Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Das Smart-Meter-Gateway

Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft

Inhaltsverzeichnis

1 Einleitung 6

2 Systemarchitektur 11

2.1 Das Lokale Metrologische Netz – LMN 11
2.2 Das Weitverkehrsnetz – WAN 12
2.3 Das Heimnetz – HAN 13

3 Sicherheitstechnische Anforderungen 15

3.1 Smart-Meter-Gateway – Schutzprofil (BSI-CC-PP-0073) 15
3.2 Bedrohungslage 16
3.3 Sicherheitsziele 16
3.4 Zertifizierungsverfahren 17

4 Technische Richtlinie TR-03109 19

4.1 TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems 19
4.2 TR-03109-2 Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls 20
4.3 TR-03109-3 Kryptographische Vorgaben – Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen 20
4.4 TR-03109-4 Smart-Metering-PKI – Public-Key-Infrastruktur für Smart-Meter-Gateways 20
4.5 TR-03109-5 Kommunikationsadapter 21
4.6 TR-03109-6 Smart-Meter-Gateway-Administration 21

5 Sicherstellung der Interoperabilität des intelligenten Messsystems 23

6 Smart-Metering-PKI (SM-PKI) 27

7 Informationssicherheit bei Administration und Betrieb 30

8 Marktanalyse 34

9 Ausblick 37

9.1 Standardisierungsstrategie zur sektorübergreifenden Digitalisierung der Energiewende 37

9.2 Fortentwicklung der BSI-Standards in weiteren Einsatzbereichen 38

10 Fazit 42

Das BSI im Dienst der Öffentlichkeit 45

Impressum 47

1 Einleitung

1 Einleitung

Die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller gesellschaftlichen Lebensbereiche stellt Staat, Wirtschaft und unsere Gesellschaft vor große Herausforderungen. Indem Produktkomponenten sowie Systeme untereinander kommunikativ verknüpft werden, werden auf der einen Seite Effizienzsteigerungen und Prozessoptimierungen in der Wirtschaft sowie mehr Komfort bei Bürgerinnen und Bürgern erreicht. Auf der anderen Seite steigt damit das Bedrohungspotential deutlich an, da sich die Anzahl der Angriffspunkte erhöht, die Kommunikationsinfrastrukturen immer komplexer werden und die zu verarbeitenden Datenmengen sich vervielfachen.

Im Zuge der Energiewende gehören Smart-Meter-Gateways (SMGW) zu den Schlüsseltechnologien und sind ein gutes Beispiel dafür, welchen Einfluss digitale und vernetzte Technologien auf den Alltag der Verbraucher haben werden und wie wichtig in diesem Zusammenhang die frühzeitige Umsetzung von hohen Vorgaben zum Datenschutz und zur IT-Sicherheit sind („Security & Privacy by Design“). Aufgabe und Anspruch des BSI ist es, die Informationssicherheit in der Digitalisierung zu gestalten und zu gewährleisten, damit die Anwender von den Vorzügen dieser innovativen Technologien profitieren können. Nur wenn Staat, Wirtschaft sowie Bürgerinnen und Bürger auf den Schutz ihrer Daten vertrauen können und ihre IT-Systeme gegen zunehmende Bedrohungen ausreichend geschützt sehen, wird diese digitale Transformation gelingen und deren Potential auch voll ausgeschöpft werden können.

Um dieses Vertrauen gewinnen zu können, sind nachweislich sichere Produktkomponenten und Systeme im Netz sowie eine sichere Kommunikationsinfrastruktur zwingend erforderlich.

Eine erfolgreiche digitale Transformation kann nur mit der frühzeitigen Entwicklung und Bereitstellung von allgemein verbindlichen Sicherheitsstandards und Maßnahmen zur Sicherung der Vertrauenswürdigkeit digitaler Infrastrukturen gelingen. Elektronische Identitäten und Verschlüsselung spielen hier eine zentrale Rolle: Durch Verschlüsselung werden Integrität, Authentizität und Vertraulichkeit der Informationen auf den Kommunikationswegen sichergestellt. Die gegenseitige Authentisierung der elektronischen Identitäten untereinander bildet die Vertrauensbasis digitaler Kommunikationsinfrastrukturen.

In Zusammenhang mit den technischen Standards des BSI schafft das „Gesetz zur Digitalisierung der Energiewende“ (GDEW) verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von intelligenten Messsystemen in unterschiedlichen Einsatzbereichen. Das GDEW ist seit September 2016 in Kraft und enthält mit dem Gesetz für den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG) ein neues Stammgesetz, welches den Infrastrukturrollout für die Digitalisierung regelt. Hier werden unter anderem die hohen technischen Standards für intelligente Messsysteme in Form

von Schutzprofilen (engl.: Protection Profiles, PP) und Technischen Richtlinien (TR) des BSI zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität festgelegt.

Diese Rahmenvorgaben sind Grundvoraussetzung für Vertrauen und Akzeptanz in die neue Technik, insbesondere, weil eine Vielzahl personenbezogener Daten verarbeitet wird. Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) entwickelt das BSI daher Anforderungen an vertrauenswürdige Produktkomponenten (SMGW mit integriertem Sicherheitsmodul), dessen sicheren IT-Betrieb (Administration) und an die vertrauenswürdige Kommunikationsinfrastruktur (Smart-Metering-Public-Key-Infrastruktur).

