Forschungsbericht WS 2013/2014

Sicherheit im Smart Grid – Anforderungen an das Smart Metering Gateway

Prof. Dr.-Ing. Rainer Bermbach

Einleitung

Das intelligente Stromnetz, das *Smart Grid*, wird als eine der Voraussetzungen zur Erreichung der Energiewende gesehen. Innerhalb des Smart Grid spielt das *Smart Metering* eine große Rolle, der Einsatz von intelligenten Zählern für Strom, Gas, Wasser, Wärme etc. und ihre Anbindung an das Smart Grid über *Smart Metering Gateways* (SMGW). Durch das Smart Metering sollen der aktuelle Bedarf der Verbraucher sowie die aktuelle Leistung bei lokaler Energieerzeugung (Photovoltaik, Windenergie, kleine Blockheizkraftwerke …) zeitnah an die entsprechenden Steuerzentralen des Stromnetzes übermittelt werden. Den Verbrauchern sollen Verbrauchsdaten aufbereitet lokal oder indirekt über das Internet ebenfalls zeitnah zur Verfügung gestellt werden. Steuerbare Verbrauchsgeräte sollen in die Lage versetzt werden, auf Über- und Unterversorgung z.B. beim Strom reagieren zu können und dadurch Lastspitzen abbauen helfen.

In den Smart Metering Gateways, aber auch an anderen Stellen des Smart Grid, werden große Mengen verschiedenster Energiedaten erfasst, gespeichert und übertragen. Daraus ergibt sich ein außerordentlich hoher Schutzbedarf personenbezogener Daten. Aber auch in weiterer Hinsicht besteht großes Gefährdungspotenzial: Manipulation von Tarifinformationen oder Zählerständen, fehlerhafte bzw. manipulierte Identitätszuweisungen, Fehlsteuerungen des Stromflusses etc. Außerdem ist die Sicherstellung der Betriebssicherheit in einem kommunikationsmäßig vernetzten Stromnetz keine leichte Aufgabe (Hackerangriffe, Schadprogramme etc., vgl. Stuxnet). Erhöhte Notwendigkeit für entsprechende Schutzmaßnahmen besteht also in den drei Bereichen:

- *Security* – Schutz vor Angriffen auf die Infrastruktur
- *Safety* – Sicherstellung der Betriebssicherheit und
- *Privacy* – Datenschutz.

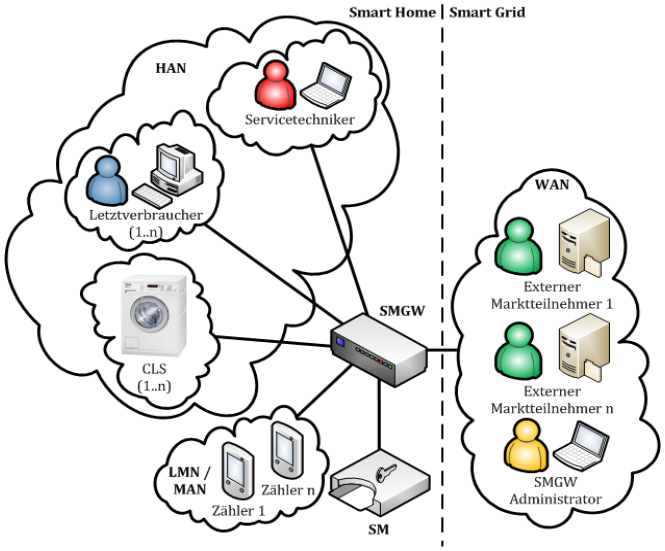

Abb. 1: Smart Metering Gateway und sein Umfeld

Die sog. Smart Metering Gateways (SMGW) bilden als Datenkonzentrator den Kommunikationsknotenpunkt eines lokalen Netzes von intelligenten Zählern und steuerbaren Geräten (s. Abb. 1, [6] nach [3]) und sichern Anschluss und Kommu-

nikation mit externen Stellen wie z.B. mit DSOs (Distribution System Operator) und TSOs (Transmission System Operator). Das SMGW hat zu diesem Zweck vier logische Kommunikationsbereiche: Im *LMN* (Local Metrological Network) befinden sich alle zu bedienenden Messstellen/Zähler. Zum *HAN* (Home Area Network) gehören zum einen alle steuerbaren Verbraucher (CLS – Controllable Local Systems, wie z. B. intelligente Hausgeräte, Photovoltaikanlagen, Klimaanlagen). Zum anderen befinden sich dort die Informationsschnittstelle für die Endverbraucher und der Servicezugang zum System. Über die Schnittstelle zum *WAN* (Wide Area Network) läuft die gesamte Kommunikation mit den externen Stellen wie Energielieferanten, Abrechnungsdienstleistern und dem Administrator des SMGW. Die vierte Schnittstelle bildet das Interface zum sog. Sicherheitsmodul (SM – Security Module), das u. a. kryptographische Aufgaben im Sicherheitskonzept übernimmt.

