Integration von TNC in ein deutsches Smart Meter Gateway

Carl-Heinz Genzel · Olav Hoffmann · Richard Sethmann

Hochschule Bremen
{carl-heinz.genzel | olav.hoffmann | sethmann}@hs-bremen.de

Zusammenfassung

Durch die gesetzliche Einführung intelligenter Messsysteme sollen das Messwesen für das Energienetz und der Umgang mit Energie in Deutschland verbessert werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat, nach dem Prinzip „Secure by Design“, hierfür Sicherheitsrichtlinien in Bezug auf eine zentrale Kommunikationseinheit, das sogenannte Smart Meter Gateway (SMGW), entwickelt. In dem Forschungsprojekt SPIDER wurden diese Richtlinien untersucht. Hierbei wurde Trusted Network Connect (TNC) als zusätzlicher Sicherheitsbaustein in einem erweiterten Sicherheitskonzept erkannt, der die Sicherheit eines SMGW und damit eines intelligenten Messsystems erhöhen kann. Diese Veröffentlichung baut auf bereits bestehenden Veröffentlichungen zu dem genannten Sicherheitskonzept aus dem Forschungsprojekt SPIDER auf und stellt eine erfolgreiche Integration von TNC in ein SMGW auf der Basis des Sicherheitskonzepts vor.

1 Einleitung

Die steigende Einbindung schwankender und dezentraler Energieerzeuger bei gleichzeitiger Wahrung der Netzstabilität erfordert die Etablierung intelligenter, steuerbarer Energienetze. Dabei ist es von besonderer Bedeutung die unterschiedlichen Interessen der einzelnen Marktteilnehmer in einem Energienetz zu berücksichtigen. Hierzu gehören der Messstellenbetreiber, der verantwortlich für die Messsysteme ist, der Messdienstleister, der das Auslesen von Verbrauchszähleinrichtungen übernimmt, der Verteilnetzbetreiber, der das örtliche Stromnetz unterhält und wartet sowie der Lieferant, der als Handelswarenvertreter auftritt und für die Nutzung des Netzes Gebühren an den Verteilnetzbetreiber zahlt. Die deutsche Regierung hat hierzu die Einführung intelligenter Messsysteme, sogenannter Smart Metering Systeme, beschlossen. Dies sind Messsysteme, die zur Kommunikation an ein Datennetz angeschlossen sind und verschiedene Aufgaben, wie die Berechnung des Energieverbrauchs und die Bereitstellung moderner Tarife zur flexiblen Bilanzierung des berechneten Energieverbrauchs, übernehmen [Bund13]. Außerdem müssen Smart Metering Systeme besonders hohen Sicherheitsanforderungen genügen, da das Energienetz zum einen zu den kritischen Infrastrukturen in Deutschland zählt und es sich zum anderen bei den Messdaten zum Teil um personenbezogene Daten handelt. Für den Bereich IT-Sicherheit hat das BSI aus diesem Grund Sicherheitsrichtlinien (vgl. [Bund15]) entwickelt, die eine Sicherheitsarchitektur für intelligente Messsysteme beschreiben. Die Architektur sieht neben intelligenten Zählern (Smart Metern) zur Erfassung von Energiemengen eine lokale Kommunikationseinheit, das SMGW, zum Schutz der Zähler und deren

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 297-308.

Messdaten vor [Bund13]. Im Rahmen des BMWi-Forschungsprojekts[1] „**S**ichere **P**owerl**i**ne-**D**atenkommunikation im intelligenten **E**ne**r**gienetz“ (SPIDER[2]) wurden diese Richtlinien analysiert und es wurde festgestellt, dass der Schutz der Integrität eines SMGW durch Konzepte aus dem Bereich Trusted Computing weiter erhöht werden kann. Hierbei geht es insbesondere um den Schutz des SMGW vor Manipulationsversuchen an dessen Hard- und Software (Tampering), da ein SMGW in weitestgehend ungeschützten Umgebungen betrieben wird (z.B. Flur oder Keller eines Wohngebäudes). Die Manipulation der Stromverbrauchserfassung durch technikaffine Letztverbraucher ist ein einfaches Beispiel hierfür, das in der Vergangenheit bereits bei herkömmlichen Metering Systemen durchgeführt wurde. Davon ausgehend wurde ein mehrstufiges Sicherheitskonzept in Anlehnung an [KRC+10], basierend auf den Vorgaben des BSI zu intelligenten Messsystemen, entwickelt [DGHS14].

Neben lokalen Schutzmaßnahmen schlägt das Konzept die Überwachung der Integrität eines SMGW aus der Ferne mit Hilfe von TNC der Trusted Computing Group (TCG) vor [DGHS14]. Diese Veröffentlichung greift das Konzept aus dem Forschungsprojekt auf und beschreibt einen Ansatz zur sinnvollen Integration der Integritätsüberwachung in den Programmablauf eines SMGW. Hierbei werden auch Probleme und ein Lösungsansatz in Bezug auf die Kommunikation angesprochen, die durch Widersprüche zwischen den Richtlinien des BSI und den Spezifikationen der TCG aufgetreten sind.

2 Smart Metering System

Ein intelligentes Messsystem besteht gem. BSI aus mehreren Komponenten, wobei zwei elementar sind, der intelligente Zähler (Smart Meter) und die Kommunikationseinheit (SMGW). Ein Smart Meter ist ein digitales Messsystem für Energiemengen, das mit dem SMGW verbunden ist, um zu kommunizieren. Das SMGW ist die zentrale Kommunikationseinheit für das gesamte Smart Metering System und wird neben den intelligenten Zählern von weiteren Komponenten und Rollen des Systems zur Kommunikation verwendet. Die wichtigsten Komponenten und Rollen aus den Vorgaben des BSI sind in Abbildung 1 dargestellt (vgl. [Bund13, Bund14, Bund13a, Bund13b]).

