Sichere Datenübertragung in Smart Grids mit Trusted Computing

Prof. Dr. Richard Sethmann[1],·Olav Hoffmann[1], Simon Busch[1]

[1]Institut für Informatik und Automation (IIA) der Hochschule Bremen,
Flughafenallee 10, 28199 Bremen
sethmann@hs-bremen.de, olavhoffmann@googlemail.com,
simonbusch@gravedo.de

Zusammenfassung

Die Energienetze der Zukunft stehen vor den Herausforderungen schwankende und dezentrale Energieerzeugung bei gleichzeitiger Wahrung der Netzstabilität zu ermöglichen. Um dies zu erreichen, ist eine sichere Datenübertragung zwischen dem Smart Meter Gateway (SMGW) und den unterschiedlichen Externen Marktteilnehmern (EMT) unumgänglich. Das vorgestellte Sicherheitskonzept für die sichere Datenübertragung in Smart Grids basiert auf dem Trusted Computing Ansatz. Zum einen wird als Vertrauensanker der Trusted Platform Module (TPM)-Chip im SMGW eingesetzt. Zum anderen wird über den Trusted Network Connect (TNC)-Ansatz dem SMGW Administrator (SMGW-Admin) der Zustand der Systemintegrität des SMGWs mitgeteilt (Remote Attestation). Die in den Technischen Richtlinien vom Bundesamt für Sicherheit in der Informationstechnik (BSI) beschriebenen Anforderungen wurden berücksichtigt. Das Sicherheitskonzept wurde gegen die in der Bedrohungsanalyse identifizierten Bedrohungen kritisch geprüft und stellt für die meisten Bedrohungen einen sehr guten Schutz dar. In einem Demonstrator konnte gezeigt werden, dass das Sicherheitskonzept praktisch umsetzbar ist und der Trusted Computing Ansatz mit den BSI-Richtlinien kompatibel ist.

1 Hintergrund

1.1 Energienetze der Zukunft

Zukünftige Energienetze stehen vor den Herausforderungen schwankende und dezentrale Energieerzeugung zu ermöglichen bei gleichzeitiger Wahrung der Netzstabilität. Weiterhin gilt es verschiedenste EMT zu berücksichtigen [Bund12b, Seite 14]: Den Messstellenbetreiber (MSB), der verantwortlich für das SMGW ist, den Messdienstleister (MDL), der das Ab- und Auslesen von Verbrauchszähleinrichtungen übernimmt, den Verteilnetzbetreiber (VNB), der das örtliche Stromnetz unterhält und wartet, den Lieferanten, der als Handelswarenvertreter auftritt und für die Nutzung des Netzes Gebühren an den VNB zahlt sowie den SMGW-Admin, der in viele wesentliche Prozesse des SMGW Lebenszyklus eingebunden ist (Messung, Datenübertragung, Administration und Eichung im laufenden Betrieb) [Bund12e, Seiten 17, 23, 32, 38].

1.2 Anforderungen an die sichere Datenübertragung

Diese neuen Anforderungen können nur durch die Koordination der Energieerzeugung und des Energieverbrauchs, sowie durch eine sichere Datenübertragung zwischen den Beteiligten erreicht werden. Neue Komponenten in intelligenten Energienetzen sind das Smart Meter

(SM) als „Intelligenter Zähler“ und das SMGW als zentrale Kommunikationseinheit. Das SMGW soll die sichere Datenübertragung zwischen dem Hausanschluss und den EMT ermöglichen. Weiterhin hat es die Funktion einer Firewall zwischen dem EMT, den Messgeräten (Strom-, Gas- und Wasserzähler) und den Energieerzeugern bzw. -verbrauchern innerhalb des Haushaltes des Endnutzers. Die sicherheitskritischen Funktionen, welche durch ein SMGW umgesetzt werden sollen, werden detailliert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschrieben. Basierend auf den Vorgaben des BSI wurde ein Systemkonzept mit einem umfangreichen Sicherheitskonzept erarbeitet. Das Ziel dabei war es, eine sichere Kommunikation zwischen dem Wide Area Network (WAN) und dem SMGW zu ermöglichen.

