirksam verhindert werden,
- wie das eigene, als auch das angebundene Netz, voreinander geschützt wird und
- wie die Netzanbindung im Betrieb gemanagt wird.

4.5.9 Einsatz Zeitserver mit gesetzlicher Zeit

Die Verfügbarkeit des Zeitservers beim SMGW Admin und der darauf laufenden Dienste müssen so ausgelegt sein, dass die Anforderungen der TR-03109-1 zur Synchronisation der zu administrierenden SMGW mit diesem Zeitserver gewährleistet werden können.

Eventuelle weitere Vorgaben befinden sich derzeit in Abstimmung mit der PTB.

4.5.10 Netzsegmentierung und -trennung

IT-Systeme sind typischerweise in lokale Netze (LANs) integriert, die ihrerseits wieder mit anderen Netzen verbunden sind. Allein aus technischen Gründen ist es bei mittleren und größeren Netzen meist erforderlich, ein LAN in mehrere Teilnetze aufzuteilen, beispielsweise weil die Anzahl der IT-Systeme pro Teilnetz oder die Gesamtlänge der Verkabelung beschränkt ist.

Die Bildung von Teilnetzen am SMGW Admin ist bereits aus Gründen der Informationssicherheit notwendig. Einerseits können sensitive Daten auf bestimmte Bereiche innerhalb des LANs begrenzt werden (Vertraulichkeit), andererseits kann verhindert werden, dass Störungen in oder Angriffe auf ein Teilnetz die Funktionsfähigkeit anderer Teilnetze beeinträchtigen (Integrität und Verfügbarkeit).

Diese Netzsegmente müssen insbesondere die Vertraulichkeitsanforderungen der verarbeiteten Daten sowie die Integritätsanforderungen der darin genutzten Software durch technische und organisatorische Maßnahmen stützen. Erforderlich ist mindestens ein physikalischer Zugangs- sowie technischer Zugriffsschutz als auch der Verzicht auf Funk basierender Netze (z.B. WLAN).

IT-Systeme auf denen die Benutzeroberfläche einer SMGW Admin Software (siehe Kapitel 4.5.6.3) betrieben werden, müssen in einem[15] eigenen Teilnetz betrieben werden. Dieses Teilnetz darf gegenüber anderen Teilnetzen nur die minimal notwendigen und zu begründenden Netzkoppelungen und Kommunikationsbeziehungen aufweisen. Erwartet wird lediglich eine notwendige Netzkoppelung zu zentralen Diensten einer SMGW Admin Software. Hingegen werden Kommunikationsbeziehungen zu einem zentralen E-Maildienst oder ein Internetzugang, selbst mittels Sicherheitsgateway gesichert, als nicht erforderlich eingeschätzt[16].

Zur logischen Trennung von Netzsegmenten sind Sicherheitsgateways einzusetzen, die den Datenfluss zwischen den Netzsegmenten reglementieren.

Eine Umgehung der Netzsegmentierung durch undokumentierte Verbindungen darf nicht möglich sein.

4.5.11 Integritätsschutz von IT-Systemen und IT-Komponenten

IT-Systeme und IT-Komponenten die am Transport, (Zwischen-) Speicherung oder Verarbeitung von Assets der Technischen Richtlinie beteiligt sind müssen in regelmäßigen[17] Intervallen mit geeigneten technischen und/oder organisatorischen Maßnahmen auf ihre notwendige Integrität geprüft werden.

Das Sicherheitskonzept beim SMGW Admin muss Regelungen beinhalten, wer über Integritätsverletzungen informiert werden muss und wer für die unverzügliche Wiederherstellung der notwendigen Integrität und geeignete Gegenmaßnahmen verantwortlich ist.

Eine Liste der zu prüfenden IT-Systeme und IT-Komponenten muss geführt werden. Jede Prüfung sowie deren Ergebnis ist revisionssicher zu dokumentieren.

4.5.12 Dienstsegmentierung

Viele Schwachstellen in IT-Systemen sind einzeln nicht für einen potentiellen Angreifer ausnutzbar. Häufig wird erst durch die Kombination von Schwachstellen ein erfolgreiches Eindringen in einen Rechner möglich. Resultierend aus der Bedrohungslage und dem Schutzbedarf der Dienste ist es zweckmäßig, auf einem Rechner nur einen Dienst zu betreiben. Dies betrifft vor allem Server, die Dienste gegenüber der WAN Anbindung oder sonstigen Anbindungen gemäß der Technischen Richtlinie anbieten.

Die Aufteilung kann verstärkt werden, indem für einen einzelnen Dienst verschiedene Aufgaben auf unterschiedliche Rechner verteilt werden.

Eine Aufteilung verschiedener Dienste auf unterschiedliche Rechner hat unter anderem folgende Vorteile:

- Leichtere Konfiguration der einzelnen Rechner
- Einfachere und sicherere Konfiguration eines vorgeschalteten Paketfilters
- Erhöhte Widerstandsfähigkeit gegenüber Angriffen

15 Sofern durch individuelle Gegebenheiten erforderlich können ggf. mehrere gleichartige Teilnetze erforderlich sein (z.B. bei SMGW Admin Betrieb an mehreren Betriebsstädten)

16 Der Zugriff aus diesem Teilnetz auf das Internet oder auf E-Mail-Server kann über Terminal-Server-Lösungen realisiert werden. Die Terminal-Server müssen sich dann in einem separaten Teilnetz befinden.

