



Bundesamt
für Sicherheit in der
Informationstechnik



Das Smart-Meter-Gateway

Sicherheit für intelligente Netze

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	17
3.3 Sicherheitsziele	17
4 Technische Richtlinie TR-03109	20
4.1 TR-03109-1 Anforderungen an die Interoperabili- tät 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

<u>5</u>	Funktionale Anforderungen	25
<u>6</u>	Public-Key-Infrastruktur (PKI)	28
<u>7</u>	Informationssicherheit bei Administration und Betrieb	31
<u>8</u>	Ausblick	35
8.1	Fortentwicklung der Vorgaben zur IT-Sicherheit und Interoperabilität im intelligenten Energienetz	35
8.2	Ausblick zum Rechtsrahmen	36
<u>9</u>	Fazit	38

Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.



Mit seinen derzeit rund 600 Mitarbeiterinnen und Mitarbeitern und 80 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Als zentraler IT-Sicherheitsdienstleister des Bundes ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und ist dadurch eine tragende Säule der Inneren Sicherheit in Deutschland.

Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. IT-Sicherheit soll als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Das BSI wendet sich mit seinem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppe sind die öffentlichen Verwaltungen in Bund, Ländern und Kommunen sowie Privatanwender und Unternehmen.

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

Angesichts knapper werdender Rohstoffe und der damit zunehmenden Bedeutung erneuerbarer Energien ist die Energieversorgung in Deutschland aber auch im Rest Europas 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, durch ihre wetterabhängige Einspeisung zu schwer vorhersehbaren Schwankungen und erheblichen Herausforderungen für die Stabilität im Stromnetz. Da elektrische Energie nur begrenzt gespeichert werden kann, steht die Energieversorgung vor einem Paradigmenwechsel: War es bisher üblich, genauso viel Strom zu erzeugen wie verbraucht wurde, so soll zukünftig möglichst dann Energie konsumiert werden, wenn diese zur Verfügung steht. Basis einer solchen 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 sowie elektronische Verbrauchsgeräte und Erzeugungsanlagen so steuern, 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. Die zukünftigen Energieversorgungssysteme, insbesondere die dafür verwendeten intelligenten Messsysteme, erfordern somit verbindliche und einheitliche sicherheitstechnische Vorgaben sowie funktionale Anforder-



rungen zur Wahrung der Interoperabilität. Das BSI entwickelt für diesen Bereich Schutzprofile nach Common Criteria (CC – Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie) sowie Technische Richtlinien, die eine international vergleichbare Sicherheitszertifizierung der entsprechenden Geräte ermöglichen. Hierdurch nimmt Deutschland bei der Umsetzung von sicheren, intelligenten Messsystemen in Europa eine Vorreiterrolle ein.

Das BSI wurde im September 2010 vom Bundesministerium für Wirtschaft und Energie (BMWi) beauftragt, Schutzprofile (Protection Profile, PP) sowie daran anschließend Technische Richtlinien (TR) für die Kommunikationseinheit eines intelligenten Messsystems (Smart-Meter-Gateway) zu erarbeiten, um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure zu gewährleisten.

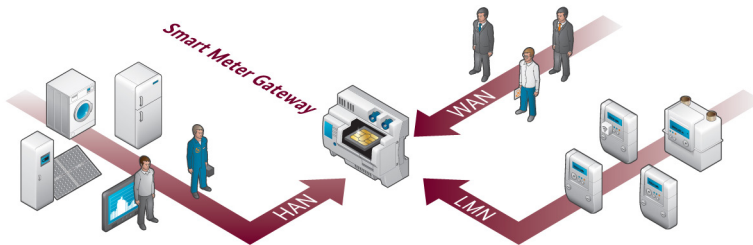
Sicherheitsstandards können nur dann erfolgreich sein, wenn sie auf breite Akzeptanz bei Herstellern und Anwendern stoßen. Daher hat das BSI diese von Anfang an in die Erstellung und Weiterentwicklung der Schutzprofile und der Technischen

Richtlinien eingebunden. In mehreren Kommentierungsrunden konnten Verbände aus den Bereichen Telekommunikation, Energie, Informationstechnik, Wohnungswirtschaft und Verbraucherschutz umfangreich und maßgeblich an den Dokumenten mitwirken.

