Integritätsmessung von Smart Meter Gateways

Kai-Oliver Detken · Marcel Jahnke · Malte Humann

DECOIT GmbH
{detken | jahnke | humann}@decoit.de

Zusammenfassung

Smart-Meter-Infrastrukturen werden zunehmend durch die Energieversorger geschaffen, um dezentrale Energienetze verwalten und betreiben zu können. Dabei nimmt ein Smart Meter Gateway (SMGW) eine zentrale Position ein, da es die Verbindung zu Smart-Meter-Sensoren hält und von außen sicher erreichbar sein soll. Dabei ist es wichtig zu wissen, ob ein SMGW im Vorfeld kompromittiert worden ist oder ob man es noch uneingeschränkt nutzen und darauf vertrauen kann. Hierzu können Trusted-Computing-Mechanismen verwendet werden, wie dies auch im Forschungsprojekt SPIDER [SPIDER16] umgesetzt wurde. Auf Basis eines Embedded-Linux-Systems wurde eine Integritätsmessung auf Grundlage eines Trusted Network Connect (TNC) implementiert, die erkennen soll, ob es Manipulationen an dem Betriebssystem oder der Hardware gab. Die Vorgaben an eine solche Sicherheitsarchitektur kommen in Deutschland vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Leider widersprechen diese den Spezifikationen der Trusted Computing Group (TCG) teilweise, so dass im SPIDER-Projekt eine Lösung umgesetzt wurde, die beiden Organisationen gerecht wird. Der entstandene Prototyp wird seit dem Projektende in ein Produkt überführt, weshalb aktuell Testbed-Analysen durchgeführt werden.

1 Einleitung

Mit der Novelle des *Energiewirtschaftsgesetzes (EnWG)* im Jahre 2011 wurde beschlossen Smart-Meter-Infrastrukturen in deutschen Energienetzen einzuführen. Solche intelligenten Messsysteme setzen sich laut EnWG aus mindestens einer elektronischen Messeinrichtung zur Erfassung von Messwerten und einer Kommunikationseinrichtung zur Verarbeitung, Speicherung und Weiterleitung dieser Messwerte zusammen. Durch intelligente Messsysteme sollen die Netzsteuerung sowie die Anbindung von Energieerzeugungsanlagen verbessert werden. Gleichzeitig sollen solche Messsysteme genutzt werden, um Verbrauchsdaten aufzubereiten, um damit die Energiebilanz von Haushalten zu verbessern.

Durch die Einstufung von Energieversorgungsnetzen als *kritische Infrastruktur (KRITIS)* legt das EnWG fest, dass Smart-Meter-Komponenten eindeutigen Sicherheits- und Interoperabilitätsstandards genügen müssen. Insbesondere die Normen und Richtlinien des BSI, der Bundesnetzagentur, der Physikalisch Technischen Bundesanstalt (PTB) und des Verbands der Elektrotechnik, Elektronik und Informationstechnik (VDE) mit den Lastenheften des Forums Netztechnik/Netzbetrieb (FNN) sind dafür ausschlaggebend. Das BSI hat in Zusammenarbeit mit weiteren Partnern eine entsprechende Sicherheitsarchitektur entworfen. Diese Architektur definiert das im EnWG vorgesehene *Smart Meter Gateway (SMGW)* eines intelligenten Messsystems als zentrale Rolle zum Schutz der angeschlossenen Messeinrichtung und deren Daten.

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 309-320.

Während das SMGW durch die definierte Sicherheitsarchitektur vor dem Zugriff von außen gut geschützt ist, kann es jedoch nicht ausgeschlossen werden, dass die Software des SMGW verändert oder manipuliert werden kann. Geschieht dies, ist ein Vertrauen in die erhobenen Messdaten nicht mehr gegeben. Aus diesem Grund wurden im SPIDER-Projekt Konzepte und Techniken der *Trusted Computing Group (TCG)* herangezogen, um Integritätsmessungen durchführen und durch den externen SMGW-Administrator (GWA) eine Manipulation remote erkennen zu können. Dabei ist besonders wichtig festzulegen, welche Werte ermittelt und gemessen werden sollten, um eine Integrität mit Sicherheit feststellen zu können.

2 Das SPIDER-Projekt

Das SPIDER-Projekt (Sichere Powerline-Datenkommunikation im intelligenten Energienetz) war ein gefördertes BMWi-Projekt mit einer Laufzeit von zwei Jahren und zwei Monaten, welches im März 2013 seine Arbeiten aufnahm. An dem Projekt waren Industriefirmen und deutsche Forschungseinrichtungen beteiligt. Als assoziierte Partner sind Energieversorger sowie ein Chiphersteller mit einbezogen worden, um die Anforderungen der Energiebranche von Anfang an zu berücksichtigen und Feldtests durchführen zu können. Ziel des Projekts war die Entwicklung eines prototypischen *Smart Meter Gateways (SMGW)*, welches den BSI-Sicherheitsanforderungen genügt. Als Besonderheit wurde die Kommunikation des SMGW über die letzte Meile nicht über bestehende Internet-Verbindungen angestrebt, sondern mittels des Stromnetzes über Power-Line Communication (PLC). Erst ab der Netzstation kommt dann das Internet als Transfernetz zum Einsatz. Das hat den Vorteil, dass die Kommunikation zum Letztverbraucher klar getrennt vorgenommen wird.