17 Unter „regelmäßig“ wird ein geeignetes Intervall verstanden, das in Übereinstimmung zum individuellen Schutzbedarf als auch technischen und organisatorischen Aufwand steht. Für Serversysteme mit selbst betriebenem Betriebssystem wird beispielsweise mindestens eine wöchentliche Integritätsprüfung als geeignet und angemessen angenommen.

- Erhöhte Ausfallsicherheit

Durch ein geeignetes zentrales Systemmanagement kann der zusätzliche Administrationsaufwand, der durch die höhere Anzahl der Rechner entsteht, begrenzt werden.

4.5.12.1 Virtualisierung

Im Falle von sicherheitskritischen Diensten sollten auch in virtuellen IT -Systemen jeweils nur ein Dienst betrieben werden, wie dies auch für physische Systeme gilt. Ein virtuelles IT-System selbst ist jedoch in diesem Sinne kein "Dienst" eines Virtualisierungsservers. Daher können auf einem Virtualisierungsserver mehrere virtuelle IT-Systeme betrieben werden. Je nachdem, auf welcher Virtualisierungstechnik (Server- oder Betriebssystemvirtualisierung) der Virtualisierungsserver beruht, kann allerdings die Varianz der durch die virtuellen IT-Systeme bereitgestellten Dienste eingeschränkt sein. Ob das eingesetzte Virtualisierungsprodukt geeignet ist, unterschiedliche Dienste in virtuellen IT-Systemen auf einem Virtualisierungsserver bereitzustellen, muss für das konkrete Produkt geprüft werden. Als Kriterien sind hierfür eine bestmögliche Ausprägung an Isolation und Kapselung der virtuellen IT-Systeme nach aktuellem Industriestandard auf dem Virtualisierungsserver heranzuziehen. Je stärker die virtuellen IT-Systeme auf dem Virtualisierungsserver isoliert sind, desto eher eignet sich das Virtualisierungsprodukt dazu, unterschiedliche Dienste in den verschiedenen virtuellen IT-Systemen zu betreiben. Die folgenden Grundsätze lassen sich für eine erste Beurteilung heranziehen:

– Auf Virtualisierungsservern mit einer Betriebssystemvirtualisierungslösung sollten in der Regel nur virtuelle IT-Systeme mit einer Funktion bereitgestellt werden. So sollten auf einem solchen Virtualisierungsserver beispielsweise ausschließlich Webserver oder ausschließlich Mailserver, aber keine Mischung aus diesen Gruppen betrieben werden. Bei einigen Produkten zur Betriebssystemvirtualisierung ist die Isolation der virtuellen IT-Systeme allerdings stark genug, so dass von dieser Vorgabe abgewichen werden kann.
– Auf Virtualisierungsservern mit einer Servervirtualisierungslösung ist es meist zulässig, virtuelle IT-Systeme mit unterschiedlichen Diensten zu betreiben. Es können also unter Umständen Webserver und Mailserver auf einem Virtualisierungsserver in jeweils getrennten virtuellen IT-Systemen gemeinsam bereitgestellt werden.

Auf einem Virtualisierungsserver selbst dürfen neben der Virtualisierungssoftware und damit direkt verbundener Dienste (wie Verwaltungsdienst für die Virtualisierung etc.) keine weiteren Dienste betrieben werden.

4.5.13 Einsatz eines oder mehrerer Protokollierungsserver

Im IT-Betrieb eines SMGW Admin fallen neben dem geforderten SMGW Admin-Log große Mengen verschiedener Protokollierungsinformationen der zahlreichen Komponenten der IT-Infrastruktur an.

Darunter fallen z.B.:

- Sicherheitsgateways
- Router und Switche
- Betriebssysteme
- Dienste

Um die Verfügbarkeit und Integrität lokaler Protokollierungsinformationen zu erhöhen, muss einer oder mehrere Protokollierungsserver betrieben werden, die Protokolldaten (siehe auch Kapitel 4.5.6.7 „Protokollierung von Zugriffen, Aktivitäten und Ereignissen“) der angeschlossenen Komponenten aufnehmen. Eine lokale Protokollierung auf den einzelnen Komponenten bleibt vom Einsatz eines oder mehrerer Protokollierungsserver unberührt.

Mit Inbetriebnahme des / der Protokollierungsserver ist eine Revisionssicherheit der Protokolldaten zu gewährleisten.

Damit die Protokollierungsinformationen zeitlich in einen zueinander stehenden Zusammenhang gesetzt werden können, ist Datum und Uhrzeit in einer einheitlichen Zeitzone zu nutzen.

Der Rolle eines Protokollierungsservers in der Sicherheitskonzeption folgend, darf dieser nicht für weitere Aufgaben (etwa als Auswertesystem oder Administrationsrechner) verwendet werden (siehe Kapitel 4.5.12 „Dienstsegmentierung“).

Administrative Zugriffe auf einen Protokollierungsserver dürfen ausschließlich im 4-Augen Prinzip erfolgen.

