PTB-Anforderungen 50.8 an BSI-zertifizierte Smart Meter Gateways

Ulrich Grottker*, Marko Esche, Marco Elfroth*****

Einleitung

Vor dem Hintergrund des novellierten Energiewirtschaftsgesetzes (EnWG) [1] hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Schutzprofil [2] auf Basis der Norm ISO/IEC 15408 „Common Criteria“ (Protection Profile, PP) sowie eine Technische Richtlinie (TR) [3] für eine Kommunikationseinrichtung (Gateway) entwickelt, das sich zwischen einem lokalen Netzwerk mit Verbrauchszählern, wie Elektrizitäts- und Gaszählern und einem lokalen Hausnetzwerk und dem Internet befindet. Da in dem Smart Meter Gateway (SMGW) aus den von Zählern gemessenen Messwerten neue Messwerte gebildet werden, die der Abrechnung des Energieverbrauchs nach unterschiedlichen Tarifmodellen dienen, unterliegt dieses Gateway auch dem Eichrecht. Die eichrechtlichen Anforderungen an das Gateway wurden in den PTB-Anforderungen 50.8 [4] formuliert. Diese Anforderungen sind abgeleitet aus dem geltenden Mess- und Eichgesetz und der zugehörigen Verordnung.

BSI und PTB sind bezüglich ihrer Aufgaben jeweils in einem anderen Rechtsrahmen beauftragt. Daher ist eine vollständige Integration der eichrechtlichen Anforderungen in die Technische Richtlinie und in das Schutzprofil nicht möglich. Es wurde aber in der Entstehungsphase der BSI-Dokumente sichergestellt, dass eichrechtliche Aspekte in PP/TR übernommen wurden, soweit es für das Konzept des BSI erforderlich war. Die PTB-A 50.8 stellen deshalb die metrologische Ergänzung zu den Schutzprofilen und der Technischen Richtlinie des BSI dar. In der Praxis bedeutet dies, dass bereits ein großer Teil der Prüfungen zur Konformitätsbewertung nach MessEG im Rahmen einer Prüfung durch eine BSI-Prüfstelle abgedeckt wird und nicht wiederholt werden muss.

Anforderungen an das Messsystem – rechtlich relevante Komponenten

Trotz der unterschiedlichen Rechtsrahmen sind technische Konzepte möglich und auch bereits entwickelt worden, die beiden gerecht werden,

* Dr. Ulrich Grottker, Arbeitsgruppe 8.51 “Metrologische Software”, E-Mail: ulrich.grottker@ptb.de

** Dr. Marko Esche, Arbeitsgruppe 8.51 “Metrologische Software”, E-Mail: marko.esche@ptb.de

*** Marco Elfroth, Arbeitsgruppe 8.51 “Metrologische Software”, E-Mail: Marco.Elfroth@ptb.de

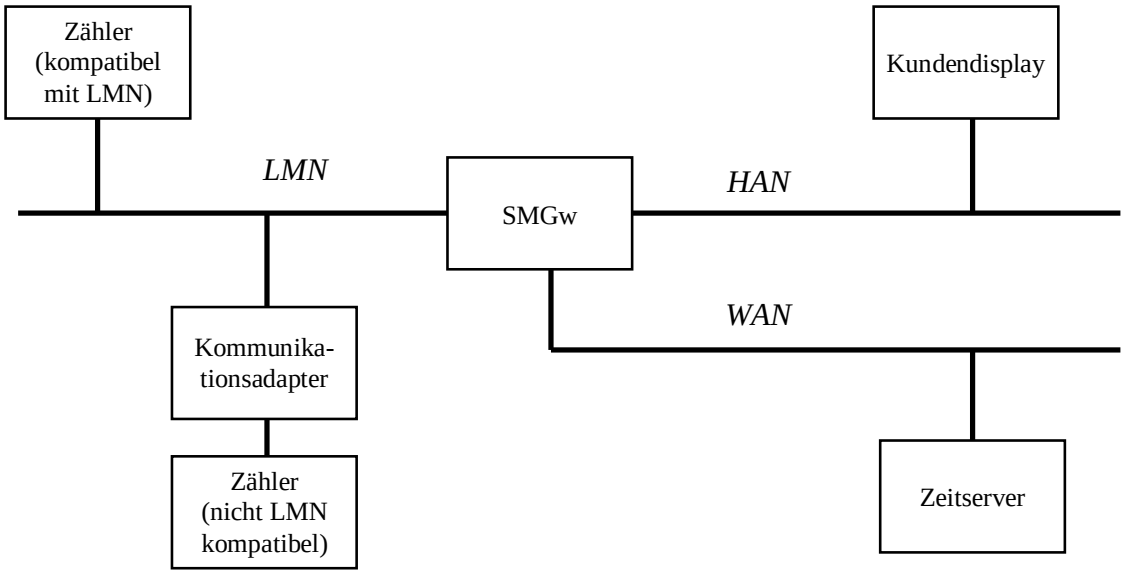

Bild 1:
Messsystem mit Smart Meter Gateway (SMGW) unter eichrechtlicher Betrachtung

