Bundesamt
für Sicherheit in der
Informationstechnik

Das Smart Meter Gateway

Sicherheit für intelligente Netze

Inhaltsverzeichnis

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 88 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 und 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, 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 Anforderungen 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.

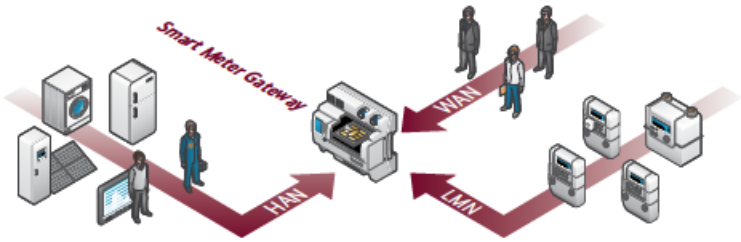
Das BSI wurde im September 2010 vom Bundeswirtschaftsministerium beauftragt, zwei Schutzprofile (Protection Profile, PP) sowie daran anschließend eine Technische Richtlinie (TR) für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway) zu erarbeiten, um einen einheitlichen technischen 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 beiden Schutzprofile und der Technischen Richtlinie eingebunden. In mehreren Kommentierungsrunden konnten Verbände aus den Bereichen Telekommunikation, Energie, Informationstechnik, Wohnungswirtschaft und Verbraucherschutz umfangreich und maßgeblich an beiden Dokumenten mitwirken. Insgesamt hat das BSI etwa 1.200 Kommentare zu den beiden Schutzprofilen und mehr als 3.100 Kommentare zur Technischen Richtlinie verzeichnet. Diese Zahlen belegen das hohe Interesse, das dem Thema in Fachkreisen und zunehmend auch in der Politik beigemessen wird.

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, Verteilnetzbetreiber oder Messstellenbetreiber) im Weitverkehrsnetz (WAN) und dem lokalen Heimnetz (HAN) verbindet.



Das Smart Meter Gateway 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 an das Gateway, wo sie gespeichert und weiterverarbeitet werden.

Das Gateway nutzt je nach Tarif des Kunden unterschiedliche Regelwerke, um die empfangenen Messwerte unter dem Gesichtspunkt 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 (SMGW-Admin) 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 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 Smart Meter 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 SMGW-Admin das Gateway über einen Wake-Up Dienst zu einem Verbindungsaufbau anstoßen.

Dabei handelt es sich um ein vom Smart Meter Gateway 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 (CLS), bspw. intelligente Hausgeräte oder eine Photovoltaikanlage anschließen, um externen Marktteilnehmer den Zugriff für Steuerungs- oder Fernwartungszwecke zu ermöglichen. Das Smart Meter Gateway trägt Sorge dafür, dass Kommunikationsverbindungen zwischen CLS 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 aber einen PC oder Tablet-Lösung 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 bringen. Diese werden benötigt, um im Fehlerfall die Ursache zu diagnostizieren und das Messsystem zu entstören. Aus Datenschutzgründen hat er keinen Zugriff auf die im Gateway hinterlegten Messwerte bzw. mandantenspezifische Daten. Die Konfiguration darf nur über den Smart Meter Gateway Administrator über die WAN-Schnittstelle vorgenommen werden.

3 Sicherheitstechnische Anforderungen

3 Sicherheitstechnische Anforderungen

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

Ein Schutzprofil legt strukturiert Bedrohungen für den sicheren und (hier insbesondere auch datenschutzfreundlichen) Betrieb dar 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 logischen 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 enthält eine Reihe von Bedrohungen, denen das Smart Meter Gateway in seiner Einsatzumgebung ausgesetzt ist. Unterschieden werden diese anhand des potentiellen Angreifers, der auf das Gateway einwirken möchte. Zum einen gibt es den lokalen Angreifer, der vor Ort direkten Zugriff auf das Smart Meter Gateway besitzt, um somit das Gateway auf physikalischem 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 Gateway ein hohes Angriffspotential für Angreifer die von außen versuchen das Gateway angreifen zu wollen. Die potentiellen 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 Gateway umgesetzt werden müssen.