1.3 Eingesetzte Technologien

Als physischer Kommunikationskanal zwischen dem SMGW und dem WAN dienen dabei die bereits vorhandenen Energienetze, die mittels der Übertragungstechnik Powerline Communication (PLC) als Datenübertragungskanal verwendet werden. Die Kommunikation wird mit dem Transport Layer Security (TLS)-Protokoll gesichert. Zusätzlich zu den Richtlinien des BSI wurde der Trusted Computing (TC)-Ansatz verfolgt. Im Speziellen wurde der TNC-Ansatz zusammen mit dem TPM im Sicherheitskonzept berücksichtigt. Der TC-Ansatz wurde dazu verwendet, die Systemintegrität des SMGWs sicherzustellen. Für die Feststellung der Authentizität von Endnutzern wird auf die vom BSI spezifizierte Smart Metering - Public Key Infrastructure (SM-PKI) zurückgegriffen. Die Auswahl kryptographischer Verfahren wurde anhand der Technischen Richtlinien (TR) des BSI und gemäß den Anforderungen der TNC-Spezifikation getroffen.

Diese Ergebnisse wurden im Rahmen eines studentischen Masterprojektes [BBF+13] innerhalb eines Semesters erarbeitet. Neben den Anforderungen des BSI wurden teilweise auch Anforderungen durch das Unternehmen devolo AG gestellt, die im PLC-Markt stark vertreten sind. Ziel war es, unter Berücksichtigung der BSI-Richtlinien und des TC-Ansatzes, eine sichere und vertrauenswürdige Datenübertragung in Smart Grids zu erreichen.

2 Stand der Technik

Die TR des BSI haben zum Ziel, angemessene IT-Sicherheitsstandards zu verbreiten. Die Richtlinien haben originär nur Empfehlungscharakter. Durch §21e Abs. 2 Nr. 1 EnWG [EnWG05a] und §21i Abs. 1 Nr. 12 EnWG [EnWG05b] ist die Einhaltung der TR und Schutzprofile des BSI für Messsysteme zur Erfassung elektrischer Energie verpflichtend. In diesem Dokument sind größtenteils die Stände der Richtlinien bis Juni 2012 berücksichtigt. Aufgrund des Umfangs der Richtlinien wurde nur vereinzelt auf neuere Richtlinien zurückgegriffen, die im März 2013 veröffentlicht wurden. Abb. 1 zeigt die Dokumentenübersicht der berücksichtigten TR des BSI.

Das National Institute of Standards and Technology (NIST) befasst sich - neben dem BSI - ebenfalls intensiv mit der Entwicklung von Standards für die Informationssicherheit in Smart Grids. In [NIST10a] wird auf drei „Guidelines for Smart Grid Cyber Security“ hingewiesen: „Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements“, „Vol. 2, Privacy and the Smart Grid“ und „Vol. 3, Supportive Analyses and References“. Eine tiefere Analyse der NIST Publikationen sowie einem damit verbundenen Vergleich zu den Technischen Richtlinien des BSI wurden im Rahmen des Projektes nicht durchgeführt. Aus [NIST10b] in Kapitel 4 ergeben sich allerdings die Anforderungen an kryptografische Verfahren und die Verwaltung des Schlüsselmaterials [NIST10b, Seite 219 und 223]. Daraus geht hervor, dass die Anforderungen aus [NIST12] entsprechend umzusetzen sind. Kapitel 4 aus

[NIST12] gibt die explizit zu verwendenden kryptografischen Verfahren vor. Kapitel 10 aus [NIST12] liefert eine Spezifikation für die Schlüsselverwaltung im Smart Grid („Key Management System“). Verglichen mit den Anforderungen des BSI sind die Anforderungen des NIST deutlich breiter aufgestellt und beinhalten zumindest die Vorgaben des BSI [Bund12f].

Abb. 1: BSI TR-03109, Dokumentenübersicht der berücksichtigten TR des BSI [Bund12c]

Die IT-Systeme beim Endverbraucher befinden sich aus Sicht der Energieversorger in einer nicht vertrauenswürdigen Umgebung. Aus diesem Grund ist eine vertrauenswürdige Kommunikation zwischen dem Endverbraucher und dem Smart Grid notwendig. Z. B. muss bei der Übertragung der Verbrauchsdaten sichergestellt werden, dass die Daten nicht manipuliert wurden (Datenintegrität) und verschlüsselt übertragen werden.

Die Trusted Computing Group (TCG) entwickelte mit der TNC-Spezifikation einen Ansatz zur Realisierung vertrauenswürdiger Verbindungen z.B. über das Internet. Die TNC-Architektur ist die Entwicklung einer offenen und herstellerunabhängigen Spezifikation zur Überprüfung der Integrität von Endpunkten, die einen Verbindungsaufbau starten. Die TNC-Architektur bezieht dabei schon bestehende Sicherheitsaspekte, wie Virtual Private Network (VPN), IEEE 802.1x (802.1x), Extensible Authentication Protocol (EAP), TLS, Hyper Text Transfer Protocol Security (HTTPS) und Remote Authentication Dial In User Service (RADIUS) mit ein [DGBS08]. Im Rahmen des Projekts wurde auf die TLS-Technologie zurückgegriffen.