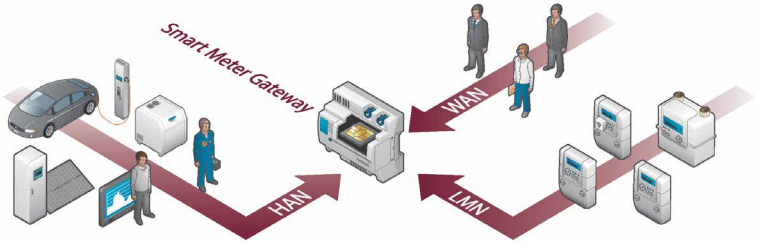
Die Voraussetzungen zum Einbau von intelligenten Messsystemen sind nun nach anspruchsvoller Entwicklungsphase gegeben, da drei SMGW voneinander unabhängiger Hersteller vom BSI zertifiziert wurden und die technische Möglichkeit zum Einbau intelligenter Messsysteme nach § 30 MsbG durch das BSI festgestellt wurde. Damit sind grundzuständige Messstellenbetreiber, in Abhängigkeit des vom Messstellenbetriebsgesetz vorgegebenen Zeitplans, zum Einbau intelligenter Messsysteme verpflichtet. Messsysteme, die nicht den Anforderungen des BSI entsprechen, dürfen nicht mehr verbaut werden und die Übermittlung aller energiewenderelevanten Daten darf nur noch ausschließlich über ein SMGW erfolgen. Durch den Start des Rollouts kann das Potential der sicheren Gateway-Kommunikationsplattform umfangreich genutzt und wertvolle Erfahrungen für die Weiterentwicklung der BSI-Standards gesammelt werden.

Gemeinsam mit dem BMWi hat das BSI bereits eine Standardisierungsstrategie zur sektorübergreifenden Digitalisierung der Energiewende erarbeitet und veröffentlicht. Auf ihrer Basis können gemeinsam mit den Verbänden und den Unternehmen der Energiewirtschaft die wesentlichen technischen Eckpunkte und die daraus resultierenden Anforderungen für ein sicheres, intelligentes Energienetz (Smart Grid) der Zukunft festgelegt werden. Dadurch können aktuelle Trends und Innovationen zielgerichtet erfasst und die Gateway-Technologie kontinuierlich in weiteren Einsatzbereichen fortentwickelt werden.

2 Systemarchitektur

2 Systemarchitektur

Das intelligente Messsystem besteht im Kern aus einer Kommunikationseinheit, dem Smart-Meter-Gateway (SMGW), welches die elektronischen Messeinrichtungen im Lokalen Metrologischen Netz (LMN) mit den verschiedenen Marktteilnehmern (bspw. Gateway-Administrator im Auftrag des Messstellenbetreibers, Verteilnetzbetreiber oder Energielieferant) im Weitverkehrsnetz (WAN) und dem lokalen Heimnetz (HAN) verbindet.



Das SMGW stellt sicher, dass alle Kommunikationsverbindungen verschlüsselt werden und dass nur bekannten Teilnehmern und Geräten vertraut wird. Die Einrichtung der Kommunikationsverbindungen obliegt dem Gateway-Administrator.

2.1 Lokale Metrologische Netz – LMN

Über das Lokale Metrologische Netz werden die Messeinrichtungen des Letztverbrauchers mit dem SMGW verbunden. Diese senden die erhobenen Verbrauchs- und Einspeisewerte sowie Netzzustandsdaten (z.B. Spannung, Phasenwinkel, Frequenz) an das Gateway, wo sie gespeichert und weiterverarbeitet werden.

Das Gateway nutzt je nach Tarif des Kunden unterschiedliche Regelwerke, um die empfangenen Messwerte sowohl unter dem Gesichtspunkt des Eichrechts als auch des Datenschutzes weiterzuverarbeiten.

2.2 Das Weitverkehrsnetz – WAN

Das SMGW kann über die WAN-Schnittstelle mit externen Marktteilnehmern kommunizieren, zu denen auch der Gateway-Administrator gehört.

Dieser ist sowohl für die Konfiguration als auch für den sicheren Betrieb verantwortlich. Er muss u.a. das kryptographische Schlüsselmaterial für die Komponenten des intelligenten Messsystems beim Letztverbraucher einspielen, aber auch die Konfiguration der Regelwerke für die Tarifierung vornehmen.

Aus Gründen der Sicherheit gehen sämtliche Kommunikationsverbindungen vom Gateway aus. Diese können bei Bedarf oder zu festgelegten Zeitpunkten durch das Gateway etabliert werden. Um aber auch auf spontane Ereignisse reagieren zu können, kann der Administrator das Gateway über einen Wake-Up-Dienst zu einem Verbindungsaufbau anstoßen.

Dabei handelt es sich um ein vom Administrator signiertes und nur für einen gewissen Zeitraum gültiges Datenpaket, auf welches das Gateway nach erfolgreicher Überprüfung reagiert, indem es eine gesicherte Verbindung zum Gateway-Administrator aufbaut.