wie im Folgenden dargelegt wird. Bezüglich der Definition des Prüfgegenstandes gibt es aber für eine BSI-Prüfstelle und für eine Konformitätsbewertungsstelle nach MessEG [5] keine volle Deckungsgleichheit. Nach BSI-Sichtweise besteht der Betrachtungsgegenstand (Target of Evaluation, TOE) aus dem Smart Meter Gateway, einschließlich der Kommunikation auf den drei Netzwerken Legal Metrology Network (LMN) , Home Automation Network (HAN) und Wide Area Network (WAN), siehe Bild 1. An den Netzwerken angeschlossene Komponenten werden hier nicht betrachtet.

Nach den eichrechtlichen Vorgaben gibt es aber in diesem System auch Komponenten, die eichrechtlich zu betrachten sind. Um z. B. den Anschluss von Zählern, die nach der europäischen Richtlinie MID [7] zugelassen bzw. zertifiziert wurden, zu ermöglichen, wird i. d. R. ein Adapter benötigt, der die von den Zählern stammenden Messdaten in für das LMN geeignete Übertragungsprotokolle konvertiert. Die Anforderungen an diesen Kommunikationsadapter sind in den PTB-A 50.8 definiert worden.

Ferner muss ein Messsystem über eine Anzeige für die im SMGW erzeugten neuen Messwerte verfügen (§ 7 MessEV, Anhang 2, Nr. 9.1 [6]). Anforderungen an diese Anzeigekomponente sind ebenfalls in den PTB-A 50.8 zu finden.

Eine weitere für die Bildung der neuen Messwerte elementare Komponente ist der Zeitserver, der die Synchronisation der Zeitbasen der Smart Meter Gateways mit der gesetzlichen Zeit sicherstellt. Die in den PTB-A 50.8 definierten Anforderungen an diese Zeitserver gewährleisten, dass die in den SMGW gebildeten neuen Messwerte die geforderten Fehlergrenzen bezüglich der gesetzlichen Zeit einhalten können.

Prüfaufwand

Es wird deutlich, dass die Konformitätsbewertungen nach MessEG, abgesehen vom Prüfgegenstand (TOE), nach dem bisher vorliegenden Entwurf der Messsystemverordnung (MsysV) weitere Komponenten beinhalten müssen. Die Prüftiefe bei diesen zusätzlichen Komponenten entspricht derjenigen, die sonst im gesetzlichen Messwesen verlangt wird (Prüfung der technischen Unterlagen, keine Codeprüfung der Software), sodass der Zusatzaufwand vergleichsweise gering ist. Beim SMGW selbst, der komplexesten der betrachteten Komponenten, wird voraussichtlich ein großer Teil der bei einer Baumusterprüfung nach MessEG notwendigen Prüfungen bereits durch das Zertifikat der BSI-Prüfstelle abgedeckt, sodass hier nur noch ergänzende Prüfungen mit geringerer Prüftiefe erforderlich sind.