In dem Projekt mussten auch verschiedene *Externe Marktteilnehmer (EMT)* mit ihren Interessen im Energienetz in einem Smart-Grid-Szenario mit berücksichtigt werden [BSI13a]:

a. **Messstellenbetreiber (MSB):** Trägt die Verantwortung für die eingesetzten Messsysteme.
b. **Messdienstleister (MDL):** Ab- und Auslesen von Verbrauchszähleinrichtungen.
c. **Verteilnetzbetreiber (VNB):** Unterhält das örtliche Stromnetz und wartet es.
d. **Lieferanten:** Handelswarenvertreter, der für die Nutzung des Netzes Gebühren an den VNB bezahlt.
e. **SMGW-Administrator (GWA):** Ist in viele Prozesse des SMGW-Lebenszyklus eingebunden (Datenübertragung, Administration und Eichung im laufenden Betrieb).

Die Sicherheit und Stabilität zukünftiger, intelligenter Energienetze hängt maßgebend von einer sicheren Datenübertragung zwischen den o.g. Teilnehmern sowie den eingesetzten Steuerkomponenten ab. Das BSI hat deshalb in diesem Umfeld eine Architektur definiert, die neben den eigentlichen intelligenten Messsystemen (Smart Meter) eine lokale Kommunikationseinheit, das sog. *Smart Meter Gateway (SMGW)*, zum Schutz dieser Messsysteme und deren Messdaten vorsieht. Sie bilden zusammen die Basis eines Smart-Metering-Systems (siehe auch [DGHS14]).

Das SMGW ist daher die zentrale Instanz eines *Smart-Metering-Systems*. Es besitzt die Logik zur verlässlichen Verarbeitung und sicheren Speicherung von Messdaten angeschlossener Messsysteme und soll die sichere Datenübertragung zwischen den einzelnen Teilnehmern in den angeschlossenen Netzen ermöglichen. Bei den Netzen handelt es sich gemäß den Vorgaben des BSI (vgl. [BSI13a]) um folgende Netzbereiche:

a. **Local Metrological Network (LMN):** ein Netz zur lokalen Anbindung von Messgeräten (Strom-, Gas- oder Wasserzähler) der Endnutzer (Letztverbraucher, LV).
b. **Home Area Network (HAN):** ein Netz zur lokalen Anbindung und Steuerung von Energieerzeugern und Energieverbrauchern (Controllable Local Systems, CLS) der Letztverbraucher sowie zur Informationsbereitstellung für Letztverbraucher und technisches Betreiberpersonal (Service-Techniker, SRV).
c. **Wide Area Network (WAN):** ein Netz zur Anbindung des GWA für die SMGW-Verwaltung und autorisierter Dritter (EMT) zur Datenvermittlung.

Der *GWA* ist die einzige vertrauenswürdige Instanz innerhalb des intelligenten Messsystems. Er kann das SMGW konfigurieren und übernimmt dessen Überwachung und Steuerung. Hierzu erstellt er verschiedene Konfigurationsprofile, wie z.B. Tarifierung, Bilanzierung und Netzzustandserfassung. Der GWA ist daher berechtigt über das WAN aktiv auf das SMGW zuzugreifen.

Abb. 1: SMGW-Komponente im Hutschienenformat

Das *SMGW* verbindet, als zentrale Kommunikationseinheit des Smart-Meter-Gesamtsystems, die beschriebenen Komponenten und Rollen über die angeschlossenen Netze miteinander (siehe Abbildung 1). Hierfür stellt es entsprechende Schnittstellen zur Verfügung. Für die Überwachung und Kontrolle der Kommunikation über diese Schnittstellen wird dabei die Funktion einer Firewall wahrgenommen. Daher schreibt das BSI vor, dass die Schnittstellen physikalisch voneinander getrennt sein müssen. Zusätzlich beinhaltet das SMGW Methoden zur Speicherung und Verarbeitung von Messwerten aus dem LMN mit Hilfe von Regelwerken zur Tarifierung, Bilanzierung und Netzsteuerung. Das SMGW kann dabei auch eigene Messwerte zum System- und Netzzustand erfassen, diese in Regelwerken abspeichern und weiterverarbeiten [Detk16].

Zur sicheren Übermittlung der Daten zwischen den einzelnen Komponenten und Rollen werden asymmetrische und symmetrische Verschlüsselungsverfahren eingesetzt. Hierbei wird zwischen *Inhaltsdaten- und Transportverschlüsselung* unterschieden. Messdaten werden generell vor der Übertragung durch das SMGW mittels Inhaltsdatenverschlüsselung gesichert und anschließend signiert. Bei der anschließenden Kommunikation muss dann eine Transportverschlüsselung eingesetzt werden. Zur Verschlüsselung verwendet das SMGW ein *Sicherheitsmodul*, welches folgende Funktionen aufweist:

a. Sichere Speicherung von Zertifikats- und Schlüsselmaterial
b. Schlüsselgenerierung und Schlüsselaushandlung auf Basis von Elliptischen Kurven
c. Erzeugung und Verifikation digitaler Signaturen
d. Zuverlässige Erzeugung von Zufallszahlen

Durch die zentrale Rolle, die ein SMGW in einer Smart-Meter-Umgebung einnimmt, müssen spezielle Methoden zum *Selbstschutz* integriert sein. Hierzu gehören zum einen die physische Versiegelung (Verplombung) und zum anderen die Kommunikationspriorisierung sowie die Systemüberwachung durch Log-Mitschnitte, Alarme und Selbsttests. Es fehlt allerdings eine Remote-Attestation-Überprüfung, bei der der GWA von seiner Stelle aus feststellen kann, ob ein Kompromittieren vorliegt oder nicht. Diese Lücke kann der TNC-Ansatz schließen, weshalb das SPIDER-Projekt diesen Ansatz untersucht und prototypisch implementiert hat [Genz15].

