Bundesamt
für Sicherheit in der
Informationstechnik

Das Smart-Meter-Gateway

Cyber-Sicherheit für die Digitalisierung der Energiewende

Inhaltsverzeichnis

Das BSI im Dienst der Öffentlichkeit 5

1 Einleitung 8

2 Systemarchitektur 12

2.1 Das Lokale Metrologische Netz – LMN 12
2.2 Das Weitverkehrsnetz – WAN 13
2.3 Das Heimnetz – HAN 14

3 Sicherheitstechnische Anforderungen 16

3.1 Smart-Meter-Gateway – Schutzprofil (BSI-CC-PP-0073) 16
3.2 Bedrohungslage 16
3.3 Sicherheitsziele 17
3.4 Zertifizierungsverfahren 18

4 Technische Richtlinie TR-03109 20

4.1 TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems 21
4.2 TR-03109-2 Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls 21
4.3 TR-03109-3 Kryptographische Vorgaben – Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen 22
4.4 TR-03109-4 Smart-Metering-PKI – Public-Key-Infrastruktur für Smart-Meter-Gateways 22

4.5 TR-03109-5 Kommunikationsadapter 22
4.6 TR-03109-6 Smart-Meter-Gateway-Administration 22

5 Sicherstellung der Interoperabilität des intelligenten Messsystems 25

6 Public-Key-Infrastruktur 28

7 IT-Sicherheit bei Administration 31

8 Ausblick 35

8.1 Fortentwicklung der Vorgaben für die sektorübergreifende Digitalisierung der Energiewende 35
8.2 Marktanalyse nach § 30 MsbG 37

9 Fazit 40

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 700 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.

1 Einleitung

1 Einleitung

Intelligente Messsysteme sind wichtige Bausteine im intelligenten Netz und benötigen Vorgaben zu IT-Sicherheit und Datenschutz bereits zu Beginn des Entwicklungsprozesses („Security & Privacy by Design“). Wird ein elektronischer Stromzähler an eine Kommunikationsplattform angeschlossen, entsteht ein intelligentes Messsystem.

Das Smart-Meter-Gateway ermöglicht als zentrale Kommunikationsplattform des intelligenten Messsystems die sichere Umsetzung vielfältiger Anwendungsfälle (engl. „use case“) sowie Szenarien und wird zum Treiber für Innovationen und Digitalisierung. 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.

Die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller gesellschaftlichen Lebensbereiche stellt Staat, Wirtschaft und unsere Gesellschaft vor große Herausforderungen. Die zunehmende Digitalisierung und Vernetzung aller gesellschaftlichen Bereiche führt auf der einen Seite zu Effizienzsteigerungen und Prozessoptimierungen in der Wirtschaft sowie zu mehr Komfort bei den Bürgerinnen und Bürgern, indem Produktkomponenten sowie Systeme untereinander kommunikativ verknüpft werden. 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.

Die Wahrscheinlichkeit erfolgreicher Angriffe auf digitalisierte Infrastrukturen wird folglich zunehmend größer. Daher sind nachweislich sichere Produktkomponenten und Systeme im Netz sowie eine sichere Kommunikationsinfrastruktur entscheidend für das Vertrauen der Anwender. 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 für eine sichere und datenschutzkonforme Digitalisierung. 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. Hierzu müssen neue Technologien in Deutschland entwickelt und erfolgreich eingeführt werden.

Das Gesetz zur Digitalisierung der Energiewende, welches zum 2. September 2016 in Kraft getreten ist, trägt diesen Kernanforderungen Rechnung und schafft deshalb entscheidende Voraussetzungen für den stufenweisen Aufbau einer intelli-

genten Infrastruktur für die Energiewende. Gegenstand des neuen Messstellenbetriebsgesetzes (MsbG) in Artikel 1 ist unter anderem die Festlegung hoher technischer 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.