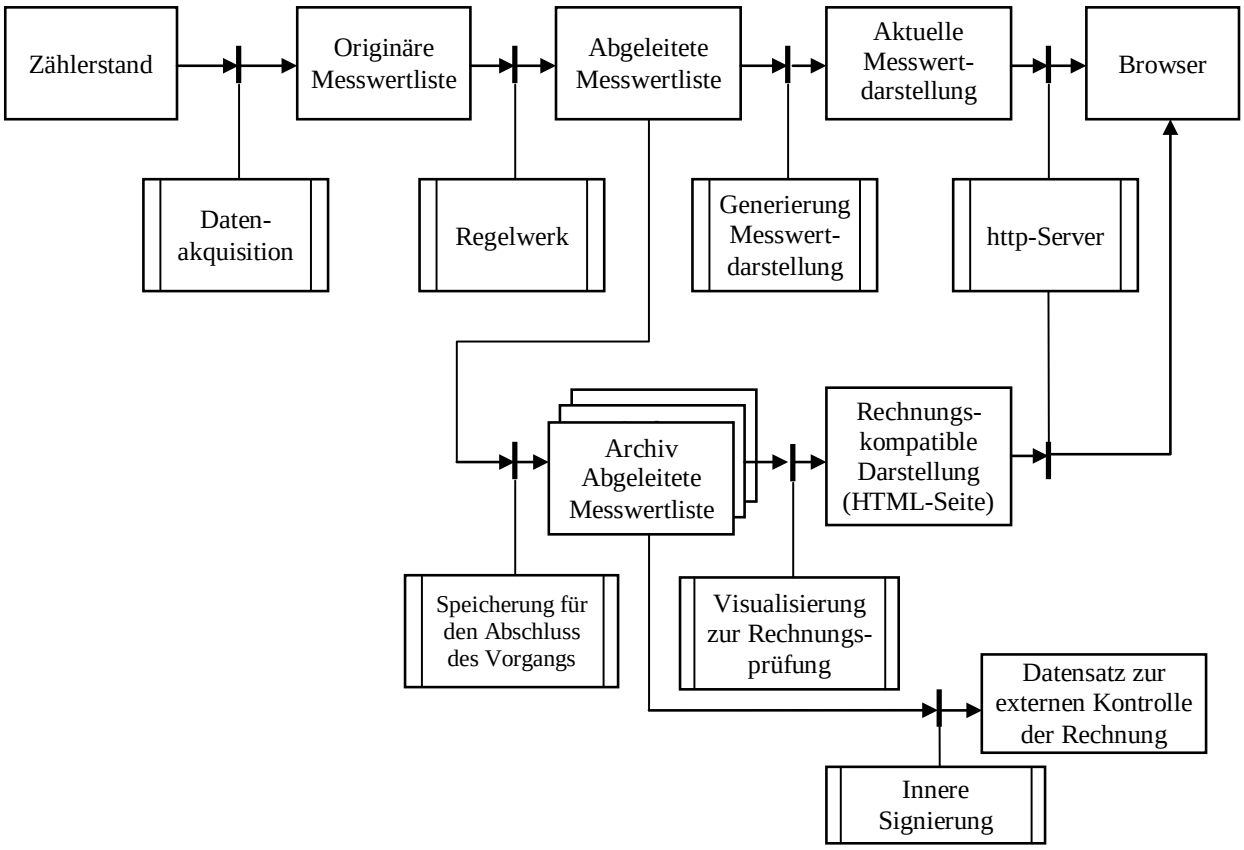

Bild 2:
Eichrechtlich relevante Software eines Systems mit SMGW

Anforderungen an das SMGW

Funktionelle Bestandteile der Software

In der TR wird das Konzept der Messwerterfassung und Messwertverarbeitung im SMGW beschrieben. Bild 2 zeigt eine Darstellung der rechtlich relevanten Datenflüsse und Funktionen, wie sie im gesetzlichen Messwesen häufig verwendet wird. Hier wird der Datenfluss in einem Messsystem ausgehend von den Signalen eines Sensors über die Messwertverarbeitung bis zur Anzeige verfolgt. Für die einzelnen Abschnitte dieser Kette gelten spezifische Anforderungen hinsichtlich Datenrepräsentation und Funktionalität. Diese Datenflussdarstellung umfasst die folgenden Blöcke:

- Datenakquisition von an LMN angeschlossenen Zählern und Kommunikationsadaptern. Erstmalige Speicherung in einem einheitlichen Darstellungsformat, den originären Messwertlisten.
- Verarbeitung der aktuellen originären Messwerte zu „neuen Messwerten“ nach den Vorgaben eines „Regelwerkes“ einschließlich erstmaliger Speicherung berechneter Messwerte.
- Erzeugung der Inhalte der eichrechtlich relevanten Anzeige.
- Übertragung der darzustellenden Inhalte an das Kundendisplay und Darstellung auf dieser Komponente.
- Speicherung aller abrechnungsrelevanten Informationen bis zum Abschluss des geschäftlichen Vorgangs. Schutz der gespeicherten Informationen gegen Manipulationen.
- Überprüfung der gespeicherten Informationen auf Manipulationen und Visualisierung zum Abschluss des Vorgangs.

Datenakquisition

Eine der wichtigsten eichrechtlich relevanten Funktionen des SMGW ist die Datenakquisition von allen am LMN direkt oder über Kommunikationsadapter angeschlossenen Zählern. Diese Funktionalität wird gemäß TR im SMGW durch *Zählerprofile* realisiert.

Da durch diese Profile die Bildung neuer Messwerte gesteuert wird und die Messrichtigkeit entscheidend davon abhängt, sind hier auch metrologische Anforderungen zu berücksichtigen. Bei den Anforderungen an die Datenakquisition wird unterschieden in Anforderungen an Software-Funktionen, die die Kommunikation im LMN realisieren, insbesondere die Einhaltung von Zeitbedingungen und die Erkennung von Fehlern und den Schutz der metrologisch relevanten Parameter.

Das SMGW empfängt die Messwerte aller zugeordneten Zähler über das LMN. Die Zähler werden entweder abgefragt (Polling) oder sie senden in festen Intervallen von sich aus im sogenannten Push-Betrieb. Das SMGW wandelt die empfangenen Datenformate in die einheitliche Datenstruktur „originäre Messwertliste“ um, welche die Basis für die anschließende Berechnung neuer Messwerte bildet. Beim Empfang der Messwerte werden diese noch mit einem Zeitstempel versehen, der ebenfalls mit abgespeichert wird. Ebenso werden erkannte Fehler kenntlich gemacht und ebenfalls registriert.