Als Besonderheit bietet TNC optionale Hardwareunterstützung mit dem TPM an, mit dem die Sicherheit von TNC erhöht werden kann. So macht das TPM es unter anderem möglich, dass eine Manipulation der Hard- oder Software festgestellt wird und nur signierte Software auf einem System ausgeführt werden kann. Das TPM (z.B. von Infineon) ist häufig serienmäßig in Notebooks eingebaut. Aktuell ist die TPM-Spezifikation der TCG in der Version 1.2 als ISO/IEC 11889 Parts 1-4 veröffentlicht. Es sei an dieser Stelle darauf hingewiesen, dass sich die Anforderungen des BSI auf die Kommunikation im Smart Grid bezieht. Das TPM wird als zusätzliche Komponente im Sicherheitskonzept gesehen und beschränkt sich auf die Messung der Systemintegrität des SMGWs. Diese Abgrenzung ist wichtig, da die TPM-Spezifikation in der Version 1.2 nicht den kryptografischen Anforderungen des BSI entspricht [Bund12f].

Die Architektur des TNC-Konzeptes wird von der TCG veröffentlicht und findet in der Spezifikation 1.5 (Revision 3) vom 7. Mai 2012 in diesem Projekt seine Anwendung [TCGr12a]. Wie in Abb. 2 zu sehen ist, besteht die verwendete TNC-Architektur aus der Einheit Access Requestor (AR) mit den Komponenten Integrity Measurement Collector (IMC), TNC-Client (TNCC) und Network Access Requestor (NAR) sowie der Einheit Policy Decision Point (PDP) mit den Komponenten Integrity Measurement Verifier (IMV), TNC-Server (TNCS) und Network Access Authority (NAA). Das Zusammenwirken der einzelnen Komponenten wird durch Interfaces (IF) realisiert. Weiterhin ist im AR das TPM als Vertrauensanker integriert. Der Zugriff auf das TPM wird über den TCG Software Stack (TSS) realisiert, der wie-

derum die bereitgestellten Dienste - über den Platform Trust Service (PTS) - dem TNCC und dem IMC zur Verfügung stellt.

Abb. 2: TNC-Architektur (In Anlehnung an [TCGr12a, Seite 30])

Mit Hilfe eines TPM kann eine Vertrauenskette (auch als Trust-Chain bezeichnet) für ein komplettes System geschaffen werden. In einer Vertrauenskette prüft grundsätzlich eine Komponente die jeweils nächste in der Kette und stellt somit sicher, dass diese nicht manipuliert wurde. Voraussetzung ist, dass die erste Komponente der Kette nicht manipulierbar sein darf, da diese nicht geprüft werden kann. Zudem muss das TPM ebenfalls gegen Manipulation gesichert sein. Die von einem Modul ermittelten Prüfwerte werden im TPM hinterlegt und sind zur Laufzeit nicht mehr veränderbar.

Mit der PLC wird eine weitere Technologie verwendet. PLC-Systeme nutzen als Medium zur Datenübertragung vorhandene Verteilungsnetze oder kundeneigene Niederspannungsinstallationen [VWEW01, Seite 7]. Konkret werden hierbei Daten über ein vorhandenes Stromnetz ausgetauscht. Im Falle des Projektes geschieht dies im Niederspannungsbereich eines Verteilungsnetzes, der sogenannten "Letzten Meile". Aus dem Blickwinkel der PLC sind hier zwei Systembereiche abzugrenzen. Zum einen gibt es den Bereich innerhalb eines Hauses, wo Geräte wie Waschmaschinen und Kühlschränke kommunizieren. Und zum anderen gibt es den Bereich außerhalb des Hauses, welcher am Haus beginnt und spätestens bei der PLC-Gegenstelle an einem Transformator-Haus endet. Auf dieser Strecke wird typischerweise eine Bandbreite von ca. 30 bis 60 kBit/s erreicht. Diese Feldmessungen wurden von der Firma devolo AG durchgeführt.

Abb. 3: Struktur eines TPM [Bund12a]

3 Bedrohungsanalyse und Szenariobeschreibung

Die Bedrohungen in dem betrachteten Szenario können in vier Kategorien eingeteilt werden: Schutz der Verbrauchsdaten des Endnutzers (Datenschutz), Manipulation des SMGWs mit dem Ziel Tarifprofile oder Verbrauchsdaten zum eigenen Vorteil zu verändern, Manipulation der Netzstatusdaten (Sabotage), die zur Laststeuerung des Energienetzes verwendet werden und eine Manipulation der steuerbaren Endgeräte beim Endverbraucher wie z.B. Blockheizkraftwerk bzw. Wäschetrockner.