3 Trusted-Computing-Integritätskonzept

Die Architektur eines *Trusted Network Connect (TNC)* wurde bereits in anderen Veröffentlichungen (u.a. [DGHS14]) beschrieben, weshalb hier nicht noch einmal im Detail darauf eingegangen wird. Beachtet werden muss aber die Integritätsmessung, die im ersten Schritt durch das SMGW vorgenommen wird. Hierfür sind Hash-Summen vorgesehen, die periodisch über ausgesuchte Komponenten (z.B. eingesetzte Firmware-Komponenten, Konfigurationsdateien, Hardware-komponenten) gebildet werden. Die Messwerte werden auf Dateiebene gespeichert und mit Hilfe der Mehrbenutzerfähigkeit und der granularen Dateisystemberechtigungen von Linux vor Veränderungen geschützt. Da die Dateisystemrechte auf Kernelebene geprüft werden, sind die Zugangsrechte nur schwer auszuhebeln.

3.1 Integritätsmessung

Im Sinne von TNC übermittelt der *Integrity Measurement Collectors (IMC)* des SMGW die Messwerte zur Attestierung an den *Integrity Measurement Verifier (IMV)*, der sich auf der Seite des GWA befindet. Dementsprechend, muss auf der Seite des GWAs ein IMV umgesetzt werden, der die Werte des IMCs interpretieren kann. TNC-Client (TNCC) und TNC-Server (TNCS) sind für die Kommunikation und die Reaktion auf die Ergebnisse der Attestierung zuständig. Sie liegen als standardisierte Komponenten bereits in entsprechenden Bibliotheken vor. Bei negativen Ergebnissen muss zusätzlich der GWA eingreifen.

Bei einer reinen softwarebasierten Umsetzung kommt es in besonderem Maße darauf an, ein System zu nutzen, dass die Integrität der Software bereits beim Systemstart verifizieren kann, um das Vertrauen in die Messwerte zu sichern. Bei einer hardwarebasierten Umsetzung würde man ein *Trusted Platform Module (TPM)* einsetzen. Allerdings entspricht die derzeitige TPM-Version nicht den kryptografischen Anforderungen des BSI. Daher wurde im SPIDER-Projekt ausschließlich an einer softwarebasierten Lösung gearbeitet.

Das Forschungsprojekt SPIDER hat durch eine selbst durchgeführte Bedrohungsanalyse festgestellt, dass die SMGW-Komponente von außen relativ gut geschützt ist. Trotzdem kann auch beim SMGW, gerade durch die Öffnung des Kommunikationswegs über das Internet, eine Manipulation nicht gänzlich ausgeschlossen werden. Ob ein SMGW bzgl. seiner Software verändert worden ist, kann aber durch die BSI-Vorgaben nicht festgestellt werden. Aus diesem Grund führte das Projekt SPIDER zusätzlich Trusted-Computing-Spezifikationen ein, um die Integrität überwachen und dementsprechend besser schützen zu können.

3.2 Integritätsebenen

Bei der Umsetzung im SPIDER-Projekt lassen sich drei Integritätskontrollen unterscheiden:

a. Physikalische Integritätskontrolle
b. Integritätskontrolle beim Bootvorgang
c. Integritätskontrolle im Betrieb

Die *physikalische Integritätskontrolle* soll bei den BSI-Vorgaben durch das Anbringen einer Plombe am Gehäuse sichergestellt werden. Dadurch kann aber nur vor Ort erkannt werden, ob das Gehäuse unerlaubt geöffnet wurde und jemand anschließend versucht hat, die Hardware zu manipulieren. In SPIDER sollte daher auch die elektronische Überwachung mit einbezogen werden, indem ein Sensor erkennt, wenn das Gehäuse geöffnet wurde. Zusätzlich sollten ausgewählte Hardware-Bausteine durch ein Tamper Resistant Grid[1] geschützt werden, wodurch ebenfalls Manipulationen an diesen Hardware-Bausteinen erkannt werden können. Allerdings ließen sich beide Ziele innerhalb des Projektes nicht umsetzen, könnten aber zukünftig wieder mit einbezogen werden. Alle sicherheitskritischen Hardware-Bausteine sind allerdings fest eingebaut worden und können nicht ohne weiteres entfernt werden. Das Gehäuse selbst (siehe Abbildung 2) ist zweigeteilt aufgebaut und beherbergt verschiedene Platinen. Ein Zusammendrücken beider Gehäusehälften nach der Inbetriebnahme verschließt das Gehäuse permanent. Nur durch Beschädigung kann es anschließend wieder geöffnet werden. Dadurch will man die unbefugte Nutzung bzw. die unerkannte Manipulation verhindern, ähnlich einer Verplombung.