4.5.14 Penetrationstest

Ergänzend zur „Durchführung interner Prüfungen“ (Kapitel 4.5.16.3) versteht sich ein Penetrationstest als ein umfassender technischer Sicherheitstest der beim SMGW Admin genutzten IT-Systeme, IT-Infrastrukturen und Komponenten der SMGW Admin Software (Frontend als auch Backend). Ein Penetrationstest muss als empirischer Teil einer Sicherheitsanalyse über den Leistungsumfang automatischer Schwachstellenscans („Vulnerability Scan“) hinaus gehen und die folgenden Ziele verfolgen:

- Identifikation technischer Schwachstellen
- Aufdeckung potentieller Bedrohungen
- Verbesserung der Informationssicherheit auf technischer und ggf. organisatorischer Ebene

Da Penetrationstests zumeist eine Momentaufnahme darstellen, müssen sowohl regelmäßige[18] als auch anlassbezogene Durchführungen erfolgen.

Penetrationstests müssen durch BSI zertifizierte Penetrationstester erfolgen. Die zur Erreichung der oben genannten Ziele geeignete Festlegung von Informationsbasis, Aggressivität, Vorgehensweise und Ausgangspunkt(e) obliegt dem ISMS des SMGW Admin.

4.5.15 Reaktion auf Verletzung der Sicherheitsvorgaben

Es ist schriftlich festzulegen, welche Reaktion auf Verletzungen der Sicherheitsvorgaben erfolgen soll, um eine klare und sofortige Reaktion gewährleisten zu können.

Untersuchungen sollten durchgeführt werden, um festzustellen, wie und wo die Verletzung entstanden ist. Anschließend müssen die angemessenen schadensbehebenden oder -mindernden Maßnahmen durchgeführt werden. Soweit erforderlich, müssen zusätzliche schadensvorbeugende Maßnahmen ergriffen werden. Die durchzuführenden Aktionen hängen sowohl von der Art der Verletzung als auch vom Verursacher ab.

Ferner sind identifizierte Sicherheitslücken in der SMGW Admin Software oder im Frontend der SMGW Admin Software unverzüglich an das BSI zu berichten. Dabei können bereits etablierte Meldewege genutzt werden.

18 Unter „regelmäßig“ wird in diesem Dokument eine jährliche Prüfung verstanden, soweit keine erheblichen und nachvollziehbaren Gründe dagegen sprechen.

4.5.16 Aufrechterhaltung der Informationssicherheit

Ein ISMS muss nicht nur das angestrebte Sicherheitsniveau erreichen, sondern muss dieses auch dauerhaft gewährleisten. Um das bestehende Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern, müssen alle Sicherheitsmaßnahmen regelmäßig überprüft werden. Diese Überprüfung muss beim SMGW Admin intern zusätzlich unabhängig von den „Auditierung und Zertifizierung“ nach Kapitel 5 veranlasst werden.

Sowohl die korrekte Umsetzung als auch die Umsetzbarkeit eines Sicherheitskonzepts müssen regelmäßig überprüft werden. Dabei ist zu unterscheiden zwischen der Prüfung, ob bestimmte Maßnahmen geeignet und effizient sind, um die gesteckten Sicherheitsziele zu erreichen (Vollständigkeits- bzw. Aktualisierungsprüfung), und der Kontrolle, inwieweit Sicherheitsmaßnahmen in den einzelnen Bereichen umgesetzt wurden (Revision der Informationssicherheit).

Die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen müssen gemäß eines Realisierungsplans umgesetzt werden. Der Umsetzungsstatus muss dokumentiert werden. Zieltermine und Ressourceneinsatz müssen überwacht und gesteuert werden. Die Leitungsebene ist dazu regelmäßig zu informieren.

Die Überprüfungen sollten zu festgelegten Zeitpunkten, müssen jedoch im Regelfall jährlich, durchgeführt werden und können auch anlassbezogen erfolgen. Insbesondere sicherheitsrelevante Zwischenfälle, Veränderungen im technischen oder technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen bzw. Bedrohungen erfordern eine Anpassung der bestehenden Sicherheitsmaßnahmen und sollten daher zu einer anlassbezogenen Überprüfung führen. Die in den einzelnen Überprüfungen ermittelten Ergebnisse müssen dokumentiert werden und nach Bewertung im ISMS Risikomanagement ggf. zu Korrekturmaßnahmen führen.

Es sollten auch gelegentlich unangekündigte Überprüfungen durchgeführt werden, da angekündigte Kontrollen häufig ein verzerrtes Bild des Untersuchungsgegenstands ergeben.

Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Abweichungen bzw. Mängel zu erkennen . Für die Akzeptanz ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass die Kontrollen keinen ausschließlich belehrenden Charakter haben. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

4.5.16.1 Einhaltung des Sicherheitskonzeptes (Sicherheitsrevision)

Hierbei muss geprüft werden, ob Sicherheitsmaßnahmen tatsächlich so umgesetzt sind und eingehalten werden wie im Sicherheitskonzept vorgegeben. Hierbei ist auch zu untersuchen, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden und ob alle vorgesehenen Detektionsmaßnahmen (z. B. Auswertung von Protokolldateien) tatsächlich durchgeführt werden.