Um seiner Rolle als Bindeglied zwischen drei unterschiedlichen Netzen gerecht zu werden, schottet das Gateway die Netze gegeneinander ab. Hierzu sind seitens des Herstellers Firewall-Mechanismen in das Gateway zu integrieren. Neben der logischen Separierung der jeweiligen Netze 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.

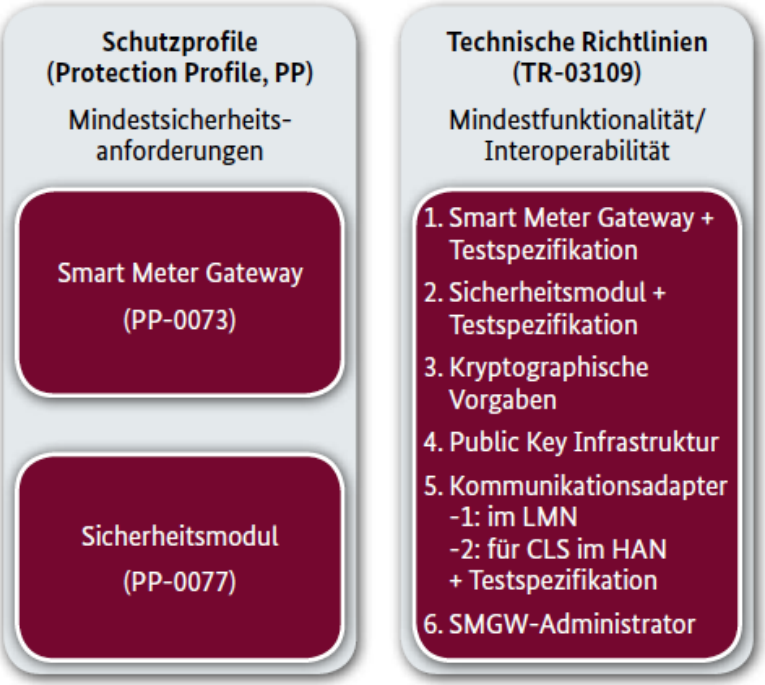
Ein besonderes Augenmerk legt das Schutzprofil auf die Kommunikation zu den angeschlossenen Zählern. Das Gateway stellt hierfür Funktionen zum Empfang und zur Abfrage von Einspeise- und Verbrauchswerten in konfigurierbaren Zeitintervallen zur Verfügung.

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 finden sich in der Technischen Richtlinie BSI TR-03109 für den sicheren Einsatz von Smart Meter Gateways 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 WAN, LMN und HAN untergliedert und definiert für diese Bereiche detaillierte technische Vorgaben für diese Kommunikationsschnittstellen. Darüber hinaus werden interne, logische Abläufe (bspw. die Tarifierung anhand von Regelwerken) weiter ausgeführt. In den Anhängen zum Teil 1 finden sich zusätzlich Prozessbeschreibungen für den Datenaustausch zwischen Gateway und SMGW-Admin.

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, das das Gateway vor allem bei der Nutzung von asymmetrischen, kryptographischen Primitiven unterstützen soll. Daneben dient das Sicherheitsmodul als zentraler Vertrauensanker und bietet mit in seinem Inneren einen sicheren Schlüsselspeicher für das private Schlüsselmaterial des Gateways. 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, Primitiven 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. Da es sich bei der Kommunikation mit dem SMGW um eine M2M-Kommunikation handelt, werden keine Zertifikate für die Schlüssel von Personen, sondern ausschließlich für die Schlüssel von Maschinen ausgestellt.