Die Schaffung verbindlicher Rahmenvorgaben für die Herstellung und den Betrieb von intelligenten Messsystemen ist Grundvoraussetzung für Vertrauen und Akzeptanz in die neue Technik, insbesondere weil personenbezogene Daten verarbeitet werden. Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) entwickelt das BSI daher Anforderungen an vertrauenswürdige Produktkomponenten (Smart-Meter-Gateway mit integriertem Sicherheitsmodul), dessen sicheren IT-Betrieb (Administration) und an die vertrauenswürdige Kommunikationsinfrastruktur (Smart-Metering-Public-Key-Infrastruktur).

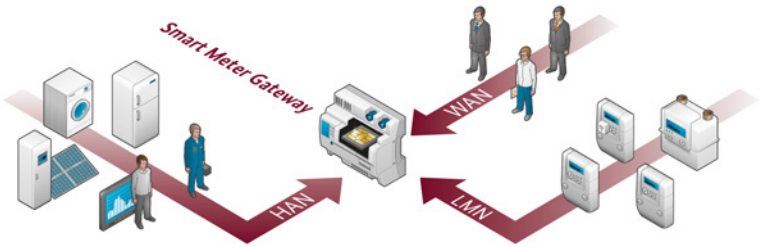
Eingebunden in die Entwicklung wurden verschiedene Verbände aus den Bereichen Telekommunikation, Informationstechnik, Energie, Wohnungswirtschaft und Verbraucherschutz sowie die Datenschutzbeauftragten des Bundes und der Länder, die Bundesnetzagentur und die Physikalisch-Technische Bundesanstalt.

Das Gesetz zur Digitalisierung der Energiewende ermöglicht den kontinuierlichen stufenweisen Ausbau der intelligenten Messsysteme und anderer Komponenten um weitere Anwendungsfälle wie beispielsweise dem netzdienlichen Einspeise- und Lastmanagement von Erzeugern und Verbrauchern, der Integration von weiteren Sparten (Gas, Wasser, Wärme) und der Ladesäuleninfrastruktur im Bereich der Elektromobilität.

2 Systemarchitektur

2 Systemarchitektur

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



Das hat in diesem Gefüge dafür Sorge zu tragen, dass alle Kommunikationsverbindungen verschlüsselt werden und dass nur bekannten Teilnehmern und Geräten vertraut wird.

2.1 Das Lokale Metrologische Netz – LMN

Über das Lokale Metrologische Netz werden die Messeinrichtungen des Letztverbrauchers mit dem Smart-Meter-Gateway 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 Smart-Meter-Gateway kommuniziert über die WAN-Schnittstelle mit allen externen Marktteilnehmern zu denen auch der Smart-Meter-Gateway-Administrator gehört.

Dieser ist sowohl für die Konfiguration des Gateways 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.

Somit können die zuvor empfangenen und verarbeiteten Messwerte zu festgelegten und für den Letztverbraucher einsehbaren Zeitpunkten an die jeweiligen Marktteilnehmer versendet werden.

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 reagieren kann.

2.3 Das Heimnetz – HAN

Die HAN-Schnittstelle ist dem Letztverbraucher zuzuordnen. An dieser kann er steuerbare Geräte, bspw. intelligente Hausgeräte oder Photovoltaikanlagen anschließen, um externen Marktteilnehmern den Zugriff für Steuerungs- oder Fernwartungszwecke zu ermöglichen. Das Smart-Meter-Gateway trägt Sorge dafür, dass Kommunikationsverbindungen zwischen steuerbaren Geräten und Marktteilnehmern gesichert werden.

Darüber hinaus kann der Letztverbraucher über diese Schnittstelle seine Verbrauchs- und ggf. Einspeisewerte abfragen. Er kann hierzu ein entsprechendes Display oder einen PC, ein Tablet oder ein Smartphone anschließen. Der Zugriff auf die Daten erfolgt nach erfolgreicher Authentifizierung ausschließlich lesend.