Zeitüberwachung der Datenakquisition

Das SMGW empfängt alle Telegramme eines Zählers und wertet sie laufend aus. Für die Abrechnung relevant sind die Telegramme, die im Zeitraster der Registrierperioden eintreffen, die übrigen gegebenenfalls empfangenen Telegramme werden nicht als originäre Messwerte verwendet. Das Zeitraster soll hierbei synchron zur gesetzlichen Zeit sein. Es ist aber ein Unsicherheitsbereich von ± 1 % der Registrierperiode zulässig, innerhalb dessen der Messwert empfangen werden muss – dies entspricht einem zulässigen Empfangsfenster, in das der Empfang mindestens eines Messwertes fallen muss. Der betreffende Zähler muss also in der Lage sein, die Messwerte ausreichend häufig zu ermitteln und zu senden oder anders ausgedrückt: Das Messintervall des angeschlossenen Zählers darf höchstens so lang sein wie das zulässige Empfangsfenster der Registrierperiode.

Im Allgemeinen ist das Messintervall gerade bei batteriegespeisten Zählern nicht beliebig verkürzbar. Daraus folgt, dass bei einem gegebenen Messintervall des Zählers auch die Mindestlänge der realisierbaren Registrierperiode vorgegeben ist und somit nicht in jedem Fall alle definierten Tarifanwendungsfälle (siehe unten) realisiert werden können. Ein Beispiel: Um die minimal mögliche Registrierperiode, für die ein Zähler verwendbar ist, zu ermitteln, muss zunächst das minimale Messintervall des Zählers bekannt sein, bspw. 20 min. Wie oben erläutert, hat das zulässige Empfangsfenster dann ebenfalls die Länge von 20 min. Fehlergrenzen werden immer symmetrisch zum Sollwert angegeben, sodass die 1-Prozent-Fehlergrenze der Registrierperiode hier ± 10 min beträgt, woraus sich wiederum hochgerechnet eine minimale Registrierperiodenlänge von 1000 min ≈ 16,7 h ergibt. Dieser Wert würde ausreichen, um bspw. eine tageweise Registrierung der elektrischen Energie oder des Gasvolumens zu realisieren. Für Registrierperioden von 15 min müsste der Zähler hingegen für Messintervalle ≤ 18 s ausgelegt sein.

Trifft aufgrund von Empfangsstörungen innerhalb des Empfangsfensters kein fehlerfreies Telegramm ein, darf ein zu spät oder zu früh eingetroffener Messwert nicht verwendet werden. Um die Verfügbarkeit zu erhöhen, können das zulässige Empfangsfenster und damit die minimale Registrierperiodenlänge soweit vergrößert werden, dass sie mindestens eine Länge von zwei oder mehr Messintervallen haben.

Auswerteprofile und Regelwerk, Tarifanwendungsfälle

Die von den Zählern empfangenen mit Zeitstempeln versehenen originären Messwerte können nun auf unterschiedliche Weise weiterverarbeitet werden. Die Software, die diese Weiterverarbeitung durchführt, wird als Regelwerk bezeichnet. Die Parameter des Regelwerkes sind in den Auswerteprofilen hinterlegt. Die vom Regelwerk erzeugten Ergebnisse werden in abgeleiteten Registern bzw. in abgeleiteten Wertelisten gespeichert, um dann für den Versand an die Marktteilnehmer vorgehalten zu werden. Im Allgemeinen entstehen hierbei im eichrechtlichen Sinne i. d. R. auch neue Messwerte, sodass die Auswerteprofile und die Regelwerke gegen unzulässige Veränderung geschützt werden müssen. Im laufenden Betrieb obliegt ihre Verwaltung dem *Gateway-Administrator* (GW-Admin).

Über die Auswerteprofile und die Regelwerke werden die sogenannten Tarifanwendungsfälle (TAF) abgebildet. Als Beispiele sind hier zu nennen: *Datensparsamer Tarif* (TAF1), *Zeitvariabler Tarif* (TAF2), *Abruf von Messwerten im Bedarfsfall* (TAF6) oder *Zentrale Tarifierung* (TAF7). Insgesamt sind in der TR 13 Tarifanwendungsfälle definiert worden. In einer Einführungsphase werden aber von einer Reihe von Herstellern zunächst nur die vier oben genannten in den Gateways der Generation 1 realisiert.

Erzeugung der Inhalte der Anzeige

Ein Messsystem muss eine Anzeige für die im SMGW generierten eichrechtlich relevanten Informationen besitzen. Die TR fordert nicht, dass ein SMGW mit einer Anzeige ausgestattet sein muss, es wird lediglich eine Schnittstelle definiert, über die eine Anzeige angesteuert werden kann und es wird ein Mindestumfang an bereitzustellenden Informationen gefordert [3]. Das bedeutet, dass die dem Letztverbraucher anzuzeigenden Inhalte im SMGW zwar erzeugt werden, die eigentliche Visualisierung aber auf einer anderen Messsystemkomponente, dem *Kundendisplay*, erfolgt. Aus eichrechtlicher Sicht ist auch ein in das SMGW integriertes Display möglich. Als mögliche technische Lösung ist in der TR im SMGW ein Webserver auf dem HAN vorgesehen, sodass Messwerte und sonstige Informationen auf einem am HAN angeschlossenen Rechner mit einem Webbrowser visualisiert werden können.