Dabei kann sich zeigen, dass Sicherheitsmaßnahmen nicht umgesetzt worden sind oder dass sie in der Praxis nicht greifen. In beiden Fällen sollten die Ursachen für die Abweichungen ermittelt werden. Als mögliche Korrekturmaßnahmen kommen - je nach Ursache - in Frage:

- organisatorische Maßnahmen sind anzupassen,
- personelle Maßnahmen, z. B. Schulungs- und Sensibilisierungsmaßnahmen, sind zu ergreifen oder disziplinarische Maßnahmen einzuleiten,
- infrastrukturelle Maßnahmen, z. B. bauliche Veränderungen, sind zu initiieren,
- technische Maßnahmen, z. B. Änderungen an Hardware und Software oder Kommunikationsverbindungen und Netzen, sind vorzunehmen,
- Entscheidungen des verantwortlichen Vorgesetzten (bis hin zur Leitungsebene) sind einzuholen.

Auf jeden Fall sollte für jede Abweichung eine Korrekturmaßnahme vorgeschlagen werden. Außerdem sollten auch hier der Zeitpunkt und die Zuständigkeiten für die Umsetzung der Korrekturmaßnahme festgelegt werden.

Im Vorfeld sollten aber auch die Reaktionen auf Verletzung der Sicherheitsvorgaben festgelegt werden. Es müssen angemessene Maßnahmen ergriffen werden, die dazu beitragen, dass sich Sicherheitsvorfälle nicht wiederholen. Dazu könnte beispielsweise die Einschränkung von Zugriffsrechten gehören.

4.5.16.2 Kontinuierliche Verbesserung des Sicherheitskonzeptes (Vollständigkeits- bzw. Aktualisierungsprüfung)

Das Sicherheitskonzept muss regelmäßig aktualisiert, verbessert und an neue Rahmenbedingungen angepasst werden. Es muss regelmäßig geprüft werden, ob die ausgewählten Sicherheitsmaßnahmen noch geeignet sind, die Sicherheitsziele zu erreichen. Dabei kann direkt untersucht werden, ob die eingesetzten Sicherheitsmaßnahmen effizient sind oder ob sich die Sicherheitsziele mit anderen Maßnahmen geeigneter erreichen lassen.

4.5.16.3 Durchführung interner Prüfungen

Entsprechend dem Prüfungszweck sind Umfang und Tiefe der internen Überprüfungen festzulegen. Als Grundlage für alle Überprüfungen dient das Sicherheitskonzept und die vorhandene Dokumentation des Sicherheitsprozesses.

Eine interne Überprüfung muss von Personen mit geeigneten Qualifikationen durchgeführt werden. Diese dürfen jedoch nicht an der Erstellung der Konzepte beteiligt gewesen sein, um Betriebsblindheit und Konflikte zu vermeiden. Die Prüfer bzw. Auditoren müssen möglichst unabhängig und neutral sein.

Jede Überprüfung ist sorgfältig zu planen. Alle relevanten Feststellungen und Ergebnisse sind in einem Bericht festzuhalten. Dieser sollte neben einer Auswertung auch Korrekturvorschläge enthalten. Der Bericht muss dem Leiter des überprüften Bereiches sowie dem ISMS-Verantwortlichen übergeben werden, die auf dieser Basis die weiteren Schritte konzipieren müssen. Schwerwiegende Abweichungen sollten direkt der Leitungsebene kommuniziert werden, damit ggf. notwendige weitreichende Entscheidungen zeitnah getroffen werden können. Sollten Prüftools eingesetzt werden, muss deren Nutzung genau geregelt werden.

Werden bei der Prüfung spezielle Audit- oder Diagnosewerkzeuge eingesetzt, muss ebenso wie bei der Ergebnisdokumentation sichergestellt sein, dass nur autorisierte Personen darauf Zugriff haben. Diagnose- und Prüftools sowie die Prüfergebnisse müssen daher besonders geschützt werden.

Wenn Externe an Prüfungen beteiligt sind, muss sichergestellt werden, dass keine Informationen der Institution missbräuchlich verwenden (z. B. durch entsprechende Vertraulichkeitsvereinbarungen) und dass sie nur auf die benötigten Informationen zugreifen können (z. B. durch Zugriffsrechte oder Vier-Augen-Kontrolle).

4.5.16.4 Korrekturmaßnahmen

Erkannte Fehler und Schwachstellen müssen zeitnah abgestellt werden.

Aufgrund der Überprüfungsergebnisse sind Entscheidungen über das weitere Vorgehen zu treffen. Insbesondere sind alle erforderlichen Korrekturmaßnahmen in einem Umsetzungsplan festzuhalten. Die Verantwortlichen für die Umsetzung der Korrekturmaßnahmen sind zu benennen und mit den notwendigen Ressourcen auszustatten.

4.5.17 Regelungen für den Einsatz von Fremdpersonal

Obwohl Fremdpersonal grundsätzlich zu vermeiden ist, kann Fremdpersonal erforderlich sein, wenn entsprechende personelle Ressourcen nicht im eigenen Haus vorhanden sind.

Beim Einsatz von externen Mitarbeitern muss auf jeden Fall sichergestellt sein, dass sie bei Beginn ihrer Tätigkeit - ähnlich wie eigene Mitarbeiter - in ihre Aufgaben eingewiesen werden und schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen verpflichtet werden.

Daneben sollte sichergestellt sein, dass auch für externe Mitarbeiter Vertretungsregelungen existieren.