Ebenfalls über die HAN-Schnittstelle wird einem Servicetechniker die Möglichkeit geboten wichtige Informationen über den Systemzustand des Smart-Meter-Gateways in Erfahrung zu bringen. Diese werden benötigt, um im Fehlerfall die Ursache zu diagnostizieren und das intelligente Messsystem zu entstören. Aus Datenschutzgründen hat er keinen Zugriff auf die im Gateway hinterlegten Messwerte bzw. mandantenspezifischen Daten. Die Konfiguration darf nur über den Administrator über die WAN-Schnittstelle vorgenommen werden.

3 Sicherheitstechnische Anforderungen

3 Sicherheitstechnische Anforderungen

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

Das Schutzprofil beschreibt mögliche Bedrohungen eines Smart-Meter-Gateways in seiner Einsatzumgebung und definiert die Mindestanforderungen für entsprechende Sicherheitsmaßnahmen. Der Aufbau eines Schutzprofils ist in den Common Criteria 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 Smart-Meter-Gateway 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 Smart-Meter-Gateways unterscheidet bezgl. möglicher Bedrohungen anhand des potenziellen Angrei-

fers, 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. Bspw. könnte ein Angreifer über Eingriffe am Gateway versuchen abrechnungsrelevante Daten oder Netzzustandsdaten zu manipulieren. Aber auch Angriffe auf die Systemuhr des Gateways oder das Ausspähen von Verbrauchsdaten gehören mit dazu.

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. Darüber hinaus können erfolgreiche WAN-Angriffe dazu führen, dass ein Angreifer Zugriff auf die Geräteeinstellungen oder -software bekommen könnte.

3.3 Sicherheitsziele

Um den zuvor beschriebenen Bedrohungen entgegen zu wirken, definiert das Schutzprofil eine Reihe von Sicherheitszielen, die durch das Smart-Meter-Gateway 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 (Protection Profiles) 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 Hersteller im CC-Zertifizierungsverfahren nachzuweisen.

Bei gültigem CC-Zertifikat genießen Hersteller und Anwender von SMGW einen insgesamt 8-jährigen Bestandschutz, sofern die Gültigkeit des Zertifikats durch ein Re-Assessment alle 2 Jahre bestätigt wird.

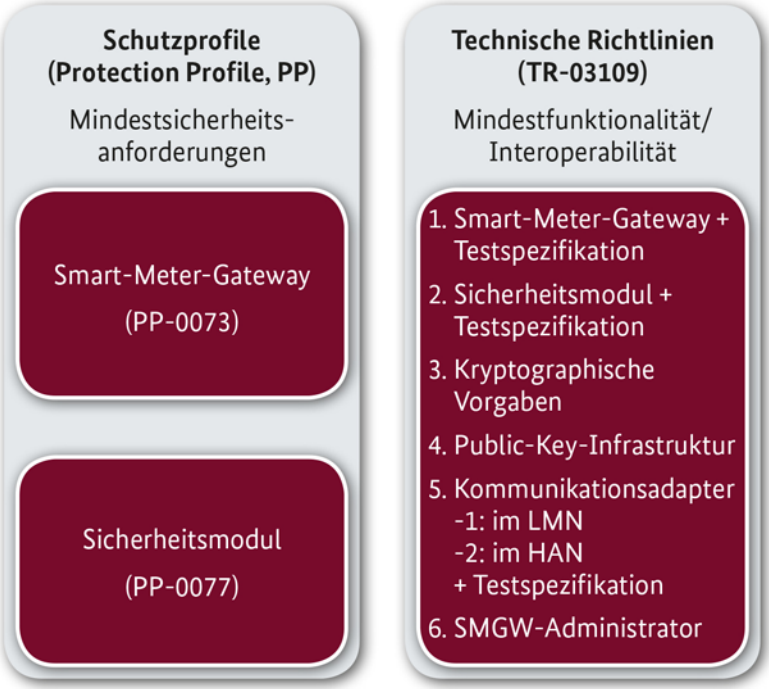
Eine Auflistung der Smart-Meter-Gateway-Hersteller, die sich aktuell im Zertifizierungsverfahren befinden, ist unter dem nachfolgenden Link abrufbar:

Web: www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/SmartMeterGateway/Zertifikate24Msbg/zertifikate24MsbG_node.html

4 Technische Richtlinien 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 Smart-Meter-Gateway und dem Sicherheitsmodul auch der Infrastruktur, bspw. der PKI oder dem Smart-Meter-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 Smart-Meter-Gateway 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 Smart-Meter-Gateway 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 Smart-Meter-Gateway 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 sichergestellt 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 Smart-Meter-Gateway beschrieben.

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

Für den sicheren, technischen Betrieb des intelligenten Messsystems ist der Smart-Meter-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 Smart-Meter-Gateways 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 Smart-Meter-Gateways sowie weiteren technischen Komponenten wie bspw. das im Gateway verbaute Sicherheitsmodul.

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. Im Rahmen der Arbeiten an der Technischen Richtlinie TR-03109-1 v1.0 wurden bereits erste funktionale Anforderungen in Form von Protokollen und technischen Prozessen spezifiziert und in Konsultationsverfahren mit der Branche abgestimmt.

Im Rahmen der Weiterentwicklung der Technischen Richtlinie hin zur Version 1.1 wird dieses Fundament nun um detaillierte technische Vorgaben und Feinspezifikationen erweitert, so dass diese als Basis für Interoperabilitäts- und Konformitätstest dienen können. Flankierend zu den Arbeiten an der Technischen Richtlinie werden parallel umfassende Testfälle für das Smart-

Meter-Gateway 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 Smart-Meter-Gateways ist die Entwicklung und Bereitstellung einer Testsuite zur Durchführung von Konformitätstests für die Prüfstellen des BSI. Das BSI wird daher eine Testsuite bestehend aus Hard- und Software-Komponenten entwickeln, so dass zukünftig neben den Tests des Smart-Meter-Gateways ggf. auch weitere Komponenten des intelligenten Messsystems auf Interoperabilität getestet werden können.

6 Public-Key-Infrastruktur

6 Public-Key-Infrastruktur

Um den Schutz der von den Haushalten übermittelten Messdaten zu gewährleisten, ist für die Verbindung des Smart-Meter-Gateways 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 Smart-Meter-Gateway 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 von Zertifikaten werden von der Root in einer Certificate Policy (Root-CP) festgelegt. In der Root-CP werden organisatorische und technische Anforderungen für die Anerkennung, Ausstellung, Verwaltung, Benutzung, Zurückziehung und Erneuerung von Zertifikaten zur Kommunikation zwischen Gateway und Marktteilnehmern spezifiziert.

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

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

Web: www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/PKI/Registrierte_Sub-CAs/registrierte_sub_cas_node.html

7 IT-Sicherheit bei Administration

7 IT-Sicherheit bei Administration

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 der IT-Grundschutz-Kataloge bzw. dem 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:

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:

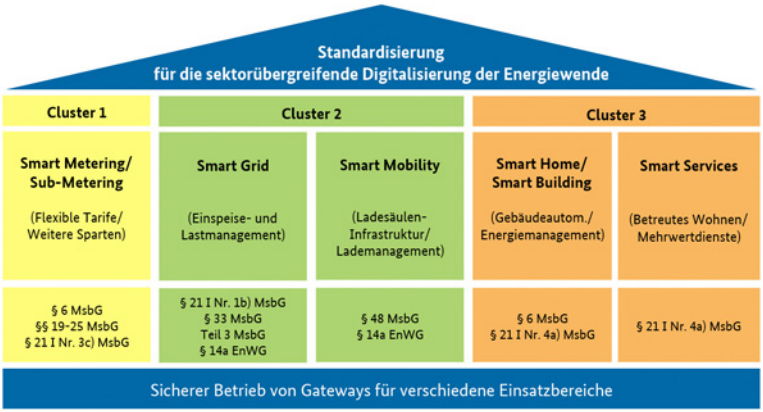
Web: www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/AdministrationBetrieb/Zertifikate25Msbg/zertifikate25MsbG_node.html