Die Anzeigefunktion des SMGW umfasst mehrere Teilaufgaben:

- Authentifizierung und Zugriffsautorisierung eines Letztverbrauchers,
- Benutzerführung,
- Anzeige aktueller Messwerte und sonstiger Daten,
- Anzeige von Messwerten und Daten, die zur Rechnungskontrolle erforderlich sind und
- Anzeige des Letztverbraucher-Logbuchs.

Für die Letztverbraucherauthentifizierung und -autorisierung müssen folgende Informationen vom SMGW über das HAN bereitgestellt werden:

- Anzeige der eingegebenen Benutzerkennung,
- Anzeige der gemäß [MsysV] § 3, Absatz 2 b notwendigen Tarifinformationen und
- Anzeige der SMGW-Kennung oder -Bezeichnung.

Jeder Letztverbraucher darf nur die Daten angezeigt bekommen, die ihn selbst betreffen. Diese Abgrenzung ist zur Umsetzung des Datenschutzes als Schutzmaßnahme in der TR gefordert. Nach dem Verbindungsaufbau muss die freie Auswahl aller, für den Letztverbraucher relevanten und freigegebenen Daten möglich sein. Hierzu muss die eichpflichtige Software im SMGW Steuerungsbefehle zur Bedienung der Anzeige und Navigation vom Kundendisplay empfangen und entsprechend reagieren.

Die Anzeige aktueller Werte muss zu jedem Zeitpunkt erfolgen können, sobald der Letztverbraucher es wünscht. Ein Merkmal der Anzeige aktueller Werte ist, dass nicht alle eichrechtlich relevanten Informationen direkt oder in jedem Fall Eingang in die Rechnung finden, dem Letztverbraucher aber dennoch zur Verfügung gestellt werden müssen (z. B. die momentane mittlere Leistung).

Die Informationen zur Rechnungsüberprüfung enthalten dagegen neben den eigentlichen historischen Messwerten weitere Daten (Stammdaten, Tarifdaten), die die Zuordnung und Kontrolle der Rechnung erst ermöglichen. Die Anzeigen zur Rechnungskontrolle beziehen sich immer auf einen zurückliegenden Zeitraum.

Zur Rechnungskontrolle muss auch eine Einsichtnahme in das Letztverbraucher-Logbuch möglich sein. Dieses enthält Messwerte (z. B. Messwertlisten), Stammdaten (z. B. Kennung des Rechnungsstellers), Tarifinformationen (z. B. Änderung von Parametern von Auswertungsprofilen) sowie eine Liste von Fehlerereignissen. Da es jederzeit für den Letztverbraucher zugänglich ist, dient es der aktuellen Information über abrechnungsrelevante Details.

Eine Besonderheit stellt der TAF 7 (zentrale Tarifierung) dar. Auch bei diesem Verfahren muss dem Letztverbraucher die Kontrolle der Rechnung über die im SMGW verarbeiteten und abgelegten Daten ermöglicht werden.

Rück- und Nebenwirkungsfreiheit der Kommunikation über Schnittstellen

Kein über die Schnittstelle empfangener Befehl oder Datenfluss darf eine unzulässige Wirkung im SMGW haben. Dies ist der übereinstimmende Grundsatz, auf dem PP und TR einerseits und die eichrechtlichen Anforderungen andererseits basieren. Die Umsetzung in einzelne Detailanforderungen führt bei PP und TR zur Definition von Rollen, denen bestimmte Aufgaben und Verantwortlichkeiten zugeschrieben werden. Die PTB-Anforderungen sind bei der Konkretisierung eher auf die technische Beschränkung von unzulässigen Funktionen und Wirkungen im Gerät ausgerichtet, unabhängig davon, welcher Rollenvertreter eine Aktion auslöst. Vor diesem Hintergrund sind in den PTB-Anforderungen im Detail einige Ergänzungen und Konkretisierungen zu dem Dokumentensystem PP/TR hinzugefügt worden.

Bei den in PP/TR definierten Bezeichnungen für Schnittstellen handelt es sich nicht um Hardware-Schnittstellen des SMGW, sondern um ein- und austretende Kommunikationsverbindungen zu dem in der Bezeichnung erscheinenden Kommunikationspartner (Rolle oder Gerät). Für diese logischen Schnittstellen sind in den PTB-A 50.8 Beschränkungen für Zugriffe auf konkrete Daten und Funktionen festgelegt worden, sofern sie eine eichrechtliche Bedeutung haben. Daher muss es einen Programmteil im eichrechtlich relevanten Teil der Software geben, der die empfangenen Befehle interpretiert. Der Interpreter darf nur gültige Befehle akzeptieren; bei Empfang anderer Befehle müssen diese als solche identifiziert und verworfen werden.