2.3 Das Heimnetz – HAN

Die HAN-Schnittstelle ist dem Letztverbraucher zuzuordnen. An dieser kann er steuerbare Geräte wie bspw. Wärmepumpen oder Photovoltaikanlagen anschließen, um externen Marktteilnehmern den Zugriff für Steuerungs- und Fernwartungszwecke zu ermöglichen. Das SMGW stellt hierfür einen sicheren, transparenten Kanal zur Verfügung, welcher nur durch den Gateway-Administrator konfiguriert werden kann.

Darüber hinaus kann der Letztverbraucher über diese Schnittstelle seine Verbrauchs- und ggf. Einspeisewerte abfragen. Er kann hierzu ein geeignetes Endgerät anschließen und erhält nach erfolgreicher Authentifizierung lesenden Zugriff auf seine Daten. Insbesondere wird jeder Datenversand im Letztverbraucher-Logbuch protokolliert und kann durch diesen nachvollzogen werden.

Ebenfalls über die HAN-Schnittstelle wird einem Servicetechniker die Möglichkeit geboten, wichtige Informationen über den Systemzustand des SMGW in Erfahrung zu bringen. Diese werden benötigt, um im Fehlerfall die Ursache diagnostizieren zu können und das intelligente Messsystem zu entstören. Aus Datenschutzgründen hat er keinen Zugriff auf die im Gateway hinterlegten Messwerte bzw. mandantenspezifische Daten.

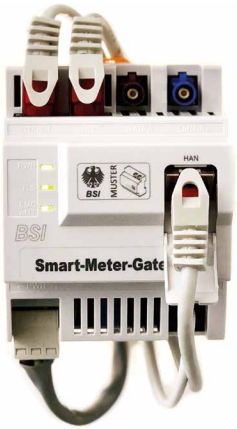
3 Sicherheitstechnische Anforderungen

3 Sicherheitstechnische Anforderungen

3.1 Smart-Meter-Gateway – Schutzprofil (BSI-CC-PP-0073)

Das Schutzprofil beschreibt mögliche Bedrohungen eines SMGW in seiner Einsatzumgebung und definiert die Mindestanforderungen für entsprechende Sicherheitsmaßnahmen.

Der Aufbau eines Schutzprofils ist in den Common Criteria (CC) geregelt. Auf Basis eines Schutzprofils können Produkte evaluiert werden, die nach einer positiven Prüfung ein Zertifikat erhalten und somit nachweislich das Schutzziel erfüllen. Zugleich lässt das Schutzprofil dem Hersteller Spielraum bei der technischen Ausgestaltung der Sicherheitsanforderungen.



Das Schutzprofil für das SMGW konzentriert sich auf die zu erfüllende Sicherheitsleistung eines verbauten Gateways und definiert für die Schnittstellen zu den drei Netzen (LMN, HAN und WAN) sicherheitstechnische Anforderungen, die jedes Gateway bereitstellen muss.

Dabei ermöglicht es, dass selbst bei unterschiedlicher Ausführung (Einfamilienhaus, Wohnungsgesellschaften, Ein- und Mehrgerätelösung) ein einheitlicher, hoher Sicherheitsstandard gewährleistet ist und stellt im Fall von neuen technischen Möglichkeiten eine kontinuierliche Weiterentwicklung der Produkte sicher.

3.2 Bedrohungslage

Das Schutzprofil des SMGW unterscheidet mögliche Bedrohungen anhand des potenziellen Angreifers, der auf das Gateway einwirken möchte. Zum einen gibt es den lokalen Angreifer, der vor Ort direkten Zugriff auf das Gateway besitzt, um somit das Gateway auf physischem Wege zu kompromittieren. Beispielsweise könnte ein Angreifer über Eingriffe am Gateway versuchen abrechnungsrelevante Daten oder Netzzustandsdaten zu manipulieren. Aber auch Angriffe auf die Systemuhr des Gateways, das Ausspähen von Verbrauchsdaten, die Manipulation der Geräteeinstellungen oder ein Auslesen und Verändern der Firmware gehören mit zu den möglichen Angriffszielen.

Zum anderen bietet die kommunikative Anbindung des Gateways ein hohes Angriffspotenzial für Angreifer, die von außen versuchen eine Vielzahl von intelligenten Messsystemen anzugreifen. Die potenziellen Angriffe aus dem WAN ähneln größtenteils denen, die lokal ein Risiko darstellen, diese sind im Risikomanagement aufgrund möglicher Schwarmeffekte jedoch als kritischer zu bewerten.

3.3 Sicherheitsziele

Um den zuvor beschriebenen Bedrohungen entgegen zu wirken, definiert das Schutzprofil eine Reihe von Sicherheitszielen, die durch das SMGW umgesetzt werden müssen. Um seiner Rolle als Bindeglied zwischen drei unterschiedlichen Netzen (LMN, HAN und WAN) gerecht zu werden, schottet das Gateway die Netze gegeneinander ab. Hierzu sind seitens des Herstellers u. a. Firewall-Mechanismen in das Gateway zu integrieren. Neben der physischen und logischen Separierung der jeweiligen Netze und Schnittstellen muss ebenfalls sichergestellt werden, dass nur Kommunikationsverbindungen von

innen nach außen aufgebaut werden können. Daneben werden sämtliche Kommunikationsflüsse, unabhängig in welches Netz kommuniziert wird, nach einer gegenseitigen Authentifizierung grundsätzlich verschlüsselt und integritätsgesichert. Ein besonderes Augenmerk legt das Schutzprofil auf die Kommunikation zu den angeschlossenen Zählern. Das Gateway stellt hierfür Funktionen zum Empfang und zur Abfrage von Einspeise- und Verbrauchswerten sowie Netzzustandsdaten in konfigurierbaren Zeitintervallen zur Verfügung.