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 IT-Sicherheit 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 IT-Betrieb beim SMGW-Admin Mindestanforderungen zur Durchsetzung der Informationssicherheit genügt. In der TR-03109-6 werden zukünftig die Aufgaben und Anwendungsfälle zum Betrieb beim Administrator (Anlage V zur TR-03109-1) um eine Schutzbedarfsanalyse ergänzt und um weitere Sicherheitsanforderungen konkretisiert 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 den Einsatz von RESTful WebServices, über diese der Zugriff aus das COSEM-basierte Objektmodell 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 er 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 protokolltechnische Vorgaben konkretisiert werden, bspw. für den Anschluss eines Kundendisplays oder steuerbaren Geräten.

Um das Erzeugen von detaillierten Nutzerprofilen des Endkunden zu verhindern und das damit verbundene Ausforschungspotential in Bezug auf Lebensgewohnheiten auf ein Minimum

zu reduzieren, enthält die Technische Richtlinie Anforderungen zur datenschutzkonformen Abbildung der Tarifierungslogik. Hierzu enthält die TR zwölf detaillierte Tarifanwendungsfälle, bspw. datensparsame, last- oder zeitvariable Tarife. Darüber hinaus wird erläutert wie die Tarifierung im Smart Meter Gateway, von der Messwerterfassung, über die eigentliche Tarifierung bis hin zum Versand der Messwerte an die entsprechenden Marktteilnehmer, in Form von Regelwerken zu erfolgen hat.

Ebenfalls finden sich in der Technischen Richtlinie Anforderungen an die Zeitsynchronisation zwischen Smart Meter Gateway und dem dazugehörigen Administrator, Vorgaben zum Einbau des Sicherheitsmoduls und dem Pairing mit dem SMGW 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 (WAN) 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.

Das gewählte Modell der PKI sieht eine zentrale, staatliche Root (Wurzel) als Vertrauensanker in der Infrastruktur der Smart Meter Gateways vor. Darunterliegend 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 Anforderungen für das Anerkennen, Ausstellen, Verwalten, Benutzen, Zurückziehen und Erneuern von Zertifikaten zur Kommunikation zwischen SMGW und Marktteilnehmern spezifiziert.

Die von der PKI herausgegebenen Zertifikate sind für den zukünftigen Betrieb von entscheidender Bedeutung und bilden insbesondere die Grundlage für Hersteller von Smart Meter Gateways und Infrastrukturkomponenten zur Entwicklung von Prototypen und zur Durchführung von Pilotprojekten.

Als Inhaber der entsprechenden Wurzelzertifikate wurde das BSI ausgewählt. Ergänzend dazu wird das BSI eine Testzertifizierungsstelle (Test-Sub-CA) für die Endnutzer zur Verfügung stellen, um die frühzeitige Durchführung von Interoperabilitätstests zu ermöglichen.

7 IT-Sicherheit bei Administration und Betrieb

7 IT-Sicherheit bei Administration und Betrieb

Für den sicheren, technischen Betrieb des intelligenten Messsystems ist der Smart Meter Gateway Administrator verantwortlich. Der SMGW-Admin muss nach der Technischen Richtlinie TR-03109 einen technisch zuverlässigen Betrieb des Messsystems gewährleisten und organisatorisch sicherstellen. Zu diesem Zweck ist der SMGW-Admin für die Installation, Inbetriebnahme, Konfiguration, Administration, Überwachung und Wartung des Smart Meter Gateways und der informationstechnischen Anbindung von Messgeräten und von anderen an das Smart Meter Gateway angebundenen technischen Einrichtungen verantwortlich. Daher muss sichergestellt sein, dass der IT-Betrieb beim SMGW-Admin Mindestanforderungen zur Durchsetzung der Informationssicherheit genügt.