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Es sind außerdem sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Außerdem muss der Ausscheidende explizit darauf hingewiesen werden, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt.

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu behandeln, d. h. beispielsweise dass der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von angestellten Mitarbeitern des SMGW Admin erlaubt ist.

4.5.18 Schlüsselmanagement

Die privaten Schlüssel des SMGW Admin müssen vor unbefugtem Zugriff besonders geschützt werden. Dazu müssen die privaten Schlüssel in Krypto-Modulen gespeichert werden, die den Anforderungen in [CP] Kapitel 6.2 genügen. Hierzu gehört u.A. die Aktivierung des privaten Schlüssels im 4-Augen-Prinzip[19] (Kapitel 6.2.7).

Die privaten Schlüssel müssen mindestens dreifach redundant gespeichert werden, damit ein Verlust weitestgehend ausgeschlossen werden kann. Beim Anlegen von Kopien bzw. Backups der privaten Schlüssel müssen die Vorgaben aus [CP] Kapitel 6.2.3 gewährleistet werden. Mindestens eine Kopie oder ein Backup ist räumlich getrennt aufzubewahren.

Sämtliche Datenträger, auf denen sich private Schlüssel oder Schlüsseldateien des SMGW Admin befinden, müssen vor unbefugtem Zugriff geschützt werden (hierzu zählen auch die Krypto-Module).

4.5.19 SMGW Firmware Update

Der SMGW Admin muss regelmäßig, mindestens täglich, die Verfügbarkeit neuer SMGW Firmware Updates bei genutzten Herstellern prüfen und beziehen. SMGW Firmware Updates, die der SMGW Admin vom Hersteller bezieht, müssen vom BSI freigegeben sein. Verfügbare SMGW Firmware Updates müssen ein Test- und Freigabeverfahren erfahren, das konform zu den Vorgaben nach Kapitel 4.5.6.2 („Software Abnahme- und Freigabeverfahren“) angewandt auszugestalten ist. Der SMGW Admin muss die Authentizität des SMGW Firmware Updates von Bezug beim Hersteller bis zur Einspielung in das SMGW gewährleisten.

SMGW Firmware Updates mit sicherheitsrelevanten Charakter müssen vom SMGW Admin unverzüglich eingespielt werden. Die Einspielung sonstiger SMGW Firmware Updates sind dem SMGW Admin freigestellt. Jedes durchgeführte SMGW Firmware Update ist im SMGW Admin-Log zu protokollieren.

19 [CP] Certificate Policy der Smart Metering PKI, mindestens in Version 1.0.1 vom 18.05.2015

4.5.20 Notfallkonzept

Ein dokumentiertes Notfallkonzept muss sicherstellen, dass im Fall eines Notfalls, bei der Inbetriebnahme und dem Betrieb von Ausweichlösungen und der Wiederaufnahme des Normalbetriebs der Schutzbedarf der Daten weiterhin gewährleistetet wird.

Die Notfallkonzeption ist nach dem gewählten Standard IT-Grundschutz oder ISO/IEC 27001 (siehe Kapitel 4 „Sicherheitsanforderungen an den Admin-Betrieb“) auszuarbeiten.

5 Auditierung und Zertifizierung

Die Umsetzung der in Kapitel 4 aufgeführten Mindestvorgaben bzgl. der zu betrachtenden Bedrohungen und der diesen entgegenwirkenden geeigneten und angemessenen Maßnahmen sind im Rahmen einer Auditierung durch einen Auditor zu begutachten bzw. zu prüfen und durch eine abschließende Zertifizierung des ISMS zu bestätigen.

Mit dem SMGW Admin-Betrieb existiert ein Bereich mit kritischen Anwendungen (vgl. Einleitung in Kapitel 1), so dass bei der Prüfung der Umsetzung des konkreten ISMS sowie der vorgegebenen Maßnahmen eine entsprechende Sorgsamkeit und Verantwortung notwendig ist. Deshalb sind in den folgenden Unterkapiteln besondere Rahmenbedingungen für Auditierung und Zertifizierung aufgeführt, die die allgemein bekannten Verfahren zum Teil ergänzen.

Im folgenden Kapitel 5.1 werden diese Besonderheiten in der Auditierung beschrieben. Das Kapitel 5.2 definiert anschließend die spezifischen Gegebenheiten für die Zertifizierung.

5.1 Auditierung

Die besonderen Rahmenbedingungen für die Auditierung lassen sich unterteilen in Anforderungen an die Auditoren, die das eigentliche Audit durchführen, und an spezifische Vorgaben für das Verfahren und die in diesem Verfahren zu betrachtenden Dokumente.

5.1.1 Anforderungen an die Auditoren

Die Anforderungen an Auditoren, die den Informationsverbund eines SMGW Admin gemäß des vorliegenden Dokuments auditieren sollen, sind in der „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ [VB-Personen] und dem dazugehörigen Dokument „Anforderungen an Antragsteller zur Zertifizierung als Auditor“ [Auditor] definiert. Diese sind in der jeweils aktuellen Version auf der Internetseite des BSI verfügbar. Vor Beginn eines Audits muss der Auditor für den Geltungsbereich dieser vorliegenden TR beim BSI zertifiziert sein.