Schnittstelle zum Kundendisplay

Über diese logische Schnittstelle erhält der Letztverbraucher Zugriff auf die ihn betreffenden Informationen im SMGW. Diese Kommunikation erfolgt über die Messsystemkomponente *Kundendisplay*. So wird dem Letztverbraucher die oben erwähnte Benutzerautorisierung, die Navigation und die Anzeige von Messwerten und sonstigen Daten ermöglicht.

Die Software des SMGW muss verhindern, dass es bei beliebigen Eingaben über diese Schnittstelle möglich ist, eichrechtlich relevante Parameter oder gespeicherte Messwerte zu verändern oder andere Funktionen auszulösen als die genannten.

Schnittstelle zum GW-Admin (WAN)

Diese Schnittstelle beschreibt die Kommunikation der Software auf einem Rechner des GW-Administrators mit dem SMGW. Folgende Kommunikation der Rolle GW-Admin über diese Schnittstelle ist zulässig:

- Erkennung und Autorisierung eines Teilnehmers mit der Rolle „GW-Admin“,
- Abruf des Eich-Logs, das alle eichrechtlich relevanten Ereignisse unlöschbar dokumentiert, und Abruf des System-Logs,
- Konfiguration bezüglich der Messwerterfassung, Messwertverarbeitung und Versand von Messwerten und anderen Informationen an externe Marktteilnehmer,
- Konfiguration der Festlegungen für die externen Marktteilnehmer, die mit dem SMGW kommunizieren dürfen und die Informationen über die externe Schnittstellen erhalten dürfen,
- Konfiguration des Sicherheitsmoduls,
- Konfiguration des Zertifikatsmaterials im SMGW und
- Parametrierungen für die einzelnen Tarifanwendungsfälle. Jede Änderung der eichrechtlich relevanten Parameter erfordert eine Eintragung im Eich-Log bzw. im Letztverbraucher-Log.

Im SMGW müssen technische Vorkehrungen getroffen sein, die die im Folgenden aufgeführten Aktionen verhindern oder beschränken:

- Gemäß der TR ist der GW-Admin berechtigt, Software-Updates nach Überprüfung der Authentizität der Software einzuspielen. Aus eichrechtlicher Sicht ist dies aber nur gewissermaßen eine Vorprüfung, denn die eigentliche Überprüfung der Authentizität und Integrität muss automatisch im SMGW gemäß den Download-Anforderungen des MessEG erfolgen, der GW-Admin darf den Vorgang nur initiieren können. Diese Anforderung betrifft insbesondere das Regelwerk. Sofern zu ladende Zählerprofile ausführbaren Code enthalten, sind die Anforderungen auch auf diese anzuwenden. Für die zu ladende Software muss eine Konformitätsbewertung durch eine benannte Stelle für das gesetzliche Messwesen durchgeführt werden.
- Der GW-Admin darf nur die im Rahmen der eichrechtlichen Baumusterprüfung festgelegten Parameter und Funktionen des SMGW beeinflussen können. Die Einstellungen durch den GW-Admin erfolgen durch Parametrierung der Zählerprofile und des Regelwerks. Die damit initiierten oder gesteuerten Funktionen müssen automatisch ohne weitere Aktionen des GW-Admin ablaufen. Der direkte Zugriff auf eichrechtlich relevante Daten oder

Funktionen darf für den GW-Admin nicht möglich sein. Der GW-Admin darf das Eich-Log und die Letztverbraucher-Logs nicht direkt löschen oder verändern können.
- Der GW-Admin darf Eich-/Letztverbraucher-Log-Einträge bei Änderung eichrechtlich relevanter Parameter nicht umgehen oder verhindern können.
- Besitzt das SMGW ein Betriebssystem, so darf der GW-Admin nicht die Rolle des Betriebssystemadministrators einnehmen können und darf nicht mit besonderen Privilegien ausgestattet sein.

Schnittstelle zu den Einrichtungen des externen Marktteilnehmers

Externen Marktteilnehmern wird Zugriff auf für sie relevante Daten durch den GW-Admin gewährt. So muss die Software des SMGW dafür sorgen, dass der externe Marktteilnehmer ausschließlich Informationen vom SMGW, die durch Auswerteprofile vom SMGW-Admin festgelegt worden sind, erhält. Er darf keinen direkten Zugriff auf Zähler im LMN und keinen direkten Zugriff auf originäre Messwertlisten erhalten, sondern nur auf die abgeleiteten Messwertlisten und gegebenenfalls auf die Datenstruktur mit dem aktuellen Zählerstand.

Schnittstelle zur Verwenderüberwachung

Der GW-Admin unterliegt der Verwendungsüberwachung durch die Behörden. Dennoch haben diese keinen direkten Zugang zu den Daten des SMGW. Der GW-Admin ist aber verpflichtet, der Überwachungsbehörde jederzeit den Inhalt der Eich-Logs beliebiger SMGW auf Anforderung zur Verfügung zu stellen.