Zur Gewährleistung der IT-Sicherheit ist der SMGW-Admin dazu verpflichtet ein ISMS nach ISO 27001 einzurichten, zu betreiben und zu dokumentieren. Ergänzend können branchenspezifische Sicherheitsstandards wie z.B. die DIN SPEC 27009 berücksichtigt werden, soweit diese anwendbar ist. Dabei muss der BSI-Standard 100-2 mit den IT-Grundschutz-Katalogen zur Erstellung der Sicherheitskonzeption und zur Umsetzung der entsprechenden Maßnahmen angewendet werden. BSI Standard 100-1 (ISMS) und BSI Standard-3 (Risikoanalyse) können angewendet werden. Als Nachweis der Einhaltung der Vorgaben ist ein Zertifikat des BSI notwendig.

ISO 27001 auf der Basis von IT-Grundschutz umfasst eine Prüfung des ISMS sowie eine über ISO 27001 hinausgehende Bewertung konkreter Sicherheitsmaßnahmen anhand der IT-Grundschutz-Kataloge. Sowohl im behördlichen Umfeld als auch in 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 Zusammenspiel mit den IT-Grundschutz-Katalogen wird in der IT-Grundschutz-Vorgehensweise nicht nur erklärt, was gemacht werden sollte, sondern es werden auch konkrete Hinweise gegeben, wie eine Umsetzung (auch auf technischer Ebene) aussehen kann.

In Abstimmung mit den beteiligten Marktakteuren werden die Aufgaben und Anwendungsfälle des SMGW-Admins durch das BSI zukünftig um eine Schutzbedarfsanalyse ergänzt und um weitere Sicherheitsanforderungen in der Technischen Richtlinie TR-03109 konkretisiert.

8 Ausblick

8 Ausblick

Der Referentenentwurf zur Verordnung über technische Mindestanforderungen an den Einsatz intelligenter Messsysteme (Messsystemverordnung – MsysV) nach § 21i Energiewirtschaftsgesetz (EnWG) hat gemeinsam mit den beiden Schutzprofilen SMGW (BSI-CC-PP-0073 V1.2) und Sicherheitsmodul (BSI-CC-PP-0077 V1.0) sowie der Technischen Richtlinie TR-03109 (V1.0) am 23. September 2013 das europäische Notifizierungsverfahren nach EU-Richtlinie 98/34/EG erfolgreich durchlaufen. Für eine Verabschiedung der Messsystemverordnung und die damit einhergehende Verrechtlichung von Schutzprofil und Technischer Richtlinie ist nun nach einem Kabinettbeschluss noch die Zustimmung des Bundestages und des Bundesrates erforderlich.

Am 30. Juli 2013 wurden zudem die Ergebnisse der Kosten-Nutzen-Analyse (KNA) durch das BMWi/Ernst & Young vorgestellt. Die Kosten-Nutzen-Analyse steckt das Mengengerüst und den Kostenrahmen für den Roll-Out intelligenter Messsysteme ab und gibt einen Ausblick auf die zu erwartenden Festlegungen des noch ausstehenden Verordnungsrahmens zum EnWG.

Insbesondere im Einspeise- und Lastmanagement wird ein hohes Potential von Smart Metering festgestellt, so dass eine Erweiterung der Pflichteinbaufälle auf alle EEG- und KWK-Alt- und Neuanlagen größer 0,25 Kilowatt empfohlen wird. Durch eine Steuerung von dezentralen Lasten und Erzeugern über intelligente Messsysteme können im Gegenzug Einsparungen beim Netzausbau in den Verteilernetzen erzielt werden. Bis 2022 könnte nach Prognose der Kosten-Nutzen-Analyse ein Roll-Out von 11,9 Mio. intelligenten Messsystemen erreicht werden.

9 Fazit

9 Fazit

Intelligente Messsysteme sind wichtige Bausteine im intelligenten Verteilnetz und benötigen „Security 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
Februar 2014

Druck
WM Druck + Verlag
53359 Rheinbach

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Artikelnummer
BSI-Bro14/332

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

www.bsi.bund.de