In seiner Eigenschaft als Kommunikationszentrale eines Smart Metering Systems benötigt das SMGW erhöhte Aufmerksamkeit bezüglich der Sicherheit des Systems. Die drei o. g. Aspekte müssen im Design der Hardware und Software des SMGW vertiefte Berücksichtigung finden. Aus diesem Grund hat sich das Bundesamt für Sicherheit in der Informationstechnik BSI im Auftrag des Bundeswirtschaftministeriums mit den Anforderungen an die Sicherheitsarchitektur von intelligenten Stromnetzen befasst, um sicherzustellen, dass von Anfang an Datenschutz und Datensicherheit gewährleistet werden. Eine Analyse der Bedrohungsszenarien lieferte die Grundlage für sog. Schutzprofile [1, 2], die alle SMGWs erfüllen müssen. Um auch Interoperabilität und die geeignete technische Umsetzung der Schutzprofile zu gewährleisten, entwickelte das BSI auch entsprechende Vorgaben in einer Technischen Richtlinie (BSI TR-03109, [3]). Nach entsprechenden vorläufigen Versionen und folgenden Anhörungen hat das BSI im März 2013 die Versionen 1.0 der Richtlinie [3] und des Schutzprofils (PP – Protection Profile [2]) des Sicherheitsmoduls und die Version 1.2 des Schutzprofils des SMGW [1] veröffentlicht. Das BSI macht dort u. a. sehr umfangreiche Vorgaben für die Sicherheit eines Smart Metering Systems. (Die eichrechtlichen Belange eines solchen Systems decken die Richtlinien PTB-A 50.7 und PTB-A 50.8 der Physikalisch-Technischen Bundesanstalt ab [4, 5].)

Während ein Projekt im Wintersemester 2012/2013 den Kommunikationsbedarf eines SMGW insbesondere in Hinblick auf die einzusetzenden Kommunikationsprotokolle prüfte, sollten im Rahmen dieses Projektes die vielfältigen Sicherheitsanforderungen an ein Smart Metering Gateway untersucht werden.

Schutzziele in Systemen der Informationstechnik

Die Gewährleistung von Datenschutz und Datensicherheit waren das erklärte Ziel der Aktivitäten des BSI. Generell werden als typische Schutzziele der Informationssicherheit die folgenden Aspekte genannt [7, 8]

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit

Aus diesen drei grundlegenden Schutzzielen können weitere Schutzziele abgeleitet werden.

4. Authentizität
5. Verbindlichkeit
6. Autorisation

Um diese Ziele zu erreichen, stützt sich das Bundesamt für Sicherheit in der Informationstechnik auf ihre IT-Grundschutzkataloge [9], die laut eigenen Aussagen als Standardwerk für IT-Grundschutz vielfältig angewendet werden. Das Dokument beinhaltet neben der Beschreibung der Bausteine der IT-Sicherheit sowie einem Maßnahmenkatalog auch einen Gefährdungskatalog, aus dem auch die für ein Smart-Metering-System relevanten Gefährdungen identifiziert werden können. In [6] wurden aus den aufgeführten

typischen Gefährdungen tatsächliche Gefahrensituationen abgeleitet. Als prinzipielle Lösungsmaßnahmen werden dort vorgeschlagen:

- Nachrichtenverschlüsselung
- Transportverschlüsselung
- Virtuelle private Netzwerke
- Speicherverschlüsselung
- Integritätsschutz
- Passwörter, PINs und TANs
- Rollen / Profile / Zugriffsverwaltung
- Transaktionslogs
- Zertifikate und Public-Key-Infrastruktur
- Firewall / Filterung des Datenverkehrs
- Firmware-Aktualisierungen
- Application Whitelists.

Fast alle dieser Maßnahmen finden sich auch in den Dokumenten des BSI zur Anwendung für ein Smart Metering Gateway. [6] ordnet auch die einzelnen Maßnahmen in der TR den o.g. Schutzzielen zu.