Um einer Software-Manipulation entgegenzuwirken, wurde im SPIDER-Projekt ein *sicheres Bootverfahren* (Secure Boot) implementiert, bei dem einzelne Bootstrap-Module in einer Bootsequenz nacheinander geladen und ausgeführt werden (siehe auch [DGHS14]). Jedes geladene Modul evaluiert hierbei sein Folgemodul durch eine kryptografische Signatur, bevor es weitere Module lädt. Der Boot-Prozess startet beim Boot-Loader, der auf einem Hardware-Baustein basiert, welcher schwer manipulierbar ist. Wenn die Signaturprüfung des Boot-Loaders erfolgreich verlaufen ist, wird dieser ausgeführt, indem der Hardware-Zustand und das Betriebssystem des SMGW getestet werden. Das Betriebssystem kann wiederum einzelne Software-Komponenten analysieren. Wenn eine Prüfung fehlschlägt wird das gesamte System zurückgesetzt und neu gestartet. Daher kann das SMGW nur dann erfolgreich in den Betrieb hochfahren, wenn alle Stationen des Startvorgangs erfolgreich geprüft wurden.

Die *Integritätskontrolle im Betrieb* soll nach BSI-Richtlinien durch einen Selbsttest umgesetzt werden. Dieser Selbsttest kann aber ebenfalls manipuliert worden sein, weshalb im SPIDER-Projekt der TNC-Ansatz als sinnvolle Ergänzung eingebracht wurde. Dadurch kann man die Integrität einer SMGW-Komponente über eine entfernte – aber vertrauenswürdige Instanz – mittels Remote Attestation kontrollieren. Der GWA muss nur eingreifen, wenn ein Integritätsproblem festgestellt wird. Da die TNC-Bausteine als Software-Komponenten in SPIDER umgesetzt wurden, müssen sie zum Schutz vor Manipulation durch das vertrauenswürdige Boot-Verfahren beim Startvorgang verifiziert und durch granulare Dateisystemberechtigungen geschützt werden.

[1] feinmaschiges Leiterbahnennetz, welches auf Veränderungen reagiert und einen Chip unbrauchbar macht

Abb. 2: Hardware-Prototyp von SPIDER

3.3 Integrationskonzept

Der *SMGW-Administrator (GWA)* nutzt im SPIDER-Projekt für die Überwachung der Integrität eines SMGW den TNC-Ansatz. Dazu empfängt der GWA kontinuierlich Messwerte von einem SMGW und prüft diese auf Basis vorgegebener Werte. Das Ergebnis der Prüfung wird vom GWA an das SMGW gesendet und parallel für spätere Überprüfungen abgespeichert. Da das Ergebnis den Zustand eines SMGW zum Zeitpunkt der Integritätsprüfung beschreibt, wird zusätzlich ein Zeitstempel zum Ergebnis gespeichert. Damit der GWA die Integritätsprüfung nachvollziehen kann, protokolliert das SMGW den Ablauf der Integritätsprüfung.

Ein GWA sollte mehrere SMGW unterschiedlicher Hersteller verwalten und überwachen können. Die Messwerte, die durch unterschiedliche SMGW-Komponenten zur Integritätsprüfung an den GWA gesendet werden, können allerdings differieren, da jeder Hersteller den Zustand der Vertrauenswürdigkeit selbst definieren kann. Ein Hersteller muss daher seine Vorgaben an den GWA weitergeben können, was durch zwei verschiedene Varianten umgesetzt werden kann:

a. Alle Hersteller unterstützen die gleiche, feste Anzahl von Attributen, die durch ein IMC gemessen und durch ein IMV überprüft werden können.
b. Jeder Hersteller stellt eine spezialisierte IMV bereit, die in der Lage ist, die SMGW-Integrität zu überprüfen.

Im ersten Fall übermittelt ein Hersteller nur die Referenzwerte, die den vertrauenswürdigen Zustand eines SMGW erkennen lassen, an den GWA. Der GWA konfiguriert die IMV des TNC-Servers (TNCS), so dass die übermittelten Werte des Herstellers zur Prüfung des SMGW verwendet werden können. Im zweiten Fall muss der GWA den TNCS so konfigurieren, dass er die bereitgestellten IMV für die Prüfung des SMGW eines Herstellers verwenden kann.

Das BSI hat festgelegt, dass zur Administration eines SMGW *COSEM*-basierte Konfigurationsprofile eingesetzt werden müssen. Diese werden über eine *RESTful-Webservice-Schnittstelle* an das SMGW verschickt, wodurch die Konfiguration, die Messwertverarbeitung und die Kommunikation ermöglicht werden. Der GWA kann über diese Schnittstelle zusätzlich Daten über den SMGW-Zustand abrufen. Da der TNC-Ansatz optional implementiert werden musste,

weil andere Herstellerlösungen diesen nicht kennen, kann die TNC-Funktionalität im SMGW auch deaktiviert werden. Das Aktivieren kann dabei über die RESTful-Schnittstelle vorgenommen werden. Der GWA bestimmt dazu das Prüfungsintervall und definiert die Verbindungsparameter für die Remote Attestation. Dabei ist der Integritätszustand eines SMGW bis zur ersten Überprüfung, sowie im Falle eines deaktivierten TNC unbekannt.