Die Bedrohungen wurden durch den STRIDE-Ansatz [MSDN13] analysiert. In Tab. 1 sind die Bedrohungen mit den zugehörigen Sicherheitseigenschaften aufgeführt. Die Bedrohungen für das System sind unterschiedlicher Art: Ein möglicher Angreifer kann durch Vortäuschen einer falschen Identität Zugriff auf das SMGW erlangen (Spoofing), durch die Verfälschung von Daten andere Teilnehmer schaden (Tampering), durch das Leugnen von gewissen Aktivitäten sich einen Vorteil verschaffen (Repudiation), die Beeinflussung der Verfügbarkeit der im System vorhandenen Dienste herbeiführen (Denial of Service) oder durch die Ausnutzung einer Sicherheitslücke mehr Rechte erlangen als eigentlich für seine Rolle vorgesehen sind (Elevation of privilege).

Um grundlegende Anforderungen an den sicheren Betrieb von Standardsystemen im Szenario nicht erneut zu betrachten, wird davon ausgegangen, dass sowohl der SMGW-Admin und alle EMT ein Informationssicherheitsmanagement betreiben. Der entsprechende Standard ISO 27001 wird in der Regel zusammen mit einem weiteren Standard für Sicherheitsverfahren zur Umsetzung der Anforderungen verwendet, z.B. die IT-Grundschutzkataloge des BSI [Bund13]. Insgesamt wird angenommen, dass der SMGW-Admin und der EMT ihre Infrastrukturen konform zu ISO 27001 auf der Basis von IT-Grundschutz betreiben.

Im Zentrum der Betrachtung stehen das SMGW und die Kommunikation ins WAN über PLC. Abb. 4 zeigt eine Übersicht der einzelnen Aufgaben, die ein SMGW zu erfüllen hat und seine Kommunikationspartner. Das SMGW ist typischerweise beim Kunden (Letztverbraucher, Consumer) eingebaut und empfängt aus dem Local Metrological Network (LMN) Messwerte von den jeweiligen SM (z.B. Strom, Wasser, Gas SM). Diese Messwerte sollen über das WAN an die EMT gesendet werden, wie z.B. MSB und VNB. In dem Home Area Network (HAN) befinden sich die steuerbaren Endgeräte (z.B. Wäschetrockner) und dezentralen Energieerzeuger (z.B. Photovoltaikanlage), die über das SMGW vom VNB gesteuert werden sollen.

Jede Kommunikation zwischen Kunde und WAN wird von einem Router an den jeweiligen Kommunikationspartner weitergereicht. Der Router befindet sich in einer Netzstation (Trafostation, Ortsnetzstation), die für die Energieversorgung des Kunden zuständig ist. In der Kommunikation zwischen SMGW und dem WAN wird auf PLC zurückgegriffen. Dazu verfügt sowohl das SMGW als auch die Ortsnetzstation über ein PLC-Modem. Im Rahmen dieses Masterprojektes wurden Prototypen eines G3-Modems der Firma devolo AG verwendet. Mit diesen ist es möglich untereinander eine PLC basierte Verbindung aufzubauen und Daten mittels Transmission Control Protocol und Internet Protocol (TCP/IP) zu übertragen.

Abb. 4: Szenario: SMGW-Kommunikation über PLC ins WAN

4 Sicherheitskonzept

Die TR des BSI schreiben vor, dass das SMGW Verbindungsaufbauwünsche aus dem WAN ignoriert. Es kann aber selbst regelmäßig eine (TLS-)Verbindung zu seinem SMGW-Admin oder dem EMT aufbauen, um Befehle entgegenzunehmen. Alternativ kann das SMGW eine aufgebaute Verbindung für einen bestimmten Zeitraum bestehen lassen oder auch durch einen Wake-Up-Mechanismus zum Verbindungsaufbau aufgefordert werden [Bund12b, Seite 16f]. Dieser Wake-Up wird ausschließlich von Seiten des SMGW-Admins ausgelöst.