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 Marktteilnehmer den Zugriff für Steuerungs- oder Fernwartungszwecke zu ermöglichen. Das Smart-Meter-Gateway trägt Sorge dafür, dass Kommunikationsverbindungen zwischen steuerbaren Geräten und Marktteilnehmer 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 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. 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 sicher-

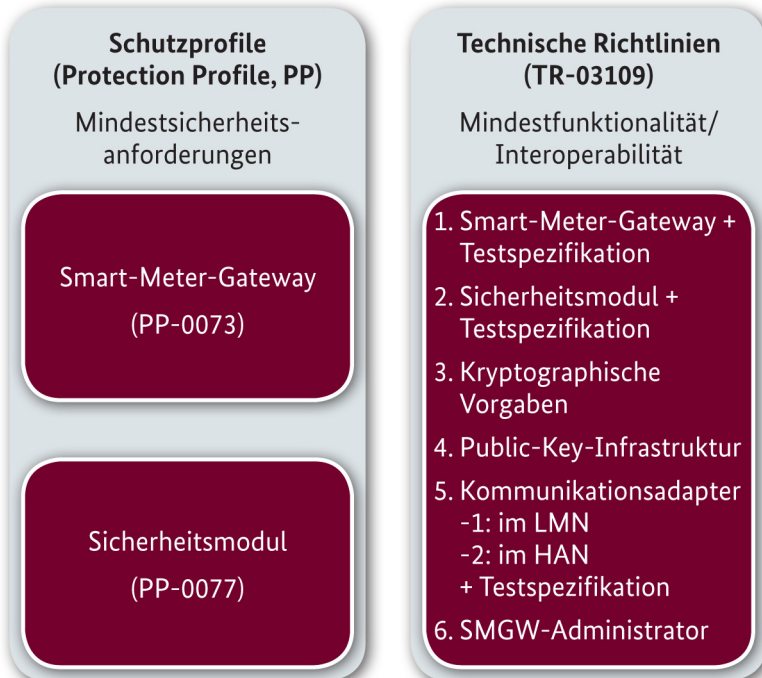
gestellt werden, dass nur Kommunikationsverbindungen von innen nach außen aufgebaut werden können. Daneben werden sämtliche Kommunikationsflüsse, unabhängig in welches Netz kommuniziert wird, nach einer gegenseitigen Authentifizierung grundsätzlich verschlüsselt und integritätsgesichert.

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.

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 Funktionale Anforderungen

5 Funktionale Anforderungen

Neben den sicherheitstechnischen Vorgaben aus dem Schutzprofil muss das Smart-Meter-Gateway ebenfalls funktionale Anforderungen erfüllen. Der Fokus liegt hierbei sowohl auf der Ausgestaltung der Anforderungen aus dem Schutzprofil als auch auf der herstellerübergreifenden Interoperabilität.

Die Technische Richtlinie TR-03109-1 spezifiziert zu allen vier physischen Schnittstellen entsprechende Kommunikationsprotokolle, die mindestens umzusetzen sind. Die Basis für alle Schnittstellen bildet hierbei das Transport Layer Security (TLS) Protokoll, das zur Sicherstellung von Vertraulichkeit, Authentizität und Integrität bei der Übertragung von Daten in unsicheren Netzwerken dient.

An der WAN-Schnittstelle fordert die Technische Richtlinie die Nutzung von WebServices und XML-basierten Datenformaten (RESTful WebServices und COSEM-basiertes Objektmodell), über die der Zugriff auf Anwendungsebene erfolgt.