3.4 Zertifizierungsverfahren

Die Zertifizierung nach Common Criteria (CC) dient dem Nachweis der Sicherheitseigenschaften des Schutzprofils (PP) und umfasst auch den Nachweis einer sicheren Produktions- und Entwicklungsumgebung beim Gerätehersteller sowie einer sicheren Auslieferung des Produkts zum Anwender. Der Nachweis der sicherheitstechnischen Vorgaben (Schutzprofil) ist durch die Hersteller im CC-Zertifizierungsverfahren nachzuweisen.

Bei gültigem CC-Zertifikat genießen Hersteller und Anwender der SMGW einen insgesamt 8-jährigen Bestandsschutz, sofern die Gültigkeit des Zertifikats durch eine Neubewertung (Re-Assessment) alle 2 Jahre bestätigt wird.

Eine Auflistung der SMGW-Hersteller, die zertifiziert wurden oder sich im Zertifizierungsverfahren befinden, ist unter dem nachfolgenden Link abrufbar:

4 Technische Richtlinie TR-03109

4 Technische Richtlinie TR-03109

Zur Gewährleistung der Interoperabilität der verschiedenen in einem intelligenten Messsystem vorhandenen Komponenten müssen diese auch rein funktionale Vorgaben erfüllen. Des Weiteren müssen auch die im Schutzprofil getroffenen Sicherheitsanforderungen näher spezifiziert werden. Diese zusätzlichen Anforderungen für intelligente Messsysteme und deren sicheren Betrieb finden sich in der Technischen Richtlinie BSI TR-03109 wieder.

Die Technische Richtlinie TR-03109 ist in mehrere Teile untergliedert und widmet sich thematisch neben dem SMGW und dem Sicherheitsmodul auch der Infrastruktur, beispielsweise der PKI oder dem Gateway-Administrator.

4.1 TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

Teil 1 der Technischen Richtlinie TR-03109 beinhaltet die funktionalen Anforderungen, die ein SMGW mindestens erfüllen muss. Das Dokument ist in die drei Themenbereiche LMN, HAN und WAN untergliedert und definiert für diese Bereiche detaillierte technische Vorgaben. Darüber hinaus werden interne, logische Abläufe (bspw. die Tarifierung anhand von Regelwerken, Zusammenspiel zwischen Gateway und Sicherheitsmodul) weiter ausgeführt.

4.2 TR-03109-2 Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls

Das Schutzprofil für das SMGW fordert den Einsatz eines zertifizierten Sicherheitsmoduls, welches das Gateway vor allem bei der Signaturerstellung und -prüfung sowie bei der Schlüssel- und Zufallszahlengenerierung unterstützt.

Zudem dient das Sicherheitsmodul als sicherer Schlüsselspeicher u. a. für das private Schlüsselmaterial und stellt damit einen wichtigen Vertrauensanker im Gateway dar. Diese und weitere funktionale Anforderungen, auch unter dem Gesichtspunkt der herstellerübergreifenden Interoperabilität, finden sich in der Technischen Richtlinie TR-03109-2 wieder.

4.3 TR-03109-3 Kryptographische Vorgaben – Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen

Welche kryptographischen Verfahren oder Schlüssellängen im SMGW und dessen unmittelbarem Umfeld zum Einsatz kommen, werden in Teil 3 der Technischen Richtlinie definiert. Diese basiert u. a. auf den Richtlinien TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ und TR-03111 „Elliptische-Kurven-Kryptographie“.

4.4 TR-03109-4 Smart-Metering-PKI – Public-Key-Infrastruktur für Smart-Meter-Gateways

Dieser Teil der Technischen Richtlinie spezifiziert die Architektur der Smart-Metering-Public-Key-Infrastruktur (SM-PKI), mit der die Authentizität der bei dieser Kommunikation eingesetzten öffentlichen Schlüssel der Kommunikationspartner sicher-

gestellt wird. Technisch wird der Authentizitätsnachweis der Schlüssel über digitale Zertifikate aus der SM-PKI realisiert.

4.5 TR-03109-5 Kommunikationsadapter

In der TR-03109-5 werden zukünftig Adapterlösungen zur Ankopplung von Bestandszählern bzw. von steuerbaren Systemen an das SMGW beschrieben.

4.6 TR-03109-6 Smart-Meter-Gateway-Administration

Für den sicheren, technischen Betrieb des intelligenten Messsystems ist der Gateway-Administrator verantwortlich. Daher muss sichergestellt sein, dass der Betrieb beim Administrator Mindestanforderungen zur Durchsetzung der Informationssicherheit genügt. Der Nachweis der Umsetzung der definierten Mindestanforderungen kann zum einen durch eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz und zum anderen durch eine Zertifizierung gemäß ISO/IEC 27001 erbracht werden.