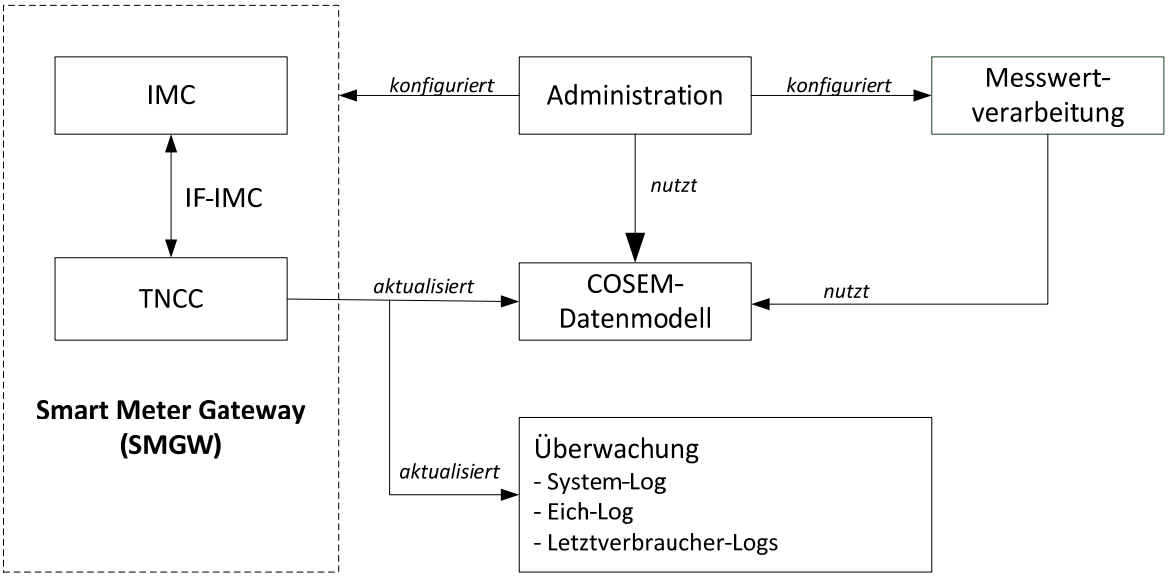

Abb. 3: TNC-Integration im SMGW

Abbildung 3 zeigt die TNC-Integration im SMGW bei SPIDER und den damit verbundenen Prozessen. Da die TCG-Spezifikation nicht alle BSI-Vorgaben erfüllt, mussten im SPIDER-Projekt entsprechende Anpassungen vorgenommen werden, die sich aber noch konform zu den ursprünglichen Spezifikationen verhalten.

Durch entsprechende *Konfigurationsprofile* können gespeicherte Integritätszustände aus dem Datenmodell über die Messwertverarbeitung auch an ein EMT gesendet werden. Zusätzlich kann der Integritätszustand bei der Verarbeitung von Messwerten aus dem LMN von einem SMGW verwendet werden, um festzustellen, ob die Messwerte unverfälscht sind. Hierzu bildet das SMGW ein Statuswort auf Basis verschiedener Prüfkriterien, das den eigenen Zustand beschreibt. Wenn der Zustand fehlerhaft ist, werden die Messwerte gekennzeichnet. Der Integritätszustand kann dabei ein Prüfkriterium für die Bildung des Statuswortes sein. Hierdurch kann das Vertrauen der EMT in die SMGW-Daten gestärkt werden.

Laut BSI-Spezifikationen muss das SMGW alle relevanten Ereignisse zur nachträglichen Überprüfung in *Logbüchern* speichern. Das Eich-Log enthält dabei nur eichtechnisch relevante Ereignisse (z.B. der Ausfall einer wichtigen Software-Komponente), die zu falschen Messwerten führen könnten. Hingegen enthält das System-Log dabei alle wichtigen Ereignisse. Hierzu gehören auch allgemeine Systemereignisse, wie fehlgeschlagene Verbindungen. Das Logbuch ist auch für den Letztverbraucher relevant, da dieser dadurch alle Vorgänge und Prozesse auf dem SMGW die ihn selbst betreffen nachvollziehen kann. Um Probleme bei der Integritätsprüfung zu erkennen, protokolliert der TNCC den Ablauf dieser Prüfung durch das System-Log. Bei einer negativen Integritätsprüfung wird dies in jedem Fall im Eich-Log hinterlegt, da der Trust-Zustand der Messdaten nicht mehr gewährleistet werden kann. Auch das Aktivieren/Deaktivieren der TNC-Funktionalität wird in allen Logbüchern festgehalten [Genz15].

4 Testbed-Ergebnisse

Im SPIDER-Projekt sind diverse Tests durchgeführt worden, um die *Interoperabilität* zu unterschiedlichen GWA-Anbietern sicherstellen und Sicherheitsmechanismen überprüfen zu können. Dabei wurden vier Arbeitsschritte einheitlich bei jedem Herstellertest durchgeführt:

a. Aushandlung der Roadmap
b. Festlegung der Infrastruktur
c. Durchführung der Interoperabilitätstests
d. Dokumentation der Ergebnisse

Die Testläufe des SMGW wurden auf Anwendungsebene durchgeführt. Als Voraussetzung für die Testfälle und Use Cases galten grundsätzlich die Anforderungen an die Infrastruktur. Die *Roadmap-Planung* diente der Abschätzung des Entwicklungsfortschritts. Diese Planung wurde durch unvollständige Definitionen der Technischen Richtlinien innerhalb des Projektes erschwert, so dass kontinuierlich Anpassungen aufgrund von Richtlinienänderungen notwendig wurden. Dennoch konnte eine Roadmap mit konkreten Zielvorgaben definiert werden.