Gefährdungen und Gegenmaßnahmen in einem Smart-Metering-System

In Ergänzung der genannten Schutzziele, Gefährdungen und potentieller Gegenmaßnahmen im Allgemeinen geht das BSI beim SMGW noch einen Schritt weiter. Es definiert sogenannte Schutzprofile (Protection Profiles, PP) für das SMGW [1] und das dazugehörige Sicherheitsmodul (SM) [2], die formal nach Common Criteria abgeleitet sind.

Das Schutzprofil für das SMGW (Protection Profile for a Gateway of a Smart Metering System) nennt dort u. a. folgende grundsätzlichen Sicherheitsmaßnahmen zur Erzielung von Datenschutz und -sicherheit in einem Smart-Metering-System: Schutz der Authentizität, der Integrität und der Vertraulichkeit, Firewall-Funktionalität, Datenschutz (Privacy Preservation) und Verbindungsaufbau nur durch das SMGW (lediglich Wake-Up Call durch SMGW-Administrator erlaubt.

Zur Betrachtung der Gefährdungslage geht das Schutzprofil für das SMGW von zwei prinzipiellen Angriffsszenarien aus. Es spricht zum einen vom Local Attacker, der physischen Zugriff auf ein SMGW hat. Zum anderen kennt es den WAN Attacker, der versucht, über die WAN-Schnittstelle das SMGW oder seine Kommunikation zu kompromittieren.

Auch wenn der Local Attacker direkten Zugriff auf Zähler, Zähler-SMGW-Kommunikation und SMGW hat, sieht das Schutzprofil diesen Angreifer „weniger motiviert“, da er immer nur ein SMGW angreifen kann. Der WAN Attacker hingegen kann durch seinen Angriff potentiell eine große Zahl von Gateways unter seine Kontrolle bringen.

Das Protection Profile führt die folgenden Bedrohungen auf:

- Veränderung von Daten lokal (T.DataModificationLocal)
- Veränderung von Daten via WAN (T.DataModificationWAN)
- Veränderung der SMGW-Zeit (T.TimeModification)
- Offenlegung von Daten auf der Verbindung zwischen Zählern und SMGW (T.DisclosureLocal)
- Offenlegung von Daten auf der WAN-Kommunikationsstrecke (T.DisclosureWAN)
- Übernahme der Kontrolle von SMGW, Zählern oder CLS (T.Infrastructure)
- Zugriff auf gespeicherte Daten im SMGW (T.ResidentData)
- Zugriff auf nicht mehr benötigte Daten des SMGW (T.ResidualData)
- Verletzung der Vertraulichkeit von Daten (T.Privacy)

Das SMGW soll diesen Bedrohungen entgegenwirken u. a. durch die folgenden Maßnahmen:

- Einsatz eines zertifizierten Sicherheitsmoduls zur Verifikation und Generierung von digitalen Signaturen, zur Speicherung, Vereinbarung und Transport von Schlüsseln sowie zur Erzeugung von Zufallszahlen (für das Sicherheitsmodul existiert ein eigenes Schutzprofil)
- Einsatz verschiedener Log-Dateien (System-Log, Letztverbraucher-Log, Eichtechnisches Log) und Festlegung, wer wie darauf zugreifen darf
- Funktion des SMGW als Firewall an der WAN-Schnittstelle
- Getrennte physische Schnittstellen für WAN, HAN und LMN (und zum SM)
- Verschleierung der WAN-Kommunikation, um Rückschlüsse auf private Information zu verhindern
- Geschützte Kommunikation mit den angeschlossenen Zählereinheiten inklusive lokaler sicherer Speicherung und bedarfsweiser Pseudonymisierung von Daten
- Kryptographischer Schutz für alle Kommunikationsschnittstellen (Authentisierung, Integritätsschutz, Verschlüsselung)
- Verwendung von Time Stamps und gesicherter Update der internen Zeit von verlässlichen Quellen
- Weitere Maßnahmen wie Eigenschutz des SMGW, sichere Firmware Updates

In ähnlicher Weise geht das Schutzprofil für das Sicherheitsmodul (Protection Profile for Security Module of a Smart Meter Gateway) auf mögliche Bedrohungen und potentielle Gegenmaßnahmen ein. Aufgrund der ebenfalls umfangreichen Vorgaben soll hier auf eine detaillierte Darstellung verzichtet werden.