8 Ausblick

8 Ausblick

8.1 Fortentwicklung der Vorgaben für die sektorübergreifende Digitalisierung der Energiewende

Das Schutzprofil für das Smart-Meter-Gateway stellt bereits mit seinen Mindestanforderungen die Basis für die Etablierung eines einheitlichen Sicherheitsniveaus im intelligenten Energienetz dar. Die Grundkonzeption ermöglicht es, das Smart-Meter-Gateway als sichere Kommunikationsplattform weiterzuentwickeln, um das erreichte Sicherheitsniveau aufrecht zu erhalten und zugleich für weitere energiewirtschaftliche und für die Energiewende relevante Anwendungsfälle zu öffnen. Der Rechtsrahmen nutzt dies und sieht deshalb weitere Einsatzbereiche für Smart-Meter-Gateways vor. Die nachfolgende Abbildung zeigt einen Überblick über die derzeit adressierten Einsatzbereiche.



Übersicht der Einsatzbereiche für die Digitalisierung der Energiewende

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

» Cluster 1: Smart- & Sub-Metering

» Cluster 2: Smart Grid & Smart-Mobility

» Cluster 3: Smart Home & Building & Services

Im Bereich Smart Metering ist die spartenübergreifende Verbrauchsmessung (Strom, Gas, Wasser, Wärme), die dezentrale Tarifierung sowie im Sinne der Energieeffizienzrichtlinie eine sichere, datenschutzkonforme Visualisierung für den Letztverbraucher erfasst.

Im Bereich Smart Grid stehen die für die Energiewende relevanten Anwendungsfälle zur Erhebung und Übermittlung von Netzzustandsdaten, der Ist-Einspeisung sowie die Fernsteuerung von Anlagen (§ 14a Anlagen, EEG- und KWKG-Anlagen) im Fokus. Das Messstellenbetriebsgesetz zeigt auch über § 48 bereits perspektivisch die Ausgestaltung von verbindlichen Mindestanforderungen zur sicheren Integration der Ladesäuleninfrastruktur von Elektromobilen in das intelligente Netz auf. Die Nutzung der Batterien von Elektromobilen als Stromspeicher und die Erzeugung von Regelenergie, die zum Ausgleich der schwankenden Einspeisung aus Windparks und Solaranlagen gebraucht wird, werden zukünftig eine wichtige Rolle spielen und stehen bezüglich der Anwendungsfälle im engen Zusammenhang mit dem Einsatzbereich Smart Grid. Denn Ladevorgänge von Elektromobilen müssen vorausschauend in Energiemanagementsystemen aufeinander abgestimmt werden, um Netzschwankungen und negative Rückwirkungen in das intelligente Netz zu vermeiden. Die zukünftige Integration des Smart-Meter-Gateways in die Ladesäule ermöglicht ein sicheres und datenschutzkonformes Laden und Abrechnen. Neben Anforderungen an die Ladesäule und an die Gesamtsystemarchitektur sind daher sichere Authentisierungsverfahren, eine sichere Administration und Betrieb der Ladepunkte, eine

datenschutzkonforme Messwertverarbeitung sowie die Notwendigkeit einer vertrauenswürdigen Kommunikationsinfrastruktur entscheidend.

Für weitere Einsatzbereiche formuliert das Messstellenbetriebsgesetz (MsbG) nach § 21 Abs.1 Nr. 4a lediglich die Anforderung, dass das Smart-Meter-Gateway „offen" für mögliche Anwendungen und Mehrwertdienste sein muss. Es handelt sich daher um ein Angebot an die Anbieter aus diesen Bereichen, das Smart-Meter-Gateway zukünftig als Plattform für ihre Dienstleistungen zu verwenden, um so den Nutzen und die Akzeptanz beim Letztverbraucher weiter zu erhöhen. Konkrete Dienstleistungen sind daher durch den Markt zunächst selbst zu entwickeln. Damit diese Mehrwertdienste (z. B. im Bereich Smart Home) auf dem Smart-Meter-Gateway aufsetzen können, stellt das Smart-Meter-Gateway bereits jetzt einen sicheren Kommunikationskanal zur Verfügung.