5 Sicherstellung der Interoperabilität des intelligenten Messsystems

5 Sicherstellung der Interoperabilität des intelligenten Messsystems

Neben der Einhaltung der sicherheitstechnischen Anforderungen stellt die Interoperabilität des SMGW als Vertrauensanker und zentrale Kommunikationsplattform einen wichtigen Eckpfeiler für einen erfolgreichen Rollout des intelligenten Messsystems dar. Aus diesem Grund spezifiziert das BSI in Form von Technischen Richtlinien funktionale Anforderungen zur Etablierung einer Mindest-Interoperabilität bei den SMGW sowie weiteren technischen Komponenten wie bspw. des im Gateway verbauten Sicherheitsmoduls.

Durch diese Festlegungen wird sichergestellt, dass beim Austausch eines Gateways durch ein Gateway eines anderen Herstellers die umliegenden Komponenten wie Zähler, steuerbare Geräte oder Backend-Systeme zur Administration nicht von diesem Wechsel betroffen sind und unverändert weiterverwendet werden können. Grundsätzlich müssen SMGW den Anforderungen der TR 03109-1 genügen, damit die Feststellung zur technischen Möglichkeit des Einbaus intelligenter Messsysteme für die jeweilige Einbaugruppe durch das BSI getroffen werden kann. Dabei werden sich die Anforderungen an die Interoperabilität, die durch die Geräte zu erfüllen sind, mit der Technischen Richtlinie kontinuierlich weiterentwickeln. Interoperabilität ist demnach kein statischer Zustand, sondern ein Reifeprozess. Mit der Veröffentlichung der TR-03109-1 Version 1.0.1 und der neu hinzugekommenen Anlage VII hat das BSI daher die Technische Richtlinie um ein Interoperabilitätsmodell und funktionale Geräteprofile erweitert.

Die Einführung funktionaler Geräteprofile ermöglicht zudem die Entwicklung spezialisierter SMGW für bestimmte Anwendungszwecke. Alle SMGW müssen mindestens das Geräteprofil SMGW_G1_BASIS erfüllen. Die dort aufgeführten Anforderungen beinhalten grundlegende Funktionalitäten, die z. B. für die Administration der Geräte sowie die sichere Kommunikation im HAN, WAN und LMN benötigt werden. Darüber hinaus umfasst das Basisprofil die für den Einsatzbereich Smart Metering grundlegenden Tarifanwendungsfälle (TAF) 1, 2, 6 und 7. Das verpflichtende Basisprofil wird zukünftig durch weitere Geräteprofile ergänzt, mit denen sich zusätzliche Einsatzbereiche durch ein SMGW erschließen lassen.

Der Nachweis über die Einhaltung der Geräteprofile und damit einhergehend die Erreichung des geforderten Interoperabilitätsniveaus erfolgt zukünftig im Rahmen der TR-Zertifizierung. Solange die Verpflichtung zum Nachweis der Interoperabilität durch ein TR-Zertifikat nicht besteht, müssen die SMGW-Hersteller die Einhaltung eines oder mehrerer Geräteprofile durch eine verbindliche Konformitätserklärung gegenüber dem BSI bestätigen.

Flankierend zu den Arbeiten an der Technischen Richtlinie werden parallel umfassende Testfälle für das SMGW beschrieben, welche zur Nachweiserbringung der geforderten Interoperabilität benötigt werden. In einem agilen Entwicklungsprozess, verbunden mit einem ebenso agilen Qualitätssicherungsprozess, wird sichergestellt, dass die Anforderungen für den vorgesehenen Einsatzzweck passend und umsetzbar sind.

Ein zentraler Baustein zur Überprüfung der Interoperabilität der SMGW ist die oben genannte TR-Zertifizierung. Hierfür entwickelt das BSI eine Testumgebung zur Durchführung von (teil-)automatisierten Konformitätstests für die Prüfstellen des BSI.

6 Smart-Metering-PKI (SM-PKI)

6 Smart-Metering-PKI (SM-PKI)

Um den Schutz der von den Haushalten übermittelten Messdaten zu gewährleisten, ist für die Verbindung des SMGW zu einem autorisierten Marktteilnehmer im Weitverkehrsnetz eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten, integritätsgesicherten Kanal. Zudem werden zu sendende Daten vom SMGW zusätzlich auf Datenebene für den Endempfänger verschlüsselt und signiert. Grundlage für diese sichere Kommunikation bildet technisch eine Public-Key-Infrastruktur (PKI), die sogenannte Smart-Metering-PKI (SM-PKI). Aus der SM-PKI erhalten die Gateways und Marktteilnehmer digitale Zertifikate mit kryptografischen Schlüsseln. Über diese Zertifikate können die Daten verschlüsselt und signiert kommuniziert werden.

Die SM-PKI sieht gemäß § 28 MsbG eine zentrale, staatliche Wurzelzertifizierungsstelle, die so genannte Root-Certificate Authority (Root-CA), als Vertrauensanker in der Infrastruktur der Gateways vor. Darunterliegend operieren private Unternehmen, sogenannte Sub-CAs (untergeordnete Zertifizierungsstellen), welche die Zertifikatsausstellung für Gateways und Marktteilnehmer übernehmen. Die Root-CA setzt die gesetzlichen Anforderungen auf techni-

scher Ebene durch und berechtigt die privaten Unternehmen eine Sub-CA zu betreiben. Hierzu muss eine Sub-CA bei der Root-CA ein Registrierungsverfahren erfolgreich abschließen. Die technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung, Verwaltung und Benutzung von Zertifikaten werden von der Root in einer Certificate Policy (Root-CP) festgelegt.