Maßnahmen zur Sicherung der Schnittstellen

Für die Interfaces des SMGW als die Standardangriffspunkte macht die TR-03109 teilweise sehr genaue Vorgaben (vgl. [12]). Abbildung 2 zeigt, wie das SMGW in seine Umgebung eingebettet ist und welche Schnittstellen vorhanden sind. Dabei sind die blau unterlegten Schichten in der Technischen Richtlinie verpflichtend vorgeschrieben. Die dunkelblau unterlegten Bereiche sind hierbei sicherheitsrelevant.

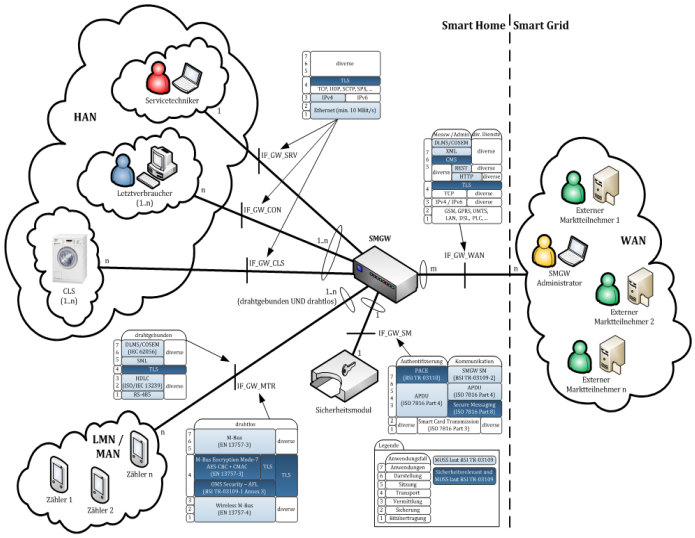

Abb. 2: Kommunikationsumgebung eines SMGW [6]

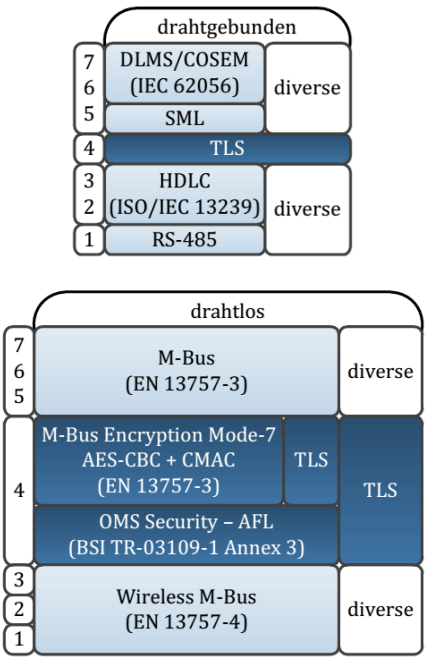

Abb. 3: Protokollstacks an der LMN-Schnittstelle eines SMGW ([6], nach [3])

Das Interface zum LMN bildet die Schnittstelle IF_GW_MTR. Hier kann die Datenübertragung entweder drahtgebunden (M-Bus) oder drahtlos (Wireless M-Bus) erfolgen. Die dafür vorgeschriebenen Protokollstacks zeigt Abb. 3.

Im Home Area Network verfügt ein SMGW über drei Schnittstellen: die IF_GW_CON für den Letztverbraucher, die IF_GW_SRV für den Servicetechniker sowie die IF_GW_CLS, die für den Anschluss sog. Controllable Local Systems (steuerbare Endgeräte) vorgesehen ist. Hier existieren vergleichsweise geringe Vorgaben für die Kommunikation, wie Abb. 4 zeigt.

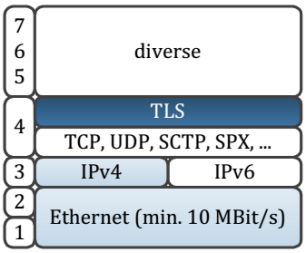

Abb. 4: Kommunikationsvorgaben für HAN-Schnittstellen ([6], nach [3])

Die für die Sicherheit wichtigste Schnittstelle nach außen ist das WAN-Interface IF_GW_WAN. Die dort zu verwendenden Protokolle sieht man in Abb. 5. Zusätzlich zur Verwendung von TLS (Transport Layer Security) für die Verschlüsselung auf der Transportschicht wie an den anderen Interfaces gibt es hier noch eine Inhaltsdatenverschlüsselung per CMS (Cryptographic Message Syntax).