Die dort aufgeführten Anforderungen gelten für alle Auditoren, unabhängig davon, ob Sie nach Grundschutz-Vorgehensweise oder auf Basis ISO/IEC 27001 arbeiten.

5.1.2 Vorgaben für das Verfahren

Die Auditierung erfolgt grundsätzlich in den zwei Phasen

- Dokumentenprüfung und

- Prüfung der Umsetzung der in der Dokumentation beschriebenen Prozesse und Maßnahmen.

5.1.3 Vorzulegende Dokumentation

Die für die Phase der Dokumentenprüfung vorzulegende Dokumentation besteht aus der individuellen Sicherheitskonzeption des zu prüfenden SMGW Admin und beinhaltet insbesondere die unter Kapitel 4.5.1 geforderten Dokumentation der internen Prozessabläufe sowie mindestens folgende Referenzdokumente:

•IT-Sicherheitsrichtlinien,
•Risikoanalyse,
•Ergebnisse der IT-Penetrationstests (siehe Kapitel 4.5.14).

Weitergehende Dokumente kann der Auditor nach seinem Ermessen nachfordern.

Die vorgelegte Dokumentation ist vom Auditor dahingehend zu prüfen, ob sie die nach dieser Technischen Richtlinie geforderten Inhalte nachvollziehbar und konsistent darstellt. Festgestellte Mängel sind vor Beginn der zweiten Phase (Prüfung der Umsetzung) zu beheben und erneut durch den Auditor zu prüfen.

5.1.4 Vorgaben für die Umsetzungsprüfung

Im Rahmen der zweiten Audit-Phase muss der Auditor zwingend die Umsetzung der geforderten und in der Dokumentation nach 5.1.3 beschriebenen Sicherheitskonzeption prüfen.

Der Auditor hat dabei insbesondere zu prüfen, ob bei der Durchführung der Risikoanalyse die in dieser Technischen Richtlinie festgelegten Assets, Schutzziele und Bedrohungen beachtet und ausreichend behandelt bzw. bewertet wurden. Diese Teilprüfung und deren Ergebnis ist explizit zu dokumentieren.

Ebenso ist während des Audits zu verifizieren, ob die normativen Vorgaben zu den Maßnahmen beachtet und angemessen umgesetzt wurden. Diese Teilprüfung und das Ergebnis ist ebenfalls explizit zu dokumentieren.

Während dieser Phase festgestellte schwerwiegende Abweichungen sind innerhalb einer vom Auditor vorgegebenen angemessenen Frist zu beheben und anschließend erneut durch den Auditor zu prüfen. Geringfügige Abweichungen sind zu kennzeichnen und innerhalb einer geeigneten Frist nachzubessern.

5.1.5 Vorgaben für die Auditberichte

Inhaltlich muss aus den Auditberichten eindeutig hervorgehen, dass die in dieser Technischen Richtlinie aufgeführten Mindestvorgaben geprüft wurden und ob sie als erfüllt angesehen werden.

Die Auditberichte müssen insbesondere die oben angegebenen Teilprüfungen nach 5.1.4 und deren Ergebnisse beinhalten. Diese dokumentierten Teilprüfungen mit den entsprechenden Ergebnissen sind vom Auditor zu unterschreiben und dem BSI vorzulegen.

5.2 Zertifizierung

Abhängig davon, ob eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz oder eine Zertifizierung nach ISO/IEC 27001 angestrengt wird, sind unterschiedliche Zertifizierungsstellen beteiligt.

Im ersten Fall ist zwingend das BSI als Zertifizierungsstelle involviert. Das geltende Zertifizierungsschema enthält alle wesentlichen Informationen für dieses Verfahren (Beantragung, Beteiligte, Audittypen, Auditbericht, Zertifikatserteilung, zeitliche Fristen, Formulare, etc.) und ist auf der Internetseite des BSI verfügbar. Die nach diesem Verfahren erteilten Zertifikate werden grundsätzlich auf den Internetseiten des BSI veröffentlicht.

Bei einer Zertifizierung nach ISO/IEC 27001 sind hingegen Zertifizierungsstellen beteiligt, die bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß ISO/IEC 27006 für ISMS akkreditiert sind. Eine Übersicht dieser Zertifizierungsstellen erhalten Sie in der Datenbank der akkreditierten Stellen auf den Internetseiten der DAkkS.

Weitere Anforderungen an die Zertifizierung sind nicht vorgesehen.

Anhang: Betriebsprozesse

Die in der TR-03109-6 genannten Anwendungsfälle des SMGW Admin (siehe Kapitel 3) lassen sich durch eine detailliertere Betrachtung ergänzen. Hierzu können zunächst die Prozesse, die bereits aus der [BSI TR-03109-1], Anlage VI, bekannt sind, herangezogen werden.
Ferner gibt es mehrere Prozesse, die in den bisherigen Unterarbeitsgruppen zur BSI TaskForce „Betriebsprozesse“ erarbeitet wurden.
Insgesamt sollen die Betriebsprozesse in der TR-03109-6 normativ sein, die aus Sicht der Informationssicherheit als kritisch anzusehen sind (z.B. Kryptoprozesse). Diese werden mit der weiteren Überarbeitung der gesamten [BSI TR-03109] konsolidiert und sollen dann hier aufgeführt werden.