Der Wirkbetrieb der Root wird seit dem 1. März 2015 unter der Aufsicht des BSI von einem Zertifizierungsdiensteanbieter durchgeführt. Des Weiteren stellt das BSI den Marktteilnehmern zusätzlich zur Root-CA verschiedene Testsysteme zur Ausgabe von digitalen Test-Zertifikaten bereit.

Eine aktuelle Auflistung der registrierten Zertifizierungsdienstleister (Sub-CAs) ist hier abrufbar:

7 Informationssicherheit bei Administration und Betrieb

7 Informationssicherheit bei Administration und Betrieb

Für den sicheren, technischen Betrieb des intelligenten Messsystems ist der Smart-Meter-Gateway-Administrator verantwortlich, dessen Funktion nach § 3 Absatz 1 Satz 2 MsbG dem Messstellenbetreiber zugewiesen ist. Es muss sichergestellt sein, dass der Betrieb beim Administrator Mindestanforderungen zur Durchsetzung der Informationssicherheit genügt. Für alle Marktteilnehmer, die die Aufgaben des Administrators selbst wahrnehmen oder als Dienstleister für Dritte anbieten möchten, ist ein vergleichbares Maß an Informationssicherheit notwendig. Die entsprechenden Mindestanforderungen an die Informationssicherheit sind in § 25 Messstellenbetriebsgesetz (MsbG) verankert und legen verbindlich fest, dass der Adminis-

trator in seiner notwendigen Sicherheitskonzeption auch die in der TR-03109-6 beschriebenen Mindestanforderungen angemessen berücksichtigen muss.

Die TR-03109-6 definiert ausgehend von den Aufgaben und Anwendungsfällen des Administrators die zu schützenden werthaltigen Objekte (Assets), beschreibt die zu beachtenden Schutzziele und gibt eine Abschätzung des Bedrohungs- und Risikopotenzials. Daraus abgeleitet werden angemessene Mindestmaßnahmen, die die identifizierten Bedrohungen und Risiken geeignet berücksichtigen und minimieren.

Der Nachweis der Umsetzung der definierten Mindestanforderungen kann zum einen durch eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz und zum anderen durch eine Zertifizierung gemäß ISO/IEC 27001 erbracht werden. Die erste Vorgehensweise (ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz) umfasst eine Prüfung des ISMS (dt. „Managementsystem für Informationssicherheit“) sowie eine über ISO 27001 hinausgehende Bewertung konkreter Sicherheitsmaßnahmen anhand des neuen Grundschutz-Kompendiums. Sowohl im behördlichen Umfeld als auch im privatwirtschaftlichen Bereich hat sich der IT-Grundschutz als Standard für die Informationssicherheit in Deutschland etabliert. Unternehmen aller Größenordnungen verwenden den IT-Grundschutz als Hilfsmittel bei der Konzeption, Realisierung und Revision von Standard-Sicherheitsmaßnahmen.

Die IT-Grundschutz-Vorgehensweise (BSI-Standard 200-2) beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Sicherheitsmanagements und der Aufbau von Organisationsstrukturen für Informationssicherheit sind dabei wichtige Themen. Diese Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept

in der Praxis erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrechterhalten und verbessert werden kann, wird beantwortet.

Im Rahmen der Vorgehensweise nach IT-Grundschutz fungiert das BSI als Zertifizierungsstelle. Für die zweite Vorgehensweise (Zertifizierung eines ISMS nach ISO/IEC 27001) sind Zertifizierungsstellen beteiligt, die bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß ISO/ IEC 27006 für ISMS akkreditiert sind. Die Konformität des Betriebs beim Smart-Meter-Gateway-Administrator zur Technischen Richtlinie TR-03109-6 muss in jedem Fall durch eine Zertifizierung bestätigt werden.

Sowohl die für eine Erst- oder Re-Zertifizierung notwendigen Audits, als auch die jährlich notwendigen Überwachungsaudits, werden durch BSI-zertifizierte Auditoren geleistet. Eine Übersicht der verfügbaren Auditoren listet der folgende Link auf:

Web: www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/AuditorSmartMeterGateway/Liste-AuditorSmartMeterGateway/liste-auditorsmg_node.html

Eine Auflistung der zertifizierten Smart-Meter-Gateway-Administratoren ist unter dem nachfolgenden Link abrufbar:

8 Marktanalyse

8 Marktanalyse

Das MsbG regelt umfassend die Ausstattung von Messstellen mit intelligenten Messsystemen (Rollout) in Deutschland und formuliert regulatorische Anforderungen an die Rolle des grundzuständigen Messstellenbetreibers. Um sicherzustellen, dass grundzuständige Messstellenbetreiber die ihnen auferlegten Pflichten fristgerecht erfüllen können, stellt das Gesetz den Startpunkt des verpflichtenden Rollouts unter den Vorbehalt der „Feststellung der technischen Möglichkeit des Einbaus von intelligenten Messsystemen".

Die Marktanalyse bildet die Basis, auf der das BSI die Feststellung der technischen Möglichkeit des Einbaus von intelligenten Messsystemen trifft. Die Veröffentlichung erfolgt jeweils zum 31. Januar eines Jahres und bei Bedarf, sofern es aktuelle Ereignisse erfordern sollten.