Die LMN-Schnittstelle untergliedert sich in eine drahtgebundene sowie in eine drahtlose Variante. Auf der drahtgebundenen Seite kommt ein auf EIA-485 basierender Bus zum Einsatz, der um das HDLC, SML, COSEM sowie das TLS-Protokoll erweitert wurde. Für die drahtlose Variante fordert die Technische Richtlinie den Einsatz des wireless M-BUS; dieser wurde jedoch um einige zusätzliche kryptographische Anforderungen erweitert, so dass dieser auch für zukünftige Szenarien einsetzbar ist.

Die Technische Richtlinie spezifiziert an der HAN-Schnittstelle als Mindestanforderung eine Ethernet-Schnittstelle mit DHCP, TCP/IP und TLS. Zukünftig sollen auch hier weitere proto-

kolltechnische Vorgaben konkretisiert werden, bspw. für den Anschluss eines Kundendisplays oder steuerbarer Geräte.

Um das Erzeugen von detaillierten Nutzerprofilen und das damit verbundene Ausforschungspotenzial in Bezug auf die Lebensgewohnheiten des Endkunden zu verhindern, enthält die Technische Richtlinie Anforderungen zur datenschutzkonformen Abbildung der Tarifierungslogik. Hierzu werden in der Technischen Richtlinie zwölf detaillierte Tarifierungsfälle beschrieben und erläutert, wie die Tarifierung im Gateway von der Messwerterfassung über die eigentliche Tarifierung bis hin zum Versand der Messwerte an die entsprechenden Marktteilnehmer technisch zu erfolgen hat. Zur Umsetzung einer dezentralen Tarifierung führt das Gateway notwendige Berechnungen zur Verbrauchsermittlung in Tarifzonen selbst durch, so dass damit ausschließlich abrechnungsrelevante Werte das Gateway verlassen. Damit müssen keine hoch aufgelösten Verbrauchsdaten zur Tarifierung an Dritte weitergeleitet werden und das Ziel der Datensparsamkeit und Datenvermeidung wird erreicht.

Ebenfalls finden sich in der Technischen Richtlinie Anforderungen an die Zeitsynchronisation zwischen Gateway und dem dazugehörigen Administrator, Vorgaben zum Einbau des Sicherheitsmoduls und dem Pairing mit dem Gateway-Prozessor sowie dem Logging von system- und eichrechtlich relevanten Ereignissen.

6 Public-Key- Infrastruktur (PKI)

6 Public-Key-Infrastruktur (PKI)

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.

Das gewählte Modell der PKI sieht eine zentrale, staatliche Root (Wurzel) als Vertrauensanker in der Infrastruktur der Gateways vor. Darunter liegend operieren private Unternehmen, sogenannte Sub-CAs (untergeordnete Zertifizierungsstellen), welche die Betreuung



der Marktteilnehmer übernehmen. Die Root setzt die gesetzlichen Anforderungen auf technischer Ebene durch und berechtigt die privaten Unternehmen eine Sub-CA zu betreiben. 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 Anforderun-

gen für das Anerkennen, Ausstellen, Verwalten, Benutzen, Zurückziehen und Erneuern 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 Zertifizierungsdienstanbieter durchgeführt. Des Weiteren werden den Marktteilnehmern zusätzlich zur Root verschiedene Testsysteme zur Ausgabe von digitalen Test-Zertifikaten bereitgestellt.

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. Daher 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. Folglich sind einheitliche organisatorische und technische Anforderungen sowie Maßnahmen für die Mindestsicherheit beim Administrator erforderlich, die in der Technischen Richtlinie TR-03109-6 festgelegt sind.



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 vorher 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. Sowohl im behördlichen Umfeld als auch im privatwirtschaftlichen Bereich hat sich der IT-Grundschutz als Standard zur 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 100-2) 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.