Zum SMGW-internen Sicherheitsmodul (SM) sieht der Kommunikationsstack völlig anders aus (Abb. 6). Hier (IF_GW_SM) erfolgt die Kommunikation über sog. APDUs (Application Protocol Data Unit) nach ISO7816 und über das PACE-Protokoll bzw. Secure Messaging.

Bis auf die Verbindung zum Sicherheitsmodul ist die Transport Layer Security TLS ein wesentlicher Bestandteil der Sicherung der SMGW-Kommunikation. Auch wenn die Sicherheit der Daten und des Datenaustausch eines SMGW nur durch das Zusammenspiel sämtlicher Schutzmaßnahmen erzielt wird, konzentrierten sich die weiteren Untersuchungen aufgrund des nicht unerheblichen Umfangs neben der Anbindung und den Funktionen des Sicherheitsmoduls auf die Implementierung von TLS und der dazu nötigen Zertifikats- und Schlüsselverwaltung.

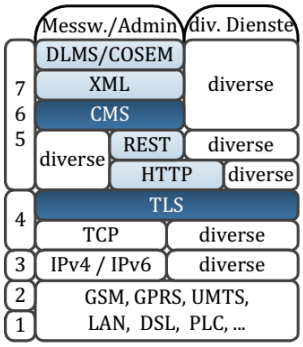

Abb. 5: Einzusetzende Protokolle der Schnittstelle IF_GW_WAN ([6], nach [3])

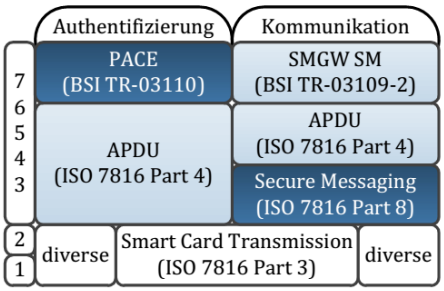

Abb. 6: Protokollvorgaben für die Schnittstelle zum Sicherheitsmodul ([6], nach [3])

Konzeptionelle Untersuchungen

Wesentlichen Anteil an der Sicherheit der Kommunikation des SMGW hat die Verwendung von TLS. Um die auf der Transportebene verschlüsselte und durch Signaturen integritätsgeschützte Kommunikation mit TLS zu realisieren, ist eine eigene PKI, eine Public-Key-Infrastruktur, notwendig, die die für TLS benötigten Zertifikate bereitstellt.

Die Anforderungen für die geforderte TLS 1.2 wurden im Rahmen des Projekts ausgiebig un-

tersucht. Da beim SMGW TLS durch ein Zusammenspiel von SM und SMGW realisiert wird, waren auch entsprechende Analysen der Funktionalität und der Sicherheitsfunktionen des SM nötig. Daraus ergaben sich konkrete Anforderungen an die logische Schnittstelle zwischen SMGW und SM, die eine definierte Softwareschnittstelle lieferten. Die folgenden Funktionen bilden das API zur Nutzung des (Hardware-) Sicherheitsmoduls (HSM) durch das SMGW:

- hsm_generate_random()
- hsm_verify_signature()
- hsm_generate_ecKeyPair()
- hsm_generate_presharedKey()
- hsm_generate_signature()

Die Speicherung von Zertifikaten im SM ist derzeit noch nicht implementiert, wohl aber Bestandteil der Forderungen der TR.

Die Technische Richtlinie schreibt für die Anwendung von TLS auch sehr genau vor, welche Cipher Suites und welche Elliptischen Kurven für die Kommunikation (im WAN) zu verwenden sind:

Tab. 1: Nach [10] zu nutzende Cipher Suites für TLS 1.2 in einer SMGW-Umgebung

Cipher Suite	Pflicht	Option
TLS_ECDHE_ECDSA_WITH_AES-_128_CBC_SHA256 (ID: 0xC023)	•	
TLS_ECDHE_ECDSA_WITH_AES-_256_CBC_SHA384 (ID: 0xC024)		•
TLS_ECDHE_ECDSA_WITH_AES_-128_GCM_SHA256 (ID: 0xC02B)		•
TLS_ECDHE_ECDSA_WITH_AES_-256_GCM_SHA384 (ID: 0xC02C)		•

Bei der Untersuchung des in der TR vorgesehenen TLS-Handshake fiel auf, dass im Gegensatz zum Standard auch eine sog. *CertificateVerify*-Nachricht vom Server zum Client vorgeschrieben ist. Eine Anfrage beim BSI ergab, dass es sich hier in der TR tatsächlich um einen Fehler handelt, der in der nächsten Version korrigiert sein wird.