Mit der Veröffentlichung der Marktanalyse hat das BSI zuletzt dargelegt, dass die Voraussetzungen für den Rollout-Start bestimmter Einbaugruppen erfüllt sind. Dementsprechend hat das BSI die Feststellung der technischen Möglichkeit des Einbaus von intelligenten Messsystemen für einen Teil der verpflichtend mit einem intelligenten Messsystem auszustattenden Messstellen getroffen.

Mit den bereits angekündigten Softwareupdates werden die zertifizierten SMGW-Hersteller weitere Tarifanwendungsfälle implementieren und ihre Geräte um wichtige Smart Grid-Funktionalitäten erweitern, sodass darauf aufbauend die Feststellung der technischen Möglichkeit für weitere Einbaugruppen

getroffen werden kann. Die Marktanalyse des BSI ist unter dem nachfolgenden Link abrufbar:

9 Ausblick

9 Ausblick

9.1 Standardisierungsstrategie zur sektorübergreifenden Digitalisierung der Energiewende

Gemeinsam mit dem BMWi hat das BSI eine Standardisierungsstrategie zur sektorübergreifenden Digitalisierung der Energiewende (BMWi-BSI-Roadmap) erarbeitet und Anfang 2019 veröffentlicht. Auf ihrer Basis können, gemeinsam mit den Verbänden und den Unternehmen der Energiewirtschaft, die wesentlichen technischen Eckpunkte und die daraus resultierenden Anforderungen für ein sicheres, intelligentes Energienetz (Smart Grid) der Zukunft festgelegt werden.

Ohne eine kontinuierliche Fortentwicklung der rechtlichen und technischen Rahmenbedingungen, ist die Migration des heute passiven Energienetzes zu einem sicheren und aktiven Smart Grid nicht denkbar. Dies gilt insbesondere für die Integration und Vernetzung von steuerbaren Erzeugungsanlagen, flexiblen Verbrauchseinrichtungen, mobilen und stationären Energiespeichern und modernen Messeinrichtungen in das intelligente Energienetz. Die Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nimmt diese Herausforderung an. Sie zeigt basierend auf den Rahmenbedingungen des GDEW auf, wie mit der Weiterentwicklung der technischen Standards des BSI der stufenweise Rollout von intelligenten Messsystemen und weiteren standardisierten Mess- und Steuerungseinrichtungen für das zukünftige Smart Grid gefördert wird. Im Zentrum hierbei steht das zertifizierte SMGW als sichere Kommunikationsplattform.

Die Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem GDEW ist unter dem nachfolgenden Link abrufbar:

9.2 Fortentwicklung der BSI-Standards in weiteren Einsatzbereichen

Durch den Roadmapprozess werden weitere Einsatzbereiche für die sichere Gateway-Kommunikationsplattform aufgezeigt, die im Vorfeld der Standardisierung analysiert werden müssen:

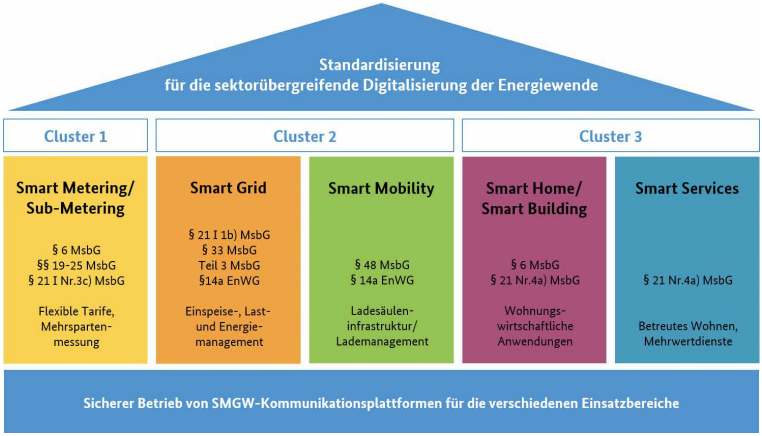


Abbildung – Übersicht der Einsatzbereiche für die Digitalisierung der Energiewende

Für die Weiterentwicklung der Standards wird es drei Schwerpunkt-Cluster geben, welche die verschiedenen Einsatzbereiche umfassen:

» Smart Metering: Mehrsparten- und Untermessung (Sub-Metering)

» Smart Grid: Steuerung und Monitoring von Einspeise-, Verbrauchs-, Speicher-, und Netzeinrichtungen

» Smart Mobility: Integration der Ladeinfrastruktur, sicheres Lademanagement und datenschutzkonforme Abrechnung