8 Ausblick

8 Ausblick

8.1 Fortentwicklung der Vorgaben zur IT-Sicherheit und Interoperabilität im intelligenten Energienetz

Das Schutzprofil für das Smart-Meter-Gateway stellt bereits mit seinen Mindestanforderungen die Basis für die Etablierung eines einheitlichen Sicherheitsniveaus im intelligenten Energienetz dar. Aufgrund der verschiedenen Einsatzszenarien und adressierten Anwendungsfälle im Zuge des Gesetzes zur Digitalisierung der Energiewende wurden nun neue und zusätzliche Anforderungen an das Smart-Meter-Gateway und den angeschlossenen Komponenten gestellt. Um das Smart-Meter-Gateway im Sinne einer sicheren und interoperablen Kommunikationsplattform für das intelligente Energienetz weiterzuentwickeln, müssen zuerst die sichere Kommunikation von netzdienlichen Informationen, von Stromverbrauchs- und Erzeugungswerten sowie das sichere Bewirken von Last- und Einspeisemanagement ermöglicht werden.

Um das volle Potenzial einer sicheren und standardisierten Kommunikationsplattform zu entfalten, müssen perspektivisch auch die Fähigkeiten zur Messung anderer Sparten (Wasser, Wärme) und die Umsetzung von sich aktuell entwickelnden Mehrwertdiensten z. B. in den Bereichen Gebäudeautomatisierung, Smart Home und betreutes Wohnen folgen. Die Entwicklung von zusätzlichen Sicherheits- und Interoperabilitätsanforderungen für Spezialanwendungen (Groß-Gasmessanlagen, Strom-Großverbraucher, Wind- und PV-Parks) sowie die sichere Anbindung von dezentralen Komponenten der Ladesäulen-Infrastruktur schließt sich dem unter Berücksichtigung internationaler Standards an.

Bei der Weiterentwicklung müssen alle bisher beteiligten Ressorts, Partnerbehörden, Hersteller und Anwender eingebunden werden, so dass ein zielgerichteter Rollout von intelligenten Messsystemen auch von den Beteiligten getragen und gesteuert werden kann. Das Verbandsanhörungsverfahren mit den entsprechenden fachlichen Arbeitsgruppen des BSI hat sich im Zuge der Entwicklung der Schutzprofile und der Technischen Richtlinie erfolgreich bewährt und wird dementsprechend für die Weiterentwicklung fortgesetzt werden.

8.2 Ausblick zum Rechtsrahmen

Mit dem Gesetz zur Digitalisierung der Energiewende wurde die sachgerechte gesetzgeberische Entscheidung getroffen, die Rechtsmaterie vollständig in ein einheitliches Gesetz außerhalb des Energiewirtschaftsgesetzes zu überführen. Dies dient insbesondere der Verfahrensklarheit und ermöglicht auch Regelungen außerhalb des Rechts der Energieversorgung mit Strom und Gas (z. B. im Bereich Smart Home, Fern- und Heizwärme) festzulegen.

Gegenstand des neuen Stammgesetzes über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG) werden die Festlegung der technischen Vorgaben des BSI zur Gewährleistung von Datenschutz und Datensicherheit (§§ 19 bis 28 in Artikel 1 – ehemals Entwurf zur Messsystemverordnung), bereichsspezifischer Datenschutzregeln für die Marktkommunikation sowie Regelungen im Zusammenhang mit dem Einbau und der Finanzierung von intelligenten Messsystemen sein.

9 Fazit

9 Fazit

Intelligente Messsysteme sind wichtige Bausteine im intelligenten Verteilnetz und benötigen „Security & Privacy by Design“. Die beiden Schutzprofile und die Technische Richtlinie TR-03109 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 Informationen zu den beiden Schutzprofilen und der Technischen Richtlinie TR-03109 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

Oktober 2015

Druck

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

Texte und Redaktion

Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis

Titelbild: Fotolia / Aania

Seite 9: Fotolia / marco2811

Seite 28: Fotolia / Maksim Kabakou

Seite 31: Fotolia / tournee

Artikelnummer

BSI-Bro15/332

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