Bei den Tests wurden die relevanten SMGW-Komponenten berücksichtigt. Dazu gehören die WAN-Schnittstelle, gemäß TR-03109-1 [BSI13a], der COSEM-Webservice und der Wake-Up-Service, die Überprüfung der Unterstützung von kryptografischen Verfahren [BSI13c] für das TLS-Protokoll, die Inhaltsdatenverschlüsselung mit Cryptography Message Syntax (CMS) und die Wake-Up-Paket-Signierung. Auch die Messung der SMGW-Systemintegrität wurde mit einbezogen, obwohl die GWA-Hersteller TNC nicht unterstützen. Aber dadurch konnten sie für diese Thematik sensibilisiert werden.

Für die *Interoperabilitätstests* kamen folgende Kommunikationsmöglichkeiten zur Anwendung:

a. Öffentliche IP-Adressen via Wide Area Network (WAN)
b. Private IP-Adressen via Virtual Private Network (VPN)
c. Private IP-Adressen via Internet Protocol Security (IPsec)

Es wurde bei den Tests stets eine bidirektionale Kommunikation zwischen GWA und SMGW verwendet, da beide Endpunkte über mindestens eine öffentliche Schnittstelle verfügen. Tabelle 1 listet die Services auf, die von den Interoperabilitätstests mit GWA-Softwareanbietern im optimalen Fall getestet wurden. Um eine vollständige Testabdeckung zu erreichen, mussten dabei alle vorhandenen WAN-Kommunikations-Szenarien (WKS) berücksichtigt werden. Des Weiteren ist TNC als zusätzliches WKS entwickelt worden.

Tab. 1: IP-Adressen und Ports der SMGW-/GWA-Dienste

Service	SMGW	GWA/EMT
Wake-Up-Service	<IP Adresse>:<Port>	-
WKS1: MANAGEMENT	-	<IP Adresse>:<Port>
WKS2: ADMIN-SERVICE	-	<IP Adresse>:<Port>
WKS3: INFO-REPORT	-	<IP Adresse>:<Port>
WKS4: NTP-HTTPS		<IP Adresse>:<Port>
WKS6: TNC	-	<IP Adresse>:<Port>

4.1 Absicherung der Inhalte und Kommunikation

Für die sichere Kommunikation müssen auf beiden Endpunkten sowohl die Schlüsselmaterialien als auch die Zertifikate ausgetauscht werden [BSI13b]. Auf dem SMGW stehen Schlüsselmaterialien für die Inhaltsdatenverschlüsselung mit CMS sowie für die gesicherte Kommunikation mit TLS zur Verfügung. Im Rahmen des SPIDER-Projektes wurden für die *X.509-Zertifikate* folgende Codierungen seitens der GWA-Softwareanbieter verwendet:

a. DER Codierung: Binäres Format
b. PEM Encoding: ASCII Format
c. PKCS #12 Archiv: geschützter Container Schlüsselmaterial (Dateiendung: .p12)

Die BSI-konformen Zertifikate [BSI13b] wurden dabei entweder vom GWA-Softwareanbieter zur Verfügung gestellt oder mit dem SPIDER-Zertifikatstool generiert. Da die BSI-Richtlinie die kryptographischen Vorgaben bis und ab 2014 unterteilte, mussten diese im Testbed entsprechend reflektiert werden. Betroffen waren davon die zulässigen Parameter für die *Elliptischen Kurven*. So war über die Laufzeit des Forschungsprojektes zunächst NIST P-256 als Elliptische Kurve zu wählen und wurde später durch BrainpoolP256r1 ersetzt [BSI15].

Als weitere Mindestanforderung wurde für die TLS-Verbindungen die TLS Cipher Suite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 vorgegeben. Für die Inhaltsdatenverschlüsselung konnte neben AES-CBC zusammen mit AES-CMAC alternativ auch AES-GCM verwendet werden, jeweils mit einem neu zufällig generierten 128-Bit-Schlüssel. Für den Schlüsselaustausch kam ECKA-EG mit X9.63 zur Schlüsselableitung zum Einsatz [BSI15].

Die *Use Cases* wurden im Vorhinein auf Basis der WAN-Kommunikationsszenarien [BSI13a] definiert und im Rahmen der Tests mit den GWA-Software-Anbietern weiterentwickelt. Sie bestehen prinzipiell aus einzelnen Testfällen. Der *Wake-Up-Service* wurde z.B. mit folgenden Use Cases getestet:

a. Der GWA sendet Wake-Up-Paket an das SMGW
b. Das SMGW validiert die Wake-Up-Paket-Datenstruktur
c. Das SMGW prüft die Wake-Up-Paket-Signatur

Für eine erfolgreiche Wake-Up-Prozedur muss eine korrekte TLS-Funktionalität vorliegen. Diese beinhaltet hauptsächlich den TLS-Handshake und die Parameter für die Cipher-Suites und Brainpool EC-Domain. Die korrekte Übertragung von Anwendungsdaten über TLS wurde wie folgt getestet:

a. Das SMGW initiiert ein TLS-Handshake mit dem GWA, basierend auf dem TLS-Schlüsselpaar
b. Das SMGW und der GWA halten für den TLS-Kanal eine Session bereit

Abbildung 4 zeigt den im Testbed verwendeten Aufbau. Um den Aufwand der Einrichtung der Testumgebung gering zu halten, teilen sich GWA und EMT eine Virtual Machine (VM), könnten alternativ aber auch auf unterschiedlichen Systemen eingerichtet werden.