Das SMGW muss es dem GW-Admin ermöglichen, das Eich-Log auszulesen und an eine Überwachungsbehörde weiterzuleiten. Das SMGW muss das Eich-Log vor Versand an den GW-Admin mit seinem privaten Schlüssel signieren. So können die Überwachungsbehörden überprüfen, ob das Eich-Log authentisch und integer ist.

Schnittstelle zum LMN

Für die Schnittstelle zum LMN, über die die Kommunikation mit den Zählern und Kommunikationsadaptern erfolgt, bedeutet Rück- und Nebenwirkungsfreiheit, dass das SMGW nur mit den bekannt gemachten Zählern und Kommunikationsadaptern kommuniziert. Dies wird in den Zählerprofilen festgelegt, welche gewährleisten müssen, dass über die Schnittstelle nur der Messwertempfang erfolgt und die Daten, Parameter und Funktionen des SMGW nicht in unzulässiger Weise über diese Schnittstelle beeinflusst werden können. Es dürfen nur zertifizierte und autorisierte Zählerprofile installiert werden können. Es darf nicht möglich sein, dass Zähler oder Kommunikationsadapter hinzugefügt, ausgetauscht oder gewechselt werden können, ohne dass dies im Eich-Log registriert wird.

Abbildung der Rollen, Mandanten-Accounts, Zugriffsrechte

Durch PP und TR werden zum Teil detaillierte Vorgaben an die Software des SMGW unter Datensicherheitsaspekten aufgestellt. Diesen liegt ein System von Rollen und ihren Berechtigungen zugrunde. Aus diesen Vorgaben ergibt sich eine grobe Softwarearchitektur, die im SMGW realisiert werden muss. Wie oben erläutert, ist es aus eichrechtlicher Sicht zum Teil erforderlich, gewisse Anforderungen zu ergänzen bzw. in der TR aufgestellte Forderungen genauer zu spezifizieren.

Im Gesetzlichen Messwesen sind Multiuser-Systeme wie das SMGW nicht üblich. Deshalb wird das Problem der Abschottung der einzelnen Nutzer des Systems gegeneinander nicht ausdrücklich in der MID [7] bzw. MessEG/EV behandelt. Es wird jedoch verlangt, dass die messtechnisch relevante Software nicht von anderer Software in unzulässiger Weise beeinflusst werden darf. Existieren mehrere virtuelle messtechnisch relevante Einrichtungen nebeneinander, wird die MessEV hier so interpretiert, dass sich diese nicht gegenseitig beeinflussen dürfen.

Die in PP bzw. TR definierten Rollen beinhalten Berechtigungen und Zugriffsverbote für die jeweiligen Rollenvertreter. Nach Eichrecht müssen diese Beschränkungen auch technisch so umgesetzt sein, dass der betreffende Vertreter der Rolle gar nicht in der Lage ist, gegen diese Vorgaben zu verstoßen. Es handelt sich nicht nur um Schutzmaßnahmen, sondern auch um funktionelle Anforderungen an das System. Entsprechend einer objektorientierten Beschreibung, die keine Vorgabe für eine reale Realisierung sein soll, wird hier von Instanzen (Objekten) gesprochen, die einem Rollenvertreter zugeordnet sind und gewisse Funktionen, Datenrepräsentationen und Parameter besitzen.

Die Softwareteile, die die eichrechtlich relevante Berechnung, Verarbeitung, Speicherung usw. eines Tarifanwendungsfalls realisieren, dürfen nicht durch die eines anderen Tarifanwendungsfalls gestört oder unzulässig beeinflusst werden können. Die Softwareteile, die einem Letztverbraucher zugeordnete Funktionen und Datenrepräsentationen realisieren, dürfen nicht durch die einem anderen zugeordnete Funktionen und Datenrepräsentationen gestört oder unzulässig beeinflusst werden können.

Diese Anforderungen können als Instanz im objektorientierten Sinne realisiert werden. Diese Instanz ist der Teil der Software, mit der ein realer Letztverbraucher kommuniziert, die Informationen über ihn bereithält und diese an andere reale Rollenvertreter oder andere Software-Objekte weitergibt, und die schließlich alle Informationen, die den Letztverbraucher betreffen, zusammenhält und gegen unzulässige Zugriffe schützt. Es ist vorteilhaft, die Software wie beschrieben zu organisieren, weil auf diese Weise automatisch eine Kapselung gegen andere Software erfolgt.

Neben den beschriebenen Modellinstanzen für den Letztverbraucher müssen nach den gleichen Grundsätzen aufgebaute weitere Modellinstanzen für die Überwachungsbehörde, den Gateway-Administrator, den Servicetechniker sowie den externen Marktteilnehmer im SMGW existieren.

Verwaltung, eichrechtlich relevante Prozeduren und Prozesse

Die Modellinstanzen für die verschiedenen Rollen dürfen nur die ihnen erlaubten Operationen in der Systemsoftware ausführen können. Die Modellinstanzen existieren während der gesamten Betriebszeit bzw. solange die Berechtigung des betreffenden Rollenvertreters für das SMGW gilt. Es wird also ein für diesen Zeitraum aktiver Account benötigt, dem die Rollenberechtigungen zugeordnet sind, unabhängig davon, ob der Rollenvertreter gerade mit dem SMGW kommuniziert oder nicht (innerer Account).