Das BSI unterscheidet in einem intelligenten Messsystem zwischen zwei generellen Bereichen. Es gibt einen öffentlichen, nicht näher eingegrenzten Bereich und einen Letztverbraucherbereich, der als geschlossene Einheit gesehen werden kann und zum Eigentum einer natürlichen oder juristischen Person zählt. In diesem Bereich befinden sich ein oder mehrere Smart Meter und ein SMGW. Das SMGW besitzt an dieser Stelle zwei Aufgaben. Zum einen ist es für die Verarbeitung und die sichere Speicherung von Messdaten zuständig, zum anderen ermöglicht es eine sichere Kommunikation zwischen den einzelnen Komponenten und Rollen des Systems. Hierfür besitzt es eine Firewall zur Steuerung der Verbindungen zwischen den einzelnen Komponenten und Rollen und unterstützt verschiedene kryptografische Methoden für eine sichere Datenübertragung. Außerdem besitzt es Funktionen zum Selbstschutz [Bund13a]. Zur Abgrenzung ihrer Privilegien hat das BSI die verschiedenen Komponenten und Rollen in unterschiedliche Kommunikationsnetze eingeordnet. Jede Komponente oder Rolle kann nur über das entsprechende Netz mit dem SMGW kommunizieren. Die folgenden Netze wurden hierzu definiert (siehe [Bund13]).

[1] Die Autoren danken dem BMWi-ZIM für die Förderung und allen SPIDER-Projektpartnern für die gute Zusammenarbeit.

[2] Das Forschungsprojekt SPIDER: http://www.spider-smartmetergateway.de

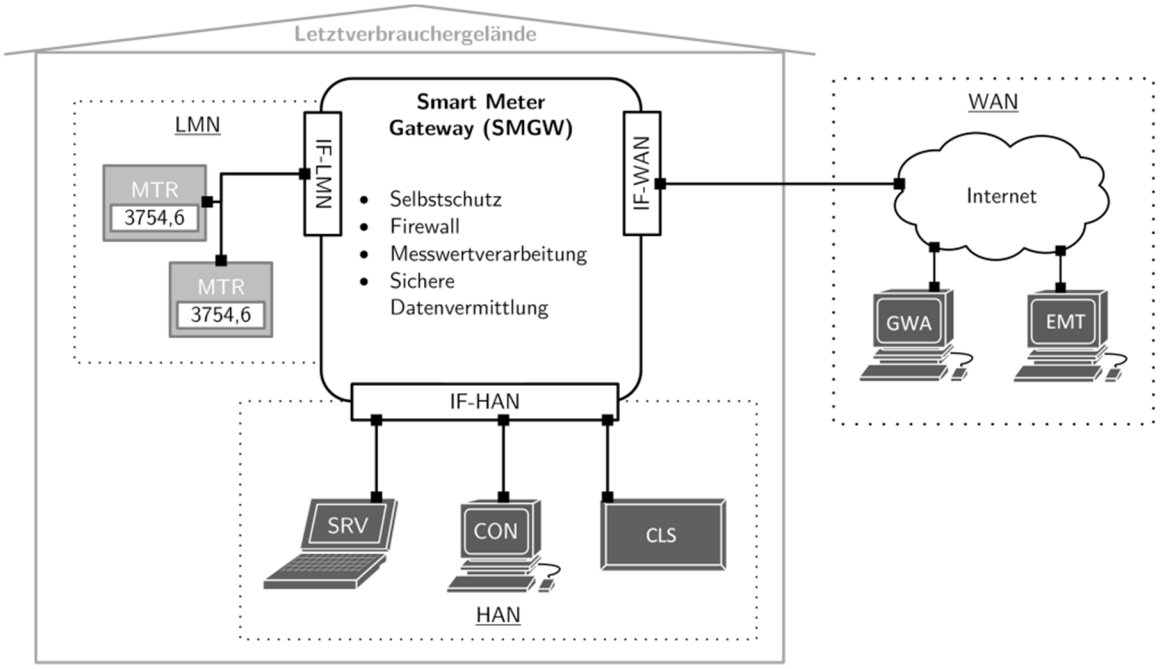

Abb. 1: Vereinfachte Architektur eines intelligenten Messsystems

Local Metrological Network (LMN): Das LMN dient zur Anbindung von lokalen intelligenten Zählern (Strom-, Gas- oder Wasserzähler) der Endnutzer (Letztverbraucher, LV). Die Messgeräte produzieren Messdaten und übergeben sie an das SMGW.

Home Area Network (HAN): Das HAN dient zur lokalen Anbindung und Steuerung von Energieerzeugern und Energieverbrauchern (Controllable Local Systems, CLS) der Letztverbraucher (z.B. Fotovoltaikanlagen). CLS nutzen das SMGW als Proxy, um mit Rollen aus dem externen Bereich zu kommunizieren (z.B. Wartungsdienstleister). Letztverbraucher können über dieses Netz Informationen zu den Messwerten aus dem LMN abrufen. Sie sind die Eigentümer der Messdaten aus dem LMN. Außerdem kann technisches Betreiberpersonal (Service-Techniker, SRV) Diagnosedaten über das HAN abrufen.