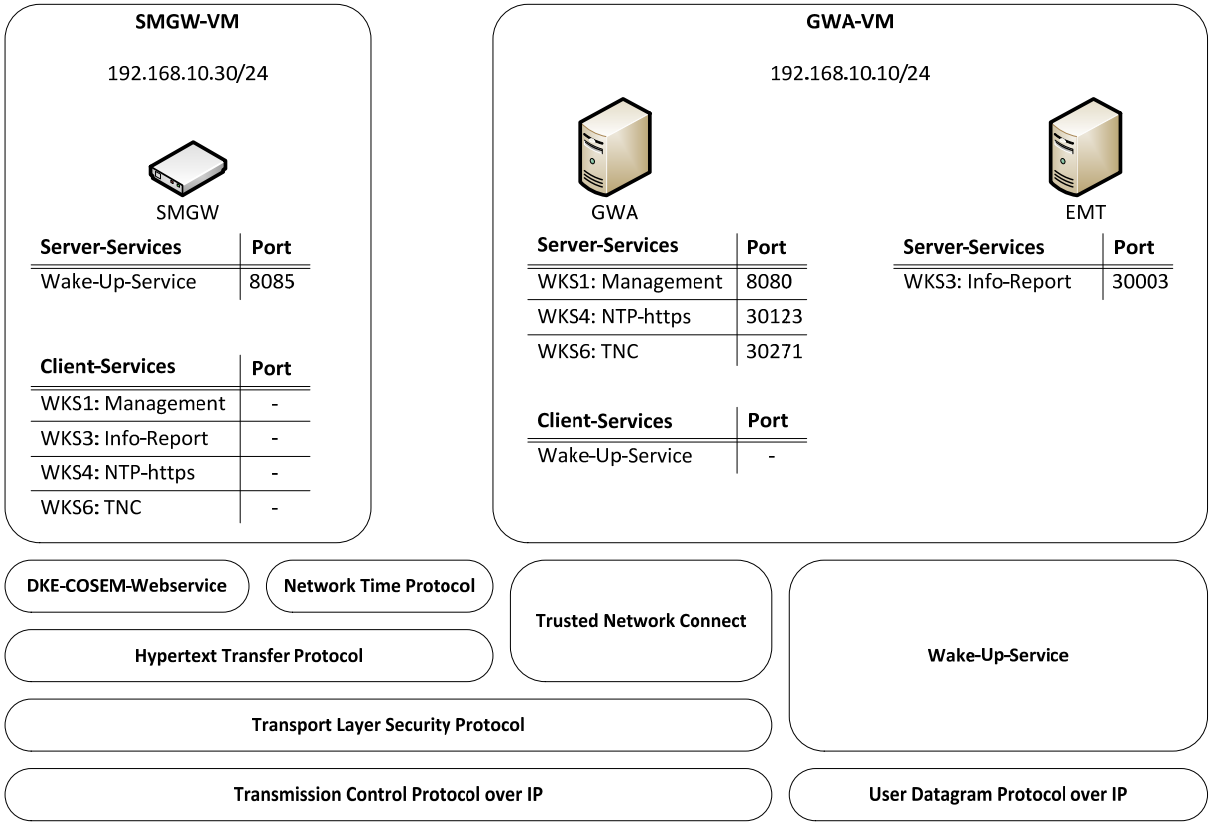

Abb. 4: Testumgebung mit SMGW, GWA und EMT

Weitere Use Cases wurden für Interoperabilitätstests mit CMS und COSEM-Webservice definiert. Dabei sind, für die Test-Definition, die unterschiedlichen Entwicklungsstände der Partner berücksichtigt worden.

4.2 One-Meter-Szenario

Einen besonderen Use Case stellt das *One-Meter-Szenario* dar, das mehrere einzelne Use Cases zu einem gemeinsamen Use Case kombiniert, wodurch die Interoperabilität vom Smart Meter bis hin zum EMT getestet werden kann. Zunächst wird über den Wake-Up-Service eine sichere Verbindung zwischen SMGW und GWA aufgebaut. Über diese Verbindung bringt der GWA die für das Szenario benötigten Profile von Zähler, Letztverbraucher, EMT und Anwendungsfall in das SMGW ein.

Die Profile werden über COSEM-Container-Klassen eingespielt, um sicherzustellen, dass diese vom COSEM-Webservice unterstützt werden. Das hat den Vorteil, dass nicht alle zu einem Profil gehörenden COSEM-Objekte einzeln in das SMGW eingebracht werden müssen, sondern direkt in einer Aktion als Bündel eingespielt (und geprüft) werden. In einem zweiten Schritt werden die Profile, soweit nötig, aktiviert. So wird überprüft, dass einzelne Attribute der COSEM-Objekte aktualisiert werden können. In einigen Fällen wurden hier zusätzlich herstellerspezifische Methoden mit berücksichtigt.

Nachdem alle relevanten Profile eingespielt und aktiviert wurden, beginnt das SMGW damit die Messwerte der Zähler zu erfassen und eine Erstauslesung für den verwendeten Anwen-

dungsfall *Datensparsame Tarife* (TAF1) an den EMT zu verschicken. Dabei wird die Anbindung eines Smart Meters an das SMGW, die Messwertverarbeitung und die Auslieferung von Messdaten an einen EMT überprüft.