Es muss für jeden am SMGW registrierten Rollenvertreter einen inneren Account geben, der ununterbrochen aktiv ist. Dies hat zum Ziel, dass auch Software-Objekte, deren Funktionen stellvertretend für den realen Rollenvertreter Operationen und Datenzugriffe ausführen, denjenigen Beschränkungen unterliegen, die für die jeweilige Rolle gelten.

Neben den rollengebundenen Operationen und der Messwertverarbeitung müssen weitere eichrechtlich relevante Aufgaben und Dienste ausgeführt werden. Hierzu sollte es einen Teil der Firmware bzw. Systemsoftware geben, der alle eichrechtlich relevanten nicht rollengebundenen Operationen ausführt. Beispiele für derartige Operationen wären:

- Datenakquisition,
- Führen des Eich-Logs,
- Funktion, die Änderungen der eichrechtlich relevanten Parameter vornimmt. Hierzu zählen z. B. ein Zählerwechsel, das Laden eines neuen Zählerprofils, das Laden eines neuen Auswerteprofils usw.,
- Funktionen, die die Zugriffsbeschränkungen für Zugriffe durch Accounts realisieren,
- Ausführung von Selbsttest-Prozeduren in regelmäßigen Abständen oder auf Veranlassung des GW-Admin und
- Durchführung und Steuerung von Software-Updates gemäß den Download-Anforderungen.

Die Softwareteile, die die inneren Accounts und den nicht rollengebundenen Diensten zugeordneten Funktionen und Datenrepräsentationen realisieren, dürfen selbst nicht durch andere Softwareteile gestört oder unzulässig beeinflusst werden können.

Funktionen, die in diesem Abschnitt diskutiert wurden, wie Datenakquisition, Zeitstempelung, Regelwerk und Auswerteprofile, Generierung der Anzeige, Verwaltung der Logs, Steuerung von Updates, Selbsttests usw. gehören zum eichrechtlich relevanten Softwareteil. Es können noch weitere hinzukommen, abhängig von der tatsächlichen Realisierung.

Es ist möglich, dass neben dem eichrechtlich relevanten Softwareteil ein weiterer, eichrechtlich nicht relevanter existiert. Beide Teile müssen voneinander getrennt sein und zwischen beiden Teilen muss eine informationstechnische Schnittstelle definiert werden. Der oben beschriebene objektorientierte Ansatz ist eine gute Voraussetzung, um diese Softwaretrennung realisieren zu können.

Zusammenfassung und Ausblick

Das Sicherheitskonzept des SMGW wurde vom Bundesamt für Sicherheit in der Informationstechnik entwickelt und die Sicherheitsanforderungen und notwendigen Funktionalitäten in Form eines Schutzprofils und einer Technischen Richtlinie veröffentlicht. Mit den PTB-A 50.8 wurde dieses Regelwerk um die eichrechtlichen Aspekte ergänzt. Hersteller können nun auf dieser Basis konkrete Geräte konstruieren und Baumusterprüfbescheinigungen bei den benannten Stellen erhalten. Eine Erprobung in größerem Umfang soll in Kürze beginnen.

Endgültige Sicherheit über die Anforderungen an das SMGW werden Hersteller, Verwender, Prüfstellen und Überwachungsbehörden aber erst mit der Verabschiedung der Messsystemverordnung bekommen. Eine überarbeitete Version der Technischen Richtlinie wurde bereits angekündigt. In diesem Zusammenhang werden auch noch einige Verfahrensfragen abschließend zu klären sein, wie das Inverkehrbringen der Geräte im eichrechtlichen Sinn, mögliche Softwareupdates im Betrieb oder Befundprüfungen durch Überwachungsbehörden. Zur Behandlung dieser Fragen wurde eine BSI-Arbeitsgruppe unter der Leitung der Eichbehörden eingerichtet, in der die PTB beratend beteiligt ist.

Literatur

[1] Energiewirtschaftsgesetz (EnWG), www.gesetze-im-internet.de/bundesrecht/enwg_2005/gesamt.pdf (letzter Aufruf: 24. September 2015)

[2] Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff und Energiemengen, SMGW-PP, Version 1.2, 18. März 2013, Certification-ID BSI-CC-PP-0073, Bundesamt für Sicherheit in der Informationstechnik, Bonn

[3] Technische Richtlinie BSI TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.0, 18. März 2013, BSI, Bonn

[4] PTB-Anforderungen PTB-A 50.8 Smart Meter Gateway, Dezember 2014, verabschiedet von der Vollversammlung für das Eichwesen 2014

[5] Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (Mess- und Eichgesetz – MessEG), 25. Juli 2013

[6] Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung (Mess- und Eichverordnung – MessEV), 11. Dezember 2014

[7] Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über Messgeräte