Für die Weiterentwicklung des Smart-Meter-Gateways z. B. um zukünftig benötigte Funktionalitäten bedarf es daher eines Dialogprozesses, der durch die Arbeitsplanung der Roadmap „Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende" näher beschrieben werden wird. Die gesetzlichen Anforderungen werden nach und nach vom BSI über detaillierte Standardvorgaben für modulare Smart-Meter-Gateway-Komponenten spezifiziert.

8.2 Marktanalyse nach § 30 MsbG

Der mit dem Gesetz zur Digitalisierung der Energiewende verankerte Rechtsrahmen zur Einführung intelligenter Messsysteme nach BSI-Standard gibt keine starren Fristen für den Beginn des Rollouts vor. Der „Startschuss" für den Rollout und damit die Pflicht zum Einbau eines Smart-Meter-Gateways

wird nach § 30 MsbG jeweils erst dann aktuell, wenn für den konkreten Anwendungsfall die technische Möglichkeit des Einbaus und dessen sicheren Betrieb besteht. Erforderlich hierfür ist nach § 30 MsbG eine am Einsatzbereich des Smart-Meter-Gateways durchgeführte Prüfung des BSI, die sogenannte Marktanalyse.

Für den Beginn des Rollouts von Smart-Meter-Gateways steht neben dem vom Gesetz geforderten Funktionsumfang der Nachweis der geleisteten Sicherheitsfunktionalität im Rahmen des CC-Zertifizierungsverfahrens für die verordneten Anwendungsbereiche im Vordergrund. Nach der gesetzlichen Regelung müssen mindestens Smart-Meter-Gateways von 3 unterschiedlichen Herstellern erfolgreich das CC-Zertifizierungsverfahren durchlaufen haben. Das vom Gesetz vorgesehene Verfahren soll den hohen Qualitäts- und Sicherheitsstandards für die auszurollende Technik sicherstellen sowie den Wettbewerb zwischen den Herstellern gewährleisten. Zusätzlich werden neben dem Status der Produktzertifizierungen auch die Umsetzung der Vorgaben für den Administrator und der Smart Metering - PKI geprüft. Abschließend sind die Festlegungen der Bundesnetzagentur zur Marktkommunikation für das zugrundeliegende Marktkommunikationsmodell nach § 60 MsbG und ihre Umsetzung im Markt relevant.

Unter der Voraussetzung, dass die technische Möglichkeit durch das BSI festgestellt wird, adressiert § 31 MsbG verschiedene Einbaugruppen zu unterschiedlichen Zeitpunkten. Hierzu wird das BSI die Ergebnisse der Marktanalyse zu den betrachteten Einbaugruppen und Einsatzbereichen auf der Internetseite (www.bsi.bund.de/SmartMeter) veröffentlichen.

9 Fazit

9 Fazit

Das Gesetz zur Digitalisierung der Energiewende schafft über Vorgaben für die Standardisierung, den Rollout intelligenter Messsysteme und die Datenkommunikation die Basis für den Aufbau einer modernen digitalen Infrastruktur für die Energiewende.

Im Fokus steht hierbei das Smart-Meter-Gateway als sichere und datenschutzkonforme Kommunikationsplattform für die Energiewende relevante 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.

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

Web: www.bsi.bund.de/SmartMeter

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 2018

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Titelbild: Getty Images / aaaaimages
Seite 9: Fotolia / marco2811
Seite 28: Fotolia / Maksim Kabakou
Seite 31: Fotolia / tournee

Artikelnummer
BSI-Bro18/332

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI; sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

www.bsi.bund.de