» Smart Building: Steuerung und Monitoring von energietechnischen Einrichtungen

» Smart Home: Digitaler Verbraucherinformation und Energieeffizienz

» Smart Services: Weitere Dienste der SMGW-Kommunikationsplattform

Um für die Weiterentwicklung von technischen Standards des BSI eine solide Basis und Akzeptanz im Markt zu schaffen, hat das BSI ein Projekt zur „Produkt- und Systemarchitektur-Analyse für die fortschreitende Digitalisierung des intelligenten Netzes der Energiewende“ gestartet. Es soll technische Eckpunkte beschreiben, die für die Weiterentwicklung der technischen BSI-Standards als Grundlage dienen. Der Prozess staffelt sich hier in eine Befragungs-, eine Interview- und eine Task-Force-Phase, um den Input aller Vertreter aus der Energiebranche und weiterer Branchen berücksichtigen zu können. Zum einen setzt die Analyse dabei auf die sektorübergreifenden Themen der Standardisierungsstrategie auf. Zum anderen berücksichtigt sie Arbeitsergebnisse des BMWi-Projekts „Digitalisierung der Energiewende: Barometer und Topthemen“, welches parallel die regulatorischen Eckpunkte zu den verschiedenen sektorübergreifenden Themen analysiert. Seitens des BMWi

wird das Ziel verfolgt, entsprechende Rechtsverordnungen (§ 46 und § 74 MsbG) zu entwickeln. Sowohl die technischen Eckpunkte als auch die Rechtsverordnungen stellen somit die Rahmenbedingungen für die kontinuierliche Weiterentwicklung der BSI-Vorgaben (Schutzprofile und Technische Richtlinien) in den kommenden Jahren dar.

10 Fazit

10 Fazit

Das GDEW schafft über Vorgaben für die Standardisierung, den Rollout intelligenter Messsysteme und die Datenkommunikation die Basis für den Aufbau einer modernen digitalen Infrastruktur für die Energienetze der Zukunft.

Im Fokus steht hierbei das SMGW als sichere und datenschutzkonforme Kommunikationsplattform für die Energiewende-relevanten Anwendungsfälle des intelligenten Netzes. Schutzprofile und Technische Richtlinien des BSI gewährleisten ein hohes Maß an Datenschutz- und Datensicherheit und sorgen für einen einheitlichen und interoperablen Sicherheitsstandard im künftigen Energieversorgungssystem. Daher sind Vertrauen und Akzeptanz durch Umsetzung der Vorgaben wesentliche Erfolgsfaktoren.

Die Einhaltung der Schutzprofile und der Technischen Richtlinie werden durch entsprechende Prüfungen bei neutralen, unabhängigen Prüflaboren mit abschließenden Zertifikaten des BSI nachgewiesen. Zudem schafft die Zertifizierung nach dem internationalen Standard der Common Criteria für die Hersteller entsprechender Geräte die Möglichkeit einer internationalen Anerkennung und Vermarktung.

Durch den Start des Rollouts kann das Potential der sicheren Gateway-Kommunikationsplattform nun umfangreich genutzt und wertvolle Erfahrungen für die kontinuierliche Weiterentwicklung der BSI-Standards gesammelt werden.

Das BSI hat auf seiner Webseite einen Themenschwerpunkt „Smart-Metering-Systems“ eingerichtet. Dort sind neben Hintergrundinformationen auch die aktuellen BSI-Sicherheitsstandards zum SMGW, zur Smart-Metering-PKI, zum Betrieb sowie deren aktueller Stand zur Umsetzung abrufbar.

Kontakt: smartmeter@bsi.bund.de

Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit

in der Informationsgesellschaft. Als Behörde ist sie damit im Vergleich zu sonstigen europäischen Einrichtungen einzigartig. Derzeit sind dort über 1.000 Informatiker, Physiker, Mathematiker und andere Mitarbeiter beschäftigt. Seinen Hauptsitz hat das BSI in Bonn.

Mit der rasanten Fortentwicklung der Informationstechnik entstehen in fast allen Bereichen des Alltags neue IT-Anwendungen – und damit auch immer neue Sicherheitslücken. Je abhängiger der Mensch von der Informationstechnik wird, desto mehr stellt sich die Frage nach deren Sicherheit. Unsere Gesellschaft ist stärker als zuvor durch Computerversagen, -missbrauch oder -sabotage bedroht. Bisher kann nicht ausreichend sichergestellt werden, dass die Informationstechnik

das tut, was sie soll, und nichts tut, was sie nicht soll. Weil die Probleme in der Informationstechnik so vielschichtig sind, ist auch das Aufgabenspektrum des BSI sehr komplex.

Diese Broschüre beschreibt das Smart-Meter-Gateway als zentrale Kommunikationslösung eines intelligenten Messsystems und beleuchtet sowohl die sicherheitstechnischen Vorgaben als auch funktionalen Anforderungen zur Interoperabilität.

Zusätzlich werden die Systemarchitektur, die Public Key Infrastruktur sowie Vorgaben zum sicheren, technischen Betrieb des intelligenten Messsystems beim Smart-Meter-Gateway-Administrator vorgestellt.

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de · www.facebook.com/bsi.fuer.buerger

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
E-Mail: smartmeter@bsi.bund.de
Internet: www.bsi.bund.de/SmartMeter
Telefon +49 (0) 22899 9582 - 0
Telefax +49 (0) 22899 9582 - 5400

Stand
Januar 2020

Druck
Appel & Klinger Druck und Medien GmbH
Bahnhofstraße 3 a
96277 Schneckenlohe
www.ak-druck-medien.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Titelbild: Freepik / fanjianhua
Seite 7: Fotolia / marco2811
Seite 27: Fotolia / Maksim Kabakou
Seite 30: Fotolia / tournee
Seiten 11, 15, 38, 45: Bundesamt für Sicherheit in der Informationstechnik - BSI

Artikelnummer
BSI-Bro20/332

www.bsi.bund.de