Wide Area Network (WAN): Über das WAN kann das SMGW Messdaten an autorisierte externe Marktteilnehmer (EMT) senden. EMT bieten Dienstleistungen auf der Basis dieser Daten an (z.B. Bilanzierung des Energieverbrauchs durch den Energielieferanten). Außerdem kann das SMGW über dieses Netz mit dem Gateway Administrator (GWA) kommunizieren. Der GWA ist die zentrale vertrauenswürdige Instanz des Smart Metering Systems. Er ist für die Steuerung und Überwachung des SMGW zuständig und benötigt hierzu das Vertrauen der einzelnen Rollen sowie der Systeme eines Smart Metering Systems. Der GWA wird hierzu mit Hilfe einer obligatorischen Zertifizierung nach DIN ISO/IEC 27001[3] regelmäßig geprüft und besitzt einen Zugang zu staatlich kontrollierten, zentralen Diensten, wie Zeitservice und Public Key Infrastruktur. Die einzige Ausnahme zu den weitreichenden Rechten eines GWA stellen die personenbezogenen Daten der Letztverbraucher dar. Diese Daten unterliegen dem Datenschutz und dürfen von dem GWA nicht eingesehen werden.

[3] DIN ISO/IEC 27001:2015-03 Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen

3 Konzept zum Schutz der Integrität eines SMGW

Im Forschungsprojekt SPIDER wurde ein Konzept zum Schutz der Integrität eines SMGW entwickelt, das auf den Richtlinien des BSI basiert. Es sieht verschiedene ergänzende Maßnahmen zum Schutz und zur Überwachung der Integrität auf drei Stufen vor. Da das SMGW die zentrale Kommunikationseinheit des Smart Metering Systems ist, wird aus Sicht des Forschungsprojekts die Sicherheit eines intelligenten Messsystems im Gesamten durch das entwickelte Konzept verbessert [DGHS14].

3.1 Schutz der Hardware

Die erste Stufe des Konzepts ist der Schutz der Hardwareintegrität. Die Hardware wird hierzu fest in ein geschlossenes Gehäuse integriert. Eine Plombe an dem Gehäuse und ein elektronischer Schalter im Gehäuse ermöglichen eine optische sowie elektronische Erkennung, falls das Gehäuse unerlaubt geöffnet wird. Zusätzlich dazu werden wichtige Hardwarebausteine mit einem sogenannten Tamper Resistant Grid geschützt, um eine Manipulation an den Bausteinen zu erkennen [DGHS14].

3.2 Schutz zur Startzeit

Die zweite Stufe des Konzepts stellt sicher, dass das SMGW nur gestartet werden kann, wenn es sich in einem vorgegebenen Zustand befindet. Hierzu wird das in Abbildung 2 dargestellte Secure Boot-Muster eingesetzt. Das Muster definiert den Startprozess eines SMGW als Sequenz sogenannter Bootstrap-Module, die in einer festen Abfolge während des Systemstarts geladen werden. Beispielsweise wird bei dem Start eines klassischen IT-Systems meist zuerst ein Bootloader geladen, der anschließend das Betriebssystem lädt, welches wiederum einzelne Anwendungen startet. Jedes Modul muss bei einem Secure Boot das folgende Modul zuvor kryptografisch auf seine Integrität prüfen. Sollte diese Prüfung negativ ausfallen, wird der Start des SMGW abgebrochen [DGHS14].

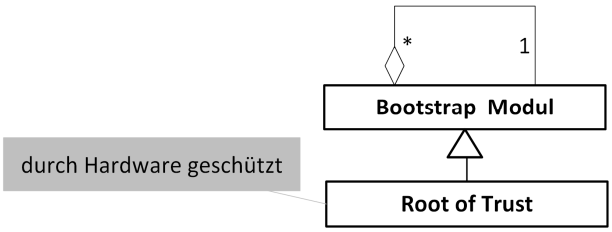

Abb. 2: Secure Boot-Muster [LöSW10]

Als weitere Schutzmaßnahme muss für ein Secure Boot zu Beginn einer solchen Startfolge, noch vor dem Bootloader, ein Modul geladen werden, das durch Hardware geschützt ist. Dieses Modul ist der Vertrauensanker („Root of Trust“). Es ist das einzige Modul, das nicht kryptografisch validiert wird, weil es als Hardware-basierte Sicherheitstechnologie besonders stark vor Manipulation geschützt ist [DGHS14].

3.3 Schutz zur Laufzeit

Die dritte Stufe dient zur Überwachung der Integrität eines SMGW, während es im Betrieb ist. Hierzu wird TNC eingesetzt. TNC ist von der TCG als eine offene, generische Architektur

definiert, die aus verschiedenen Rollen und Komponenten besteht, um die Integrität eines Systems innerhalb eines Netzes aus der Ferne (Remote Attestation) prüfen zu können. Zur Prüfung der Integrität eines Systems mit Hilfe der Remote Attestation führt das zu prüfende System Messungen durch, und sendet die erfassten Messwerte anschließend zu einer vertrauenswürdigen Instanz. Die vertrauenswürdige Instanz prüft daraufhin diese Messwerte mit Hilfe von Referenzwerten, die den gewünschten Zustand des gemessenen Systems beschreiben. Das Ergebnis der Prüfung wird durch diese Instanz zurück an das geprüfte System gesendet [Trus12]. In einem Smart Metering System soll das Ergebnis dieser Prüfung, dem Konzept entsprechend, als fortlaufende Überwachung der Integrität eines SMGW beim GWA eingesetzt werden. Das Konzept definiert TNC hierfür als ergänzende Sicherheitsmaßnahme. Dazu sollen die Komponenten und Rollen, wie in Abbildung 3 dargestellt, eingesetzt werden [DGHS14].