Tab. 2: Nach [10] zu nutzende Elliptische Kurven für TLS 1.2 in einer SMGW-Umgebung

Elliptische Kurve	Pflicht	Option
NIST P-256 (OID: 1.2.840.10045.3.1.7)	•	
NIST P-384 (OID: 1.3.132.0.34)		•
BrainpoolP256r1 (OID: 1.3.36.3.3.2.8.1.1.7)		•
BrainpoolP384r1 (OID: 1.3.36.3.3.2.8.1.1.11)		•
BrainpoolP512r1 (OID: 1.3.36.3.3.2.8.1.1.13)		•

Weiterhin wurde untersucht, welche Anforderungen die Technische Richtlinie an die Zertifikate und ihre Handhabung stellt [3, 6]. Für jeden der Kommunikationsbereiche HAN, LMN und WAN existieren entsprechende Zertifikate der Kommunikationspartner. Da im HAN und LMN keine Inhaltsdatenverschlüsselung stattfindet, wird seitens des SMGW nur ein Zertifikat für die (beliebig) vielen Kommunikationspartner (sog. CLS, Letztverbraucher, Servicetechniker, Zähler) benötigt. Die Zertifikate aus HAN und LMN stammen nicht aus der SM-PKI. Für die TLS-Kommunikation im HAN und im LMN wird dasselbe Betriebsschlüsselpaar verwendet, welches auch innerhalb der TLS-Kommunikation im WAN Anwendung findet.

Im WAN muss es für jeden externen Marktteilnehmer (EMT) einen Datensatz geben, der aus den entsprechenden SM-PKI-Zertifikaten inkl. der zugehörigen öffentlichen Schlüssel des jeweiligen EMTs besteht. In ähnlicher Weise braucht man für den SMGW-Administrator einen Datensatz mit SM-PKI-Zertifikaten inkl. der öffentlichen Schlüssel. Das SMGW stellt seinerseits dem SMGW-Administrator und den EMTs seine SM-PKI-Zertifikate samt öffentlichen Betriebsschlüsseln zur Verfügung, um eine TLS-Verbindung zwischen ihm und dem Administrator bzw. EMT herstellen zu können.

Implementation exemplarischer Teile des Sicherheitskonzeptes

Basierend auf den konzeptionellen Untersuchungen entstanden auch Realisierungen von Sicherheitsfunktionen für ein SMGW. Um ein reales Sicherheitsmodul zu implementieren, ist spezielle Hardware in Form von Secure Cards, JavaCards o. ä. vonnöten. Dieser Aufwand war aus Zeit- und Kostengründen im Projekt nicht zu leisten. Dennoch konnte ein Konzept für ein SM entworfen und eine erste Implementierung durchgeführt werden. Die Kommunikationsanforderung unter Einsatz von PACE, Secure Messaging und sog. APDU wurden bereits oben erwähnt. Auf dieser Basis entstand eine Erstimplementierung der Schnittstelle IF_GW_SM. Durch die Definition der funktionalen Softwareschnittstelle zum SMGW (s. o.) in Kombination mit freien Softwarebibliotheken für PACE und Secure Messaging (OpenPACE, Crypto++) konnte eine eigene Library, die SmartMetering-Lib, geschaffen werden, die die geforderte Kommunikation zwischen SMGW und SM zur Verfügung stellt (s. Abb. 7, [11]).

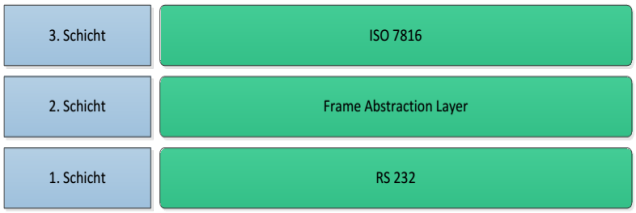

Abb. 7: Kommunikationsschichten der SmartMeteringLib

Wie Bild 7 schon andeutet, kommunizieren SMGW und SM der Einfachheit halber über RS232, da die TR hierfür keine verpflichtenden Vorgaben macht. Das ganze System wurde auf einem sog. ZED Board implementiert, einer Entwicklungshardware mit einem Xilinx FPGA, das neben programmierbarer Logik auch ein reichlich mit Schnittstellen ausgestattetes ARM-Prozessorsystem zur Verfügung stellt. Auf dieser Hardware läuft ein Embedded Linux-System, das zwei völlig getrennte Softwareprozesse beherbergt: den SMGW-Simulator und das implementierte Sicherheitsmodul (s. Abb. 8, [11]). Auf diese Weise können beide Funktionen unabhängig voneinander auf der gleichen Hardware laufen und kommunizieren. In einem weiteren Schritt könnten die derzeit noch in Software realisierten Ver- und Entschlüsselungsfunktionen in die programmierbare Logik ausgelagert werden.