Anhang: Vereinfachte tabellarische Darstellung von Mindestvorgaben zu den Schutzzielen

Ergänzend zu den Mindestvorgaben zu den Schutzzielen nach Kapitel 4.3 fasst dieser Anhang Detailangaben in tabellarischer Darstellung zusammen. Der kompakten Darstellung geschuldet, können normative Detailvorgaben fehlen.

Des Weiteren soll mit der tabellarischen Darstellung nicht der Eindruck erweckt werden, dass eine beliebige Vergleichbarkeit von Zeilen- oder Spalteninhalten stets zueinander möglich sei.

Die nachfolgende Tabelle konsolidiert die in Kapitel 4.3.1 („Übersicht“) beschriebenen Mindestvorgaben nach den Schutzzielen. Zur einfachen Verwendung in dieser Anlage wurde eine Referenzkennung eingeführt.

Referenz-kennung	**Schutzziel**			
	Verfügbarkeit	Vertraulichkeit	Integrität	Authentizität
K	Keine Mindestvorgabe	Keine Mindestvorgabe	Keine Mindestvorgabe	Keine Mindestvorgabe
S	Die Verfügbarkeit [der Daten/ der Anweisung / des Dienstes / der Anbindung] SOLL gewährleistet werden.	Die Kenntnis um [den Dateninhalt/ Inhalt und Übertragungsdetails der Anweisung] SOLL auf den spezifischen SMGW Admin beschränkt sein.	Die Integrität [der Daten / der Anweisung] SOLL gewährleistet werden.	Die Authentizität [der Daten/der Anweisung] SOLL gewährleisten werden.
M.0	Die Verfügbarkeit der Daten MUSS gewährleistet sein wenn sie benötigt werden.	Die Kenntnis um [den Dateninhalt / Inhalt und Übertragungsdetails der Anweisung] MUSS auf den spezifischen SMGW Admin beschränkt sein.	Die Integrität [der Daten / der Anweisung / des Dienst] MUSS gewährleistet werden.	Die Authentizität [der Daten/der Anweisung] MUSS mindestens in ihrer vertrauenswürdigen Echtheit gemäß Technischer Richtlinie gewährleistet werden.
M.1	Die Verfügbarkeit [der Daten / der Anweisung / des Dienst / der Anbindung] MUSS gewährleistet sein wenn und so lange sie benötigt werden.	Die Kenntnis um [den Dateninhalt / Inhalt und Übertragungsdetails der Anweisung] MUSS auf den spezifischen SMGW Admin und SOLL zweckgebunden beschränkt sein.	-	Die Authentizität [der Daten/der Anweisung] MUSS in vertrauenswürdiger und überprüfbarer Echtheit gemäß Technischer Richtlinie gewährleistet werden.
M.2	-	Die Kenntnis um den [Dateninhalt / Inhalt und Übertragungsdetails der Anweisung] MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.	-	-
M.3	-	Die Kenntnis um den Dateninhalt sowie dessen Existenz in konkreter inhaltlicher Ausprägung MUSS auf den spezifischen SMGW Admin zweckgebunden beschränkt sein.	-	-

Tabelle 111: Schutzziele und mögliche Mindestvorgaben

Die nachfolgende Tabelle konsolidiert die Angaben des Kapitel 4.3.2 („Mindestvorgaben zu den Assets“) über Mindestvorgaben zu den Schutzzielen nach Asset. Die Mindestvorgaben werden mittels der in vorheriger Tabelle eingeführten Referenzkennung angegeben.