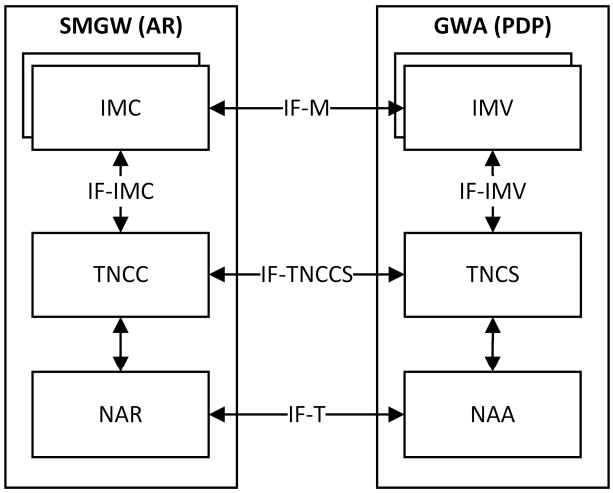

Abb. 3: Eingesetzte Komponenten und Rollen von TNC

Das SMGW muss regelmäßig geprüft werden. Aus diesem Grund wird es als sogenannter Access Requestor (AR) definiert. Der GWA ist die zentrale vertrauenswürdige Instanz in einem Smart Metering System und führt daher die Prüfung des SMGW zur Überwachung der Integrität durch. Er wird als sogenannter Policy Decision Point (PDP) definiert. Für die Durchführung der Remote Attestation besitzen beide Rollen interne Komponenten, die ihren Funktionen entsprechend in unterschiedlichen Ebenen angeordnet sind. Die Komponenten in der obersten Ebene sind für die Erfassung und Prüfung der einzelnen Messwerte eines Systems zuständig (z.B. Firmware oder Konfigurationsdaten). Ein oder mehrere Integrity Measurement Collector-Komponenten (IMC) erfassen Messwerte über die Integrität eines SMGW. Dem gegenüber stehen ein oder mehrere Integrity Measurement Verifier-Komponenten (IMV), die in der Lage sind die Messwerte zu prüfen. Die Komponenten kommunizieren mit Hilfe von Nachrichten, die durch die Schnittstelle IF-M definiert sind. Die Nachrichten werden zur Übertragung mit Hilfe der Schnittstellen IF-IMC und IF-IMV an die Komponenten TNC Client (TNCC) und TNC Server (TNCS) in der nächsten Ebene weitergeleitet. Diese Ebene ist für die Steuerung der Integritätsprüfung verantwortlich. Hierzu kommunizieren der TNCC und der TNCS, ebenfalls mit Hilfe von Nachrichten, über die definierte Schnittstelle IF-TNCCS. Die Nachrichten dieser Ebene werden zur Übertragung an die nächste Ebene weitergeleitet. Hierzu gibt es jedoch keine explizite Schnittstellendefinition. Diese Ebene ist für die physische Übertragung und den Schutz der Nachrichten aus den höheren Ebenen, während der Übertragung zwischen den beiden Rollen AR und PDP, verantwortlich. Hierzu kontrollieren die Komponenten Network Access Requestor (NAR) und Network Access Authority (NAA) die physische Verbindung. Die

Kommunikation erfolgt wiederum mit Hilfe von Nachrichten, die durch die Schnittstelle IF-T spezifiziert sind [Trus12, DGHS14].

4 Integration von TNC im Smart Metering System

Das Sicherheitskonzept aus dem Forschungsprojekt SPIDER beschreibt drei Sicherheitsstufen. Die ersten zwei Sicherheitsstufen werden mit Hilfe von speziellen Hardwaremaßnahmen umgesetzt. Diese Stufen bilden die Basis für ein sicheres SMGW und sind unabhängig von anderen Systemen umsetzbar. Im Forschungsprojekt SPIDER wird, neben den bereits genannten Schutzmaßnahmen für die Hardware (siehe Abschnitt 3.1), ein spezieller Co-Prozessor für den Schutz zur Startzeit durch das Secure Boot-Muster (siehe Abschnitt 3.2) eingesetzt [DGHS14].

Die dritte Stufe des Sicherheitskonzeptes wird dagegen mit Hilfe von Software umgesetzt. Sie dient dazu Manipulationen an einem SMGW, mit Hilfe von TNC, für die Rollen im Smart Metering System zur Laufzeit sichtbar zu machen. Dazu ist es wichtig, dass TNC mit dem Anwendungskontext, in dem diese Technologie eingesetzt wird, verknüpft ist. Eine Verbesserung der Sicherheit eines Smart Metering Systems durch TNC ist nur möglich, wenn der ermittelte Integritätszustand den verschiedenen Teilnehmern zur Verfügung gestellt wird. Der ermittelte Integritätszustand des SMGW ist hierbei für den GWA, der für die Verwaltung des SMGW zuständig ist und den EMT, der auf die Richtigkeit der Daten eines SMGW angewiesen ist, in gleichem Maße wichtig. Im Folgenden wird hierzu eine erfolgreiche Integration von TNC in ein Smart Metering System auf der Basis des erläuterten Sicherheitskonzeptes (s. Abschnitt 3) vorgestellt, die im Rahmen des Forschungsprojekts SPIDER zur Demonstration des Mehrwerts umgesetzt wurde.

4.1 Gateway Administrator

Der GWA nutzt TNC in der Demonstration für die Überwachung des Integritätszustands eines SMGW. Dazu empfängt und prüft er als PDP regelmäßig Messwerte von dem AR eines SMGW, die den Integritätszustand des SMGW beschreiben. Das Ergebnis der Prüfung leitet der GWA an das SMGW weiter (vgl. [DGHS14]) und speichert es parallel dazu, für die Verwaltung des SMGW, ab. Abbildung 4 stellt die Beziehungen zwischen TNC und den durch das Forschungsprojekt SPIDER identifizierten und implementierten Funktionen eines GWA dar, die für die Realisierung benötigt werden. Die Abhängigkeiten sind hierbei so definiert, dass TNC unabhängig von anderen Komponenten beim GWA eingesetzt werden kann und die Integritätsdaten für weitere Komponenten zur Verfügung stellt [Genz15].