Um die Überlegungen zur Zertifikatsverwaltung überprüfen zu können, entstand ein exemplarischer, manueller und skriptgesteuerter Aufbau einer Sicherheitsmodul-basierten Public-Key-Infrastruktur mit OpenSSL inklusive der Erstellung der Schlüssel und Zertifikate für die Root-CA, Sub-CAs, die Endnutzer sowie die Schlüssel und Zertifikate für HAN und LMN. Auch die Erstellung der Zertifikatsperrliste gehört zum Funktionsumfang.

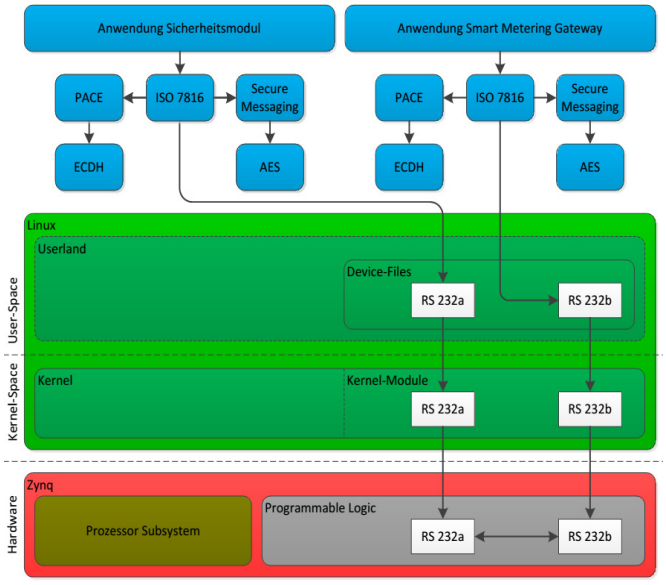

Abb. 8: Kommunikationsmodell zwischen Sicherheitsmodul und SMGW

Ein praktischer Test der Überlegungen erfolgte durch Programmierung eines Servers (SMGW-Administrator) und eines Clients (SMGW), die mittels der generierten PKI per TLS kommunizierten. Dabei kam die TLS-Bibliothek GnuTLS

zum Einsatz. Die Verwendung des o. g. Hardware-Sicherheitsmoduls konnte im Rahmen des Projekts noch nicht abgeschlossen werden. Die nötigen Umsetzungen der Bibliothek GnuTLS, um das dafür vorgesehene API per Callback-Funktionen nutzen zu können, sind aber bereits spezifiziert.

Ergebnisse

Das Projekt untersuchte die grundsätzliche Gefährdungssituation ebenso wie die umfangreichen, sicherheitsrelevanten Vorgaben des BSI für das Smart Metering Gateway und das Sicherheitsmodul. Generelle Schutzziele und Lösungsmaßnahmen wurden erarbeitet, die in den Schutzprofilen des BSI dargestellte Bedrohungslage und ihre Gegenmaßnahmen analysiert. Einen wesentlichen Teil des Schutzes bilden die Vorgaben zur geschützten Kommunikation auf den Schnittstellen des SMGW. Hier spielt die Transport Layer Security (TLS 1.2) eine wichtige Rolle, die für alle externen Interfaces vorgeschrieben ist. Für die besonders kritische WAN-Verbindung erfolgt zusätzlich eine Inhaltsdatenverschlüsselung per Cryptographic Message Syntax (CMS). Das Sicherheitsmodul des SMGW ist über eine eigene Schnittstelle verbunden, die über APDUs (ISO7816) und das PACE-Protokoll bzw. Secure Messaging kommuniziert.