Asset	Objekt Typ	Detail	Mindestvorgaben zu den Schutzzielen			
	Zuordnung nach Kapitel 4.3.1	Asset Kapitel	Verfügbarkeit	Vertraulichkeit	Integrität	Authentizität
Gesetzliche Zeit	Daten	4.3.2.1	M.0	K	M.0	M.0
SMGW Nachricht vom Typ Alarm	Daten	4.3.2.2	M.1	M.3	M.0	M.0
SMGW Nachricht vom Typ Benachrichtigung	Daten	4.3.2.3	M.1	M.3	M.0	M.0
Betriebsinformationen zu einem SMGW	Daten	4.3.2.4	M.1	M.2	M.0	K
SMGW Firmware Update	Daten	4.3.2.5	M.1	M.3	M.0	M.1
Anweisung an SMGW zur Aktivierung eines Firmware-Update	Anweisungen	4.3.2.6	M.1	S	M.0	M.0
Profile	Daten	4.3.2.7	M.1	M.2	M.0	M.0
Private Schlüssel des SMGW Admin	Daten	4.3.2.8	M.1	M.3	M.0	K
Zertifikate	Daten	4.3.2.9	M.1	S	M.0	M.1
Zertifikatsrequest	Daten	4.3.2.10	M.1	K	M.0	M.1
Anweisung an SMGW zur Generierung eines Zertifikatsrequest	Anweisungen	4.3.2.11	M.1	M.0	M.0	S
Wake-Up-Paket	Anweisungen	4.3.2.12	M.1	K	M.0	S
Anweisung an SMGW zum Setzen der Speicherfrist für das Letztverbraucher-Log	Anweisungen	4.3.2.13	M.1	M.1	M.0	M.0
Initiale Konfigurationsdatei	Daten	4.3.2.14	M.1	M.0	M.0	M.1
Logeintrag System-Log	Daten	4.3.2.15	M.1	M.3	M.0	M.0
Logeintrag eichtechn. Log	Daten	4.3.2.16	M.1	M.3	M.0	M.0
SMGW Admin Logeintrag	Daten	4.3.2.17	M.1	M.3	M.0	M.0
Anweisung an SMGW zur Durchführung eines Selbsttests	Anweisungen	4.3.2.18	M.1	M.1	M.0	M.0
Ergebnisdaten eines SMGW Selbsttests	Daten	4.3.2.19	vorerst offen	vorerst offen	vorerst offen	vorerst offen
Anweisung an SMGW zur Übermittlung von Logdaten	Anweisungen	4.3.2.20	M.1	M.1	M.0	M.0
Verschlüsselte und signierte Messwerte	Daten	4.3.2.21	M.1	S	M.0	M.0
Pseudonymisierte Netzzustandsdaten	Daten	4.3.2.22	M.1	M.3	M.0	M.0
Anweisung an SMGW zur Unterstützung der Messwertverarbeitung	Anweisungen	4.3.2.23	M.1	M.1	M.0	M.0
Log des SMGW Admin	Dienste	4.3.2.24	M.1	K	M.0	K
Dienst zum Empfang und Ausliefern von Messwerten	Dienste	4.3.2.25	M.1	K	M.0	K
Zeitserver SMGW Admin	Dienste	4.3.2.26	M.1	K	M.0	K
PTB Anbindung	Anbindungen	4.3.2.27	M.1	K	K	K
Zeitsynchronisation-Webservice des SMGW Admin	Dienste	4.3.2.28	M.1	K	M.0	K
WAN Anbindung	Anbindungen	4.3.2.29	M.1	K	K	K
Nachrichten Empfangsservice des SMGW Admin	Dienste	4.3.2.30	M.1	K	M.0	K
EMT Anbindung	Anbindungen	4.3.2.31	M.1	K	K	K
Fachlicher Ablaufzustand	Daten	4.3.2.32	M.1	M.2	M.0	S
Bestätigung oder Fehlermeldung eines SMGW	Daten	4.3.2.33	M.1	M.1	M.0	M.0

Asset	Objekt Typ	Detail	Mindestvorgaben zu den Schutzzielen			
	Zuordnung nach Kapitel 4.3.1	Asset Kapitel	Verfügbarkeit	Vertraulichkeit	Integrität	Authentizität
SMGW Admin Update Dienst	Dienste	4.3.2.34	M.1	K	M.0	K
Anbindung zur Sub-CA	Anbindungen	4.3.2.35	M.1	K	K	K
SMGW Admin Software	Dienste	4.3.2.36	M.1	K	M.0	K
Frontend SMGW Admin Software	Dienste	4.3.2.37	M.1	K	M.0	K
SMGW Hersteller Anbindung	Anbindungen	4.3.2.38	M.1	K	K	K
Sperrliste	Daten	4.3.2.39	M.1	K	M.0	M.1

Tabelle 112: Assets und Mindestvorgaben

Literaturverzeichnis

Auditor	"Anforderungen an Antragsteller zur Zertifizierung als Auditor", Bundesamt für Sicherheit in der Informationstechnik, noch nicht verfügbar
BSI CC-PP-0073	"Protection Profile for the Gateway of a Smart Metering System", BSI, 2013
BSI TR-03109	"Technische Richtlinie BSI TR-03109", Bundesamt für Sicherheit in der Informationstechnik, 2013
BSI TR-03109-1	"Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems", Bundesamt für Sicherheit in der Informationstechnik, 2013
BSI TR-03109-3	"Technische Richtlinie BSI TR-03109-3 Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen", Bundesamt für Sicherheit in der Informationstechnik, 17.04.2014
BSI TR-03109-4	"Technische Richtlinie BSI TR-03109-4 Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways", Bundesamt für Sicherheit in der Informationstechnik, 18.05.2015
CP	"Certificate Policy der Smart Metering PKI", Bundesamt für Sicherheit in der Informationstechnik, 2015
ISO27001	"Information technology - Security techniques -Information security management systems requirements specification", ISO/IEC JTC1/SC27, 2013
IT-GS	"IT-Grundschutz", BSI,
PTB-A 50.8	"PTB-Anforderungen 50.8", Physikalisch-Technische Bundesanstalt,
RFC2119	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997
RFC5905	"Network Time Protocol Version 4: Protocol and Algorithms Specification", D. Mills et al., June 2010
VB-Personen	"Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen", Bundesamt für Sicherheit in der Informationstechnik, noch nicht verfügbar

Tabellenverzeichnis

Glossar und Abkürzungsverzeichnis

BSI
: Bundesamt für Sicherheit in der Informationstechnik

CC
: Common Criteria

CLS
: Controllable Local Systems

EMT
: externer Marktteilnehmer

HAN
: Home Area Network

ISMS
: Informationssicherheit-Managementsystem

NTP
: Network Time Protocol

PKI
: Public Key Infrastructure

PP
: Protection Profile

PTB
: Physikalisch-Technische Bundesanstalt

RFC
: Request for Comments

SecMod
: Security Module (Sicherheitsmodul)

SMGW
: Smart Meter Gateway

SMGW Admin
: Smart Meter Gateway Administrator