Eine wesentliche Aufgabe des GWA ist die Verwaltung eines SMGW (siehe [Bund15a]). Das BSI definiert dazu, dass der GWA die Funktionen eines SMGW mit Hilfe von Konfigurationsprofilen über das WAN konfigurieren kann (siehe [Bund13c]). Hierzu gehört auch die Konfiguration von TNC auf dem SMGW, wenn TNC durch den GWA unterstützt wird. Des Weiteren soll der GWA ein SMGW überwachen und in diesem Zusammenhang zum Beispiel das System-Log oder die Netzzustandsdaten von einem SMGW auslesen und auf Ereignisse eines SMGW reagieren können (siehe [Bund15a])]. Das Ergebnis einer Integritätsprüfung durch TNC wird in diesem Kontext als ein Ereignis eingeordnet, auf das der GWA reagieren kann, wenn er TNC unterstützt. Hierzu speichert der TNCS beim GWA das Ergebnis einer Integritätsprüfung zu einem SMGW in einem Datenmodell ab, auf das die anderen Funktionen des GWA für die Verwaltung eines SMGW zugreifen können. Zur Diagnose wird der Ablauf der

Integritätsprüfung außerdem durch den TNCS in einem Logbuch beim GWA protokolliert [Genz15].

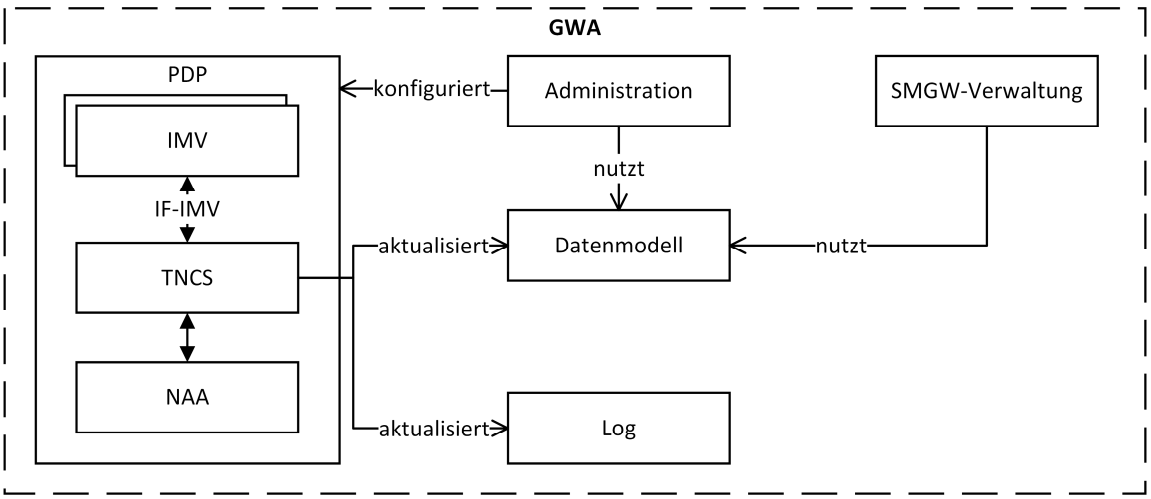

Abb. 4: TNC-Integration beim GWA [Genz15]

Ein GWA kann mehrere SMGW von unterschiedlichen Herstellern, die TNC unterstützen, verwalten und dementsprechend überwachen. Die Messwerte, die durch die verschiedenen SMGW zur Integritätsprüfung an den GWA gesendet werden, sind hierbei davon abhängig, wie ein Hersteller den Zustand definiert, in dem ein SMGW als vertrauenswürdig gilt. Da der GWA als verwaltende Instanz keinen Einblick in die genaue Systemstruktur eines SMGW hat, ist er auf Vorgaben für die Integritätsprüfung durch die Hersteller der SMGW angewiesen. Hierzu gibt es zwei Möglichkeiten, wie ein Hersteller Vorgaben an den GWA weitergeben kann. Die erste Möglichkeit besteht darin, dass alle Hersteller die gleiche, fest definierte Anzahl von Messwerten unterstützen müssen, die durch einen IMC gemessen und durch einen IMV beim GWA überprüft werden können. Ein Hersteller übermittelt in diesem Fall entsprechende Referenzwerte an den GWA, die den vertrauenswürdigen Zustand seiner SMGW definieren. Mit diesen übermittelten Werten konfiguriert der GWA die IMV für die Integritätsprüfung mit Hilfe der Administration. Die zweite Möglichkeit besteht darin, dass jeder Hersteller spezialisierte IMV bereitstellt, welche die Integrität seiner SMGW evaluieren können. In diesem Fall muss der GWA den TNCS konfigurieren, sodass die bereitgestellten IMV für die Prüfung verwendet werden. Ergänzend dazu kann der GWA über die Administration weitere Parameter, wie die Verbindungsparameter zu einem SMGW für die Remote Attestation durch TNC, konfigurieren [Genz15].

4.2 Smart Meter Gateway

Für die Demonstration wird TNC im SMGW integriert, um die Überwachungs- und Selbstschutzmaßnahmen des SMGW zu ergänzen. Hierzu misst und versendet das SMGW als AR regelmäßig seinen Integritätszustand zur Prüfung an den GWA (vgl. [DGHS14]). Das SMGW speichert das vom GWA empfangene Ergebnis der Integritätsprüfung als Messwert zum Systemzustand, um es im Programmablauf weiter verarbeiten zu können. Abbildung 5 stellt die Beziehungen zwischen TNC und den durch das Forschungsprojekt SPIDER identifizierten und implementierten Funktionen des SMGW (vgl. [Bu13a]) dar, die für die Demonstration benötigt werden [Genz15].