4.3 Zusammenfassung der Testbed-Ergebnisse

Zusammenfassend konnte festgestellt werden, dass bei allen acht getesteten Herstellern der Wake-Up-Service weitestgehend umgesetzt war. Trotzdem konnten noch Fehler festgestellt und dokumentiert werden. Durch diverse Testzyklen wurden diese aber behoben. Der TLS-Handshake ließ sich bei sechs Herstellern erfolgreich testen. Auch hier konnte man auftauchende Fehlfunktionen erfolgreich kompensieren. Ähnliche Ergebnisse ließen sich bei der Inhaltsdatenverschlüsselung mittels CMS-Bibliothek und dem COSEM-Webservice ausmachen. In allen Fällen stellten die durchgeführten Interoperabilitätstests einen Mehrwert für die teilnehmenden Parteien dar, da Fehlfunktionen erkannt und beseitigt werden konnten. Es ließ sich dabei auch der entsprechende Reifegrad der jeweiligen Lösung feststellen. Auch zeigten sich durch die Tests, dass sich die Richtlinien des BSI unterschiedlich interpretieren lassen.

Auch kann als Ergebnis festgehalten werden, dass innerhalb des Forschungsprojektes mehrere Kompromisse gemacht werden mussten, um einen funktionsfähigen Prototypen innerhalb des Projektes entwickeln zu können. Aufgrund der guten Ergebnisse, die man im Testbed erzielt hatte, und der zu erwartenden Absatzmenge wurde entschieden, dass die Ergebnisse zu einem Produkt weiterentwickelt werden sollen. Zum gegenwärtigen Zeitpunkt (Stand: Mitte 2016) ist das One-Meter-Szenario einsatzbereit und wird von einem Energieversorger in einem Feldtest getestet. Weitere Aufgaben wurden aber bereits identifiziert und sind in Arbeit, wie z.B. die Steigerung der Performance oder die Senkung des Firmware-Speicherbedarfes.

Auch andere Konsortien entwickeln derzeit SMGW-Komponenten, um fristgerecht den Markt bedienen zu können. Den Einsatz von Trusted Computing wird dabei aber von den wenigsten Firmen bisher adressiert und konnte im SPIDER-Projekt als Innovation bzw. Sicherheitsverbesserung eingestuft werden.

5 Fazit

Das SPIDER-Konsortium hat sich an ein ganz neues Arbeitsfeld gewagt, indem es ein *Smart Meter Gateway (SMGW)* prototypisch entwickelte und zugleich einen innovativen Integritätscheck auf Basis von TNC implementierte. Dabei gab es einige Fallstricke und Hindernisse im Projekt zu beachten, was zum einen an den teilweise unfertigen Spezifikationen lag und zum anderen an dem Realisierungsgrad vorhandener TPM-Chips. Es bestand im SPIDER-Projekt von Anfang an die Zielsetzung nach Projektende ein SMGW-Produkt zu entwickeln. Daher wurde die Entwicklung dahingehend ausgerichtet. Trotzdem ist es immer ein weiter Weg von einem Prototyp zu einem fertigen Produkt, da in der Forschung auch Wege beschritten werden müssen, die evtl. nicht zu einem unmittelbaren Ergebnis führen. Zwei Industriepartner des Projektes haben trotzdem am Ende des Forschungsprojektes weiterhin dieses Ziel vor Augen und befinden sich auf einem guten Weg dorthin.

Danksagung

Das SPIDER-Projekt war ein gefördertes BMWi-Projekt mit einer Laufzeit von zwei Jahren, das im März 2013 seine Arbeiten begann. An dem Projekt waren die Firmen devolo AG (Projektleitung), DECOIT GmbH und datenschutz cert sowie die deutschen Forschungseinrichtungen Fraunhofer FOKUS, Hochschule Bremen und Universität Siegen beteiligt. Als assoziierte

Partner waren die Energieversorger Vattenfall und RWE sowie der Chiphersteller Maxim Integrated beteiligt. Daher gilt der Dank den Partnern des Projektes, die durch ihre Beiträge und Arbeiten die SMGW-Prototypen-Entwicklung erst ermöglicht haben. Seit dem Projektende im Mai 2015 arbeiten die industriellen Partner devolo AG und DECOIT GmbH an einem finalen SMGW-Produkt. Sie führen damit die Arbeiten des ehemaligen Konsortiums weiter.

Literatur

[BSI13a] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-1, Version 1.0. Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, 18.03.2013

[BSI13b] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-4, Version 1.0. Smart Metering PKI – Public Key Infrastruktur für Smart Meter Gateways, 18.03.2013

[BSI13c] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-3, Version 1.0. Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, 18.03.2013

[BSI15] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03116-3. Kryptographische Vorgaben für Projekte der Bundesregierung: Teil 3 – Intelligente Messsysteme, 26.03.2015

[Detk16] K.-O. Detken: Das SPIDER-Projekt – Sicherstellen der Geräteintegrität in Smart-Meter-Umgebungen. NET 04/16, 70. Jahrgang, ISSN 0947-4765, NET Verlagsservice GmbH, Woltersdorf 2016

[DGHS14] K.-O. Detken, C.-H. Genzel, O. Hoffmann, R. Sethmann: Absicherung von Smart-Meter-Umgebungen mit Trusted Computing. In P. Schartner, P. Lipp (Hrsg.) D.A.CH Security 2014: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, ISBN 978-3-00-046463-8, 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, Hochschule Bremen, Studiengang: Informatik – komplexe Softwaresysteme, Bremen im Mai 2015

[SPIDER16] SPIDER-Projektwebseite: http://www.spider-smartmetergateway.de