Ein weiterer Aufgabenpunkt im Rahmen des Projekts entwickelte ein erstes Konzept zur Realisierung der geforderten Sicherheitsmechanismen. Dieses Konzept konzentrierte sich auf die auf der Transportebene verschlüsselte und durch Signaturen integritätsgeschützte Kommunikation mit TLS. Sie benötigt eine eigene PKI, die die für TLS benötigten Zertifikate bereitstellt. Das Zusammenspiel des SMGW mit dem SM lieferte die Definition einer Softwareschnittstelle zum Sicherheitsmodul. Die Technische Richtlinie macht auch für die zu verwendenden Cipher Suites und die zugehörigen Elliptischen Kurven sehr genaue Vorgaben. Das Konzept umfasst auch, welche Zertifikate und Schlüssel für welche Kommunikation notwendig sind. Ein Fehler in der Technischen Richtlinie konnte nach Rücksprache mit dem BSI geklärt werden.

Die Tragfähigkeit der Konzepte wurde mit der Implementation von exemplarischen Teilen überprüft. Ein erster Entwurf eines Sicherheitsmoduls auf einem Embedded System nutzt die entworfene Softwareschnittstelle und kommuniziert mit einem (Dummy-) SMGW. Um die Überlegungen zur Zertifikatsverwaltung überprüfen zu können, wurden ein Server (SMGW-Administrator) und ein Client (SMGW) programmiert, die die generierte PKI für ihre TLS-basierte Kommunikation einsetzen. Eine Umsetzung zur Verwendung des implementierten Hardware-SM ist vorbereitet.

Die recht umfangreichen Untersuchungen und Implementationen zeigen, dass die Realisierung der Sicherheitsfunktionalität eines Smart Metering Gateways sehr komplex ist und viel Aufwand erfordert. Derzeit wurde mit weiteren Untersuchungen und Arbeiten begonnen, die sich mit der Inhaltsdatenverschlüsselung per Cryptographic Messaging System (CMS) sowie mit der Nutzung von JavaCards für die Realisierung eines hardwarebasierten Sicherheitsmoduls beschäftigen.

Literatur

[1] BSI: *Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073)*. Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2013.

[2] BSI: *Schutzprofil für das Sicherheitsmodul eines Smart Meter Gateways (BSI-CC-PP-0077)*. Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2013.

[3] BSI: *Technische Richtlinie BSI TR-03109*. Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2013.

[4] PTB: *PTB-A 50.7 Anforderungen an elektronische und softwaregesteuerte Messge-*

räte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme. Physikalisch-Technische Bundesanstalt, Braunschweig, 2004.

[5] PTB: *PTB-A 50.8 Anforderungen Smart Meter Gateway*. Physikalisch-Technische Bundesanstalt, Braunschweig, 2013. (von der Vollversammlung für das Eichwesen verabschiedet, noch nicht veröffentlicht)

[6] Fricke, H.: *Entwurf eines Softwarekonzepts für die Sicherheitsarchitektur von Smart Meter Gateways nach BSI TR-03109*. Masterarbeit. Wolfenbüttel: Ostfalia Hochschule für angewandte Wissenschaften, 2013.

[7] Kappes, M.: *Netzwerk- und Datensicherheit – Eine praktische Einführung*. Wiesbaden: Teubner (jetzt Springer Vieweg), 2007.

[8] Appelrath, H.-J.; Beenken, P.; Bischofs, L.; Uslar, M. (Hrsg.): *IT-Architekturentwicklung im Smart Grid – Perspektiven für eine sichere markt- und standardbasierte Integration erneuerbarer Energien*. Berlin, Heidelberg: Springer, 2012.

[9] BSI: *IT-Grundschutz-Kataloge*. 13. Aufl. Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2013.

[10] BSI: *Technische Richtlinie BSI TR-03116-3. eCard-Projekte der Bundesregierung – Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen*. Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2013.

[11] Burghard, G.: *Entwicklung der kryptographischen Kommunikationsstrukturen zwischen Smart Metering Gateway und Sicherheitsmodul nach BSI TR-03109*. Bachelorarbeit. Wolfenbüttel: Ostfalia Hochschule für angewandte Wissenschaften, 2013.

[12] Bermbach, R.: *Kommunikation im Smart Grid – Kommunikationsbedarf eines MUC Controllers*. Forschungsbericht WS 2012/2013. Wolfenbüttel: Ostfalia Hochschule für angewandte Wissenschaften, 2013.

Kontaktdaten

Ostfalia Hochschule für angewandte Wissenschaften
Fakultät Elektrotechnik
Prof. Dr.-Ing. Rainer Bermbach
Salzdahlumer Straße 46/48
38302 Wolfenbüttel
Telefon: +49 (0)5331 939 42620
E-Mail: r.bermbach@ostfalia.de
Internet: www.ostfalia.de/pws/bermbach