TNC ist eine optionale Funktion innerhalb des SMGW, da es nicht zwingend von einem GWA unterstützt werden muss (siehe [DGHS14]). Aus diesem Grund ist TNC innerhalb des SMGW werksseitig deaktiviert und muss explizit durch den GWA mit Hilfe entsprechender Konfigurationsprofile (siehe Abschnitt 4.1) über das WAN aktiviert werden. Hierbei kann der GWA ein Prüfungsintervall und die Verbindungsparameter für die Verbindung zum GWA konfigurieren. Solange TNC deaktiviert ist, gilt der Integritätszustand eines SMGW als unbekannt [Genz15].

Das Ergebnis einer Integritätsprüfung mit TNC beschreibt den Integritätszustand des SMGW zum Zeitpunkt der Prüfung. Aus diesem Grund wird das Ergebnis durch den TNCC des SMGW nach jeder Integritätsprüfung, im Datenmodell des SMGW, aktualisiert. Eine Prüfungshistorie ist ebenfalls möglich. Die Daten werden auf dem SMGW mit Hilfe der Mehrbenutzerfähigkeit und den granularen Dateisystemberechtigungen von Linux vor Veränderungen geschützt (vgl. [DGHS14]).

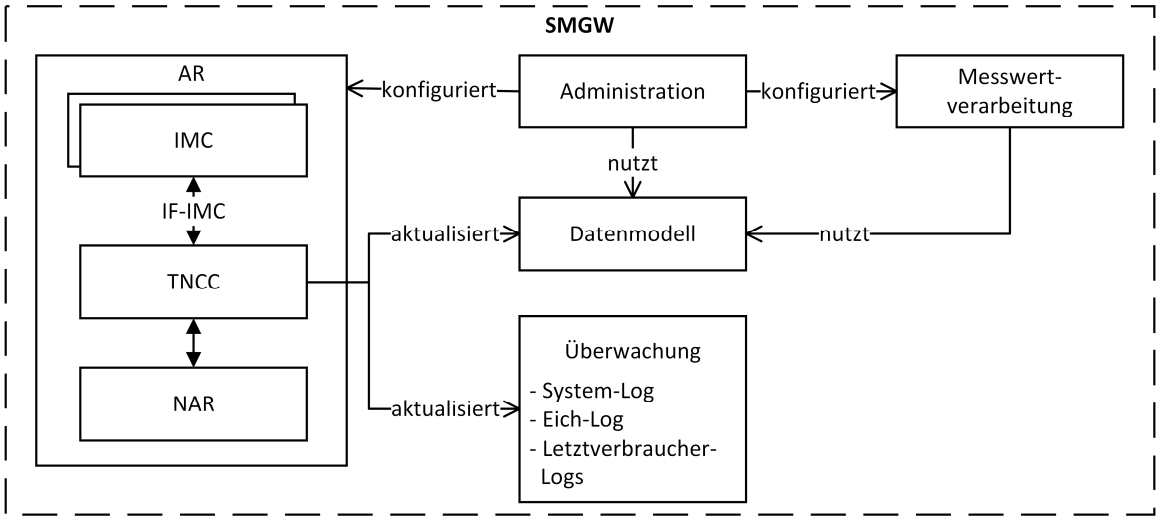

Abb. 5: TNC-Integration beim SMGW [Genz15]

Mit Hilfe entsprechender Konfigurationsprofile des GWA kann der Integritätszustand aus dem Datenmodell, als Teil der Netzzustandsdaten eines SMGW, über die Messwertverarbeitung auch an EMT im WAN weitergeleitet werden (vgl. [Bund13]). Hierzu wird eine für die Kommunikation im WAN vorgegebene Datenstruktur mit der Bezeichnung Register eingesetzt (vgl. [Deut14]). Außerdem kann ein gespeicherter Integritätszustand, insbesondere während der Verarbeitung von Messwerten, aus dem LMN von einem SMGW genutzt werden, um sicherzustellen, dass die Messwerte nicht durch interne Fehler verfälscht wurden. Das SMGW bildet hierzu ein Statuswort mit Hilfe verschiedener Prüfkriterien, das den eigenen Zustand beschreibt. Wenn der Zustand fehlerhaft ist, werden die Messwerte zur Diagnose gekennzeichnet (siehe [Bund13]). Der Integritätszustand kann hierbei als Prüfkriterium herangezogen werden [Genz15].

Das BSI hat festgelegt, dass das SMGW alle relevanten Ereignisse zur Überwachung in Logbüchern speichert. Das Eich-Log enthält in diesem Kontext nur eichtechnisch relevante Ereignisse. Hierzu zählen alle Ereignisse, die zu verfälschten Messwerten führen können. Das System-Log enthält alle wichtigen Ereignisse des SMGW. Hierzu gehören, neben den Ereignissen im Eich-Log, auch allgemeine Systemereignisse. Außerdem gibt es ein Logbuch für jeden Letztverbraucher, damit dieser alle ihn betreffenden Vorgänge auf dem SMGW nachvollziehen kann [Bund13]. Zur Diagnose wird der Ablauf der Integritätsprüfung durch TNC im System-

Log protokolliert (siehe Abbildung 5). Das Ergebnis der Integritätsprüfung wird zudem in den Logbüchern der Letztverbraucher vermerkt. Sofern die Integritätsprüfung negativ ausfällt, wird dies zusätzlich im Eich-Log eingetragen, da die Vertrauenswürdigkeit der Messdaten nicht mehr gegeben ist. Darüber hinaus wird in allen Logbüchern ein Eintrag vorgenommen, sobald TNC aktiviert oder deaktiviert wird. Hierdurch kann nachvollzogen werden, ob der Integritätszustand wie beschrieben im SMGW verwendet wird. Solange TNC deaktiviert ist, wird der Integritätszustand nicht wie beschrieben verwendet, da der Integritätsstatus eines SMGW dann nicht zuverlässig bestimmt werden kann [Genz15].

4.3 Übertragung von TNC-Daten

In Abschnitt 3.3 wird die Schnittstelle IF-T als Schnittstelle zur physischen Übertragung von TNC-Daten in Form von Nachrichten vorgestellt. IF-T dient hierbei als Abstraktionsebene zu weiteren Übertragungsprotokollen auf tieferen Ebenen. Die TCG hat in Abhängigkeit zu diesen tieferen Ebenen die folgenden zwei unterschiedlichen Spezifikationen für IF-T definiert [Trus12]:

- TNC IF-T: Protocol Bindings for Tunneled EAP Methods. Diese Spezifikation beschreibt die Einbindung von TNC als Methode des Extensible Authentication Protocol zur Prüfung der Integrität eines Systems während der Authentifizierung für den Zugriff auf ein Kommunikationsnetz [Trus14].
- TNC IF-T: TNC IF-T: Binding to TLS. Diese Spezifikation beschreibt den Einsatz von TNC zur Prüfung der Integrität eines Systems, wenn es bereits Teil eines Kommunikationsnetzes ist. Hiermit lässt sich auch eine längerfristige Systemüberwachung mit Hilfe regelmäßiger Integritätsprüfungen umsetzen. Die TNC-Daten werden dabei mit Hilfe von Transport Layer Security (TLS) geschützt [Trus13].

Die Analyse zur Anwendbarkeit von TNC im Forschungsprojekt SPIDER hat jedoch ergeben, dass die bestehenden Spezifikationen der TCG für IF-T den Vorgaben des BSI zu den eingesetzten Protokollen im WAN teilweise widersprechen oder nicht eingesetzt werden können. Eine detaillierte Betrachtung zeigt, dass [Trus14] nicht eingesetzt werden kann, weil ein SMGW immer durch den GWA erreichbar sein muss. Die Spezifikation [Trus13] ist dagegen für bestehende Verbindungen vorgesehen. Die Vorgaben dieser Spezifikation zum Einsatz von TLS widersprechen jedoch den Vorgaben des BSI zum Einsatz von TLS im WAN. Zur Lösung dieses Problems wurden verschiedene auf das SMGW angepasste Ansätze für IF-T entworfen. Hierzu zählt unter anderem der Einsatz eines vom BSI definierten Protokolls für die Alarmierung und Ereignisvermittlung im WAN, wie in [DGHS14] vorgeschlagen. Die anschließende Bewertung der einzelnen Ansätze für IF-T, zwischen einem SMGW und einem GWA, führte allerdings zu einem anderen Ergebnis. Entgegen der Annahme aus [DGHS14] kann IF-T am einfachsten durch die Anpassung von [Trus13] umgesetzt werden. Hierbei sind die kryptografischen Vorgaben und der Protokollablauf an die Vorgaben aus den Richtlinien des BSI angepasst [GeSe15].

Im Gegensatz zu den Vorgaben der TCG in [Trus13] kann eine Verbindung für eine Integritätsprüfung nicht durch beide Kommunikationspartner hergestellt werden. Nur das SMGW kann eine Verbindung für eine Integritätsprüfung zum GWA herstellen. Eine Verbindung kann außerdem nur für eine einzelne Integritätsprüfung genutzt werden und wird im Voraus mit Hilfe von Zertifikaten durch beide Kommunikationspartner authentifiziert. Andere, durch die TCG erlaubte, Authentifizierungsmethoden sind nicht möglich (vgl. [Trus13]). Entgegen den Vorgaben der TCG sind, für den Einsatz von TLS, zudem nur kryptografische Verfahren erlaubt, die

elliptische Kurven verwenden (vgl. [Bund16]). Außerdem ist eine erneute Verhandlung der Sicherheitsparameter für eine bestehende, durch TLS gesicherte, Verbindung nicht erlaubt und die Dauer einer Verbindung wurde durch das BSI im Vergleich zu den Vorgaben der TCG auf maximal 48 Stunden eingeschränkt. An wenigen Stellen lässt das BSI jedoch auch Ergänzungen für den Einsatz von TLS zu. Hierdurch kann ein eindeutiger Wert zu einer TLS gesicherten Verbindung (tls-unique) als Schutz vor Man in the Middel-Angriffen eingesetzt werden (vgl. [Trus13]). Darüber hinaus ist eine weiterführende Prüfung von Zertifikaten anhand des Namens eines Kommunikationspartners möglich (vgl. [Trus13, GeSe15]).

Die Kompatibilität zu [Trus13] bleibt trotz der beschriebenen Änderungen weitestgehend erhalten, sodass die Schnittstelle auch mit anderen standardisierten Umsetzungen von TNC eingesetzt werden kann. IF-T ist damit ein zusätzliches Protokoll zur Kommunikation zwischen dem SMGW und dem GWA im WAN. Die darüber liegenden Ebenen von TNC sind in Software umgesetzt und von den Richtlinien des BSI nicht beeinflusst, daher können die dort vorhandenen Spezifikationen ohne Anpassungen verwendet werden. Alle weiteren Vorgaben des BSI zur Kommunikation im WAN (vgl. [Bund13]) bleiben davon unberührt [GeSe15].

5 Fazit und Ausblick

Das Sicherheitskonzept aus dem Forschungsprojekt SPIDER definiert verschiedene Maßnahmen aus dem Bereich Trusted Computing zum Schutz der Integrität eines SMGW mit dem Ziel, die Sicherheit eines intelligenten Messsystems zu verbessern. Ein wesentlicher Aspekt des Sicherheitskonzeptes ist die Überwachung der Integrität eines SMGW mit Hilfe von TNC durch den GWA aus der Ferne. Eine Verbesserung der Sicherheit eines Smart Metering Systems durch TNC ist aber nur möglich, wenn der ermittelte Integritätszustand den verschiedenen Rollen im Smart Metering System zur Verfügung gestellt wird. Der ermittelte Integritätszustand des SMGW ist hierbei für den GWA, der für die Verwaltung des SMGW zuständig ist, und den EMT, der auf die Richtigkeit der Daten eines SMGW angewiesen ist, in gleichem Maße wichtig. Diese Veröffentlichung beschreibt hierzu eine demonstrative Integration von TNC im Smart Metering System auf Basis des genannten Sicherheitskonzepts und zeigt damit eine sinnvolle, interoperable Einbindung der Integritätsüberwachung mit TNC in die Programmabläufe eines Smart Metering Systems und den damit verbundenen Mehrwert. Gleichzeitig wird die Umsetzbarkeit und Praxisrelevanz des Sicherheitskonzepts demonstriert und es werden Probleme bei der Kombination der Vorgaben des BSI und der TCG sowie ein entsprechender Lösungsweg angesprochen. Zum Ende des Forschungsprojekts wurde die vorgestellte Integration gemeinsam mit den anderen Funktionseinheiten eines SMGW in die Produktentwicklung[4] überführt.

Die geringe Komplexität der Umsetzung soll an dieser Stelle als anregendes Beispiel für weitere Anwendungsbereiche von Trusted Computing zum Schutz der Integrität kritischer Infrastrukturen dienen. Im Rahmen der Umsetzung wurden außerdem Code-Bibliotheken[5] zu den aktuellen Vorgaben aus dem Bereich TNC entwickelt, die zukünftig weiter gepflegt und bearbeitet werden müssen, um sie für Hersteller und weiterführende Forschung und Entwicklung interessant zu machen. Die angesprochenen Code-Bibliotheken sind als Open Source lizenziert.

[4] devolo Smart Meter Gateway: http://www.devolo.com/de/SmartGrid/Technologie-Smart-Meter-Gateway

[5] Java basierte Code-Bibliothek zu TNC (jTNC): https://github.com/trusthsbremen/jtnc

Abkürzungen

AR	Access Requestor
BSI	Bundesamt für Sicherheit in der Informationstechnik
CLS	Controllable Local Systems
EMT	Externer Marktteilnehmer
GWA	Gateway Administrator
HAN	Home Area Network
IMC	Integrity Measurement Collector
IMV	Integrity Measurement Verifier
LMN	Local Metrological Network
LV	Letztverbraucher
NAA	Network Access Authority
NAR	Network Access Requestor
PDP	Policy Decision Point
SMGW	Smart Meter Gateway
SPIDER	Sichere Powerline-Datenkommunikation im intelligenten Energienetz
SRV	Service-Techniker
TCG	Trusted Computing Group
TLS	Transport Layer Security
TNC	Trusted Network Connect
TNCC	TNC Client
TNCS	TNC Server
WAN	Wide Area Network

Literatur

[Bund13] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, BSI (2013).

[Bund13a] Bundesamt für Sicherheit in der Informationstechnik: Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), BSI (2013).

[Bund13b] Bundesamt für Sicherheit in der Informationstechnik: Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), BSI (2013).

[Bund13c] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-1 Anlage VI : Betriebsprozesse, BSI (2013).

[Bund14] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-2 Smart Meter Gateway Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, BSI (2014).

[Bund15] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-0 Dachdokument, BSI (2015).

[Bund15a] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-6 Smart Meter Gateway Administration, BSI (2015).

[Bund16] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3: Intelligente Messsysteme, BSI (2015).

[Deut14] Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE: Smart Meter Gateway Teil 2: Klassen-Definition zur TR 03109 nach COSEM, DKE(2014).

[DGHS14] K.-O. Detken, C.-H. Genzel, O Hoffmann, R. Sethmann: Absicherung von Smart-Meter-Umgebungen mit Trusted Computing. In: P. Schartner, P Lipp: D.A.CH Security 2014: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, syssec-Verlag (2014).

[Genz15] C.-H. Genzel: Konzeption und Implementierung von Trusted Network Connect mit einer angepassten Transportschnittstelle für auf BSI-Spezifikationen beruhende intelligente Messsysteme, Master Thesis (2015).

[GeSe15] C.-H. Genzel, R. Sethmann: Custom Transport Interface for the Integration of Trusted Network Connect in German Smart Metering Systems. In: J. Brynielsson, M. Hoon Yap: 2015 European Intelligence and Security Informatics Conference, IEEE Computer Society CPS (2015) 45-52.

[KRC+10] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, A. Monti: Trust infrastructures for future energy networks. In: Power and Energy Society General Meeting, IEEE (2010) 1-7.

[LöSW10] H. Löhr, A.-R. Sadeghi, M. Winandy: Patterns for Secure Boot and Secure Storage in Computer Systems. In: IEEE: ARES '10 International Conference on Reliability, and Security, IEEE (2010) 569-573.

[Trus12] Trusted Computing Group: TCG Specification Architecture Overview Specification. TCG PUBLISHED (2012).

[Trus13] Trusted Computing Group: TCG Trusted Network Connect TNC IF-T: Bindings to TLS. TCG PUBLISHED (2013).

[Trus14] Trusted Computing Group: TCG Trusted Network Connect TNC IF-T: Protocol Bindings for Tunneled EAP Methods. TCG PUBLISHED (2014).