4.1 Ziel und Aufbau der Smart Metering - PKI

Das Ziel der Smart Metering - Public Key Infrastructure (SM-PKI) ist der Aufbau einer Vertrauenskette über das gesamte Smart Grid. Generell ist das Ziel hinter dem Aufbau einer solchen PKI die effizientere Verteilung und Prüfung von Zertifikaten. Mechanismen innerhalb von Institutionen und Geräten des Smart Grids und spezieller eines Smart Metering Systems sind in der Lage, die Korrektheit von Zertifikaten sicherzustellen und damit zu verifizieren, dass ein Kommunikationspartner von hoheitlicher Position aus berechtigt ist, einen Kommunikationsaufbau mit dem Ziel des Datentransportes oder Versendung von Anfragen durchzuführen. Weiterhin können beliebige versendete Daten über Zertifikate dieser PKI signiert werden,

um die Authentizität der Daten zu bescheinigen. So ist es möglich, Daten über mehrere Zwischenstellen weiterzuleiten und dennoch den Versender der Daten und damit die Daten selbst als vertrauenswürdig zu verifizieren. Auch die Sperrung einzelner Zertifikate, welchen vom hoheitlichen Vertrauensanker und dessen untergeordneten Stellen das Vertrauen nicht mehr zugesprochen werden, wird an zentraler Stelle publiziert, womit für alle Teilnehmer der PKI diese Zertifikate als ungültig und nicht mehr vertrauenswürdig erachtet werden. Somit kann Schaden durch Missbrauch verhindert werden. Ein weiteres Ziel des Einsatzes von Zertifikaten ist der Aufbau einer verschlüsselten, integritätsgesicherten Verbindung über einen TLS-Kanal. Es ist jedoch eine Herausforderung die Endnutzerzertifikate alle zwei Jahre zu erneuern [Bund12d, Seite 17].

Abb. 5 zeigt die Systemumgebung des Sicherheitskonzepts. Das Gehäuse des SMGWs wird sinnbildlich durch das oberste Symbol und die gestrichelte Linie dargestellt. Eine Firewall schützt das Gerät vor einem unerlaubten, äußeren Zugriff. Die Abbildung des TPMs repräsentiert den Vertrauensanker (für das clientseitige Kommunizieren mittels TNC). Das TPM ist eine Ergänzung zum Sicherheitsmodul. Eine Funktion des Sicherheitsmoduls ist das Aufbewahren von Zertifikaten, hier konkret den Endnutzerzertifikaten. Das eingesetzte Sicherheitsmodul muss dabei nach dem „Protection Profile for the Security Module of a Smart Metering System“ [Bund11] zertifiziert sein [Bund12d, Seite 24]. Der SMGW-Admin ist der zentrale Anlaufpunkt für jegliche Kommunikationspartner. Er beinhaltet z. B. auch den TNCS und ist somit für die Feststellung der Integrität des SMGWs zuständig. Anders als beim SMGW sind die Endnutzerzertifikate nicht in einem solchen Sicherheitsmodul aufzubewahren, sondern müssen nach entsprechenden Common Criteria Protection Profiles (PPs) durch das BSI zertifiziert sein [Bund12d, Seite 24].

Die Root-Certificate Authority (CA) bildet den Vertrauensanker der SM-PKI und kann von einer externen Einrichtung übernommen werden, die die vorgegebenen Mindestanforderungen aus [Bund12d] erfüllt. Die Aufgabe der Root-CA ist es, Zertifikate für Sub-CAs auszustellen und sie damit für das Ausstellen von Zertifikaten für Endnutzer zu autorisieren. Beide CAs sind verpflichtet alle ausgestellten Zertifikate in einer Datenbank vorzuhalten und entsprechende Informationen über den Verzeichnisdienst Lightweight Directory Access Protocol (LDAP) zu veröffentlichen. Sperrlisten können entweder via HTTP oder LDAP publiziert werden [Bund12d, Seite 19, 21]. Eine Sub-CA kann entweder unternehmensintern bei einem EMT oder unternehmensübergreifend unterhalten werden [Bund12d, Seite 10]. Im Falle des Projekts müssen alle Endnutzer, d. h. SMGW, SMGW-Admin und EMT über Endnutzerzertifikate verfügen, um u. a. miteinander über das TLS-Protokoll kommunizieren zu können.

Zusätzlich zur SM-PKI werden zwischen den SMGWs und dem SMGW-Admin die Aspekte der Hardware- und Netzsicherheit des TCs angewandt. Jedes SMGW tritt als AR mit TNC-Client auf und verfügt über ein TPM innerhalb des Sicherheitsmoduls, um die Integrität seiner Hard- und Software zu messen. Der SMGW-Admin übernimmt die Rolle des PDP mit TNCS und somit die Zugriffskontrolle für sämtliche ihm zugeteilten SMGWs. Detailliertere Ausführungen zur Anwendung des TCs folgen im nächsten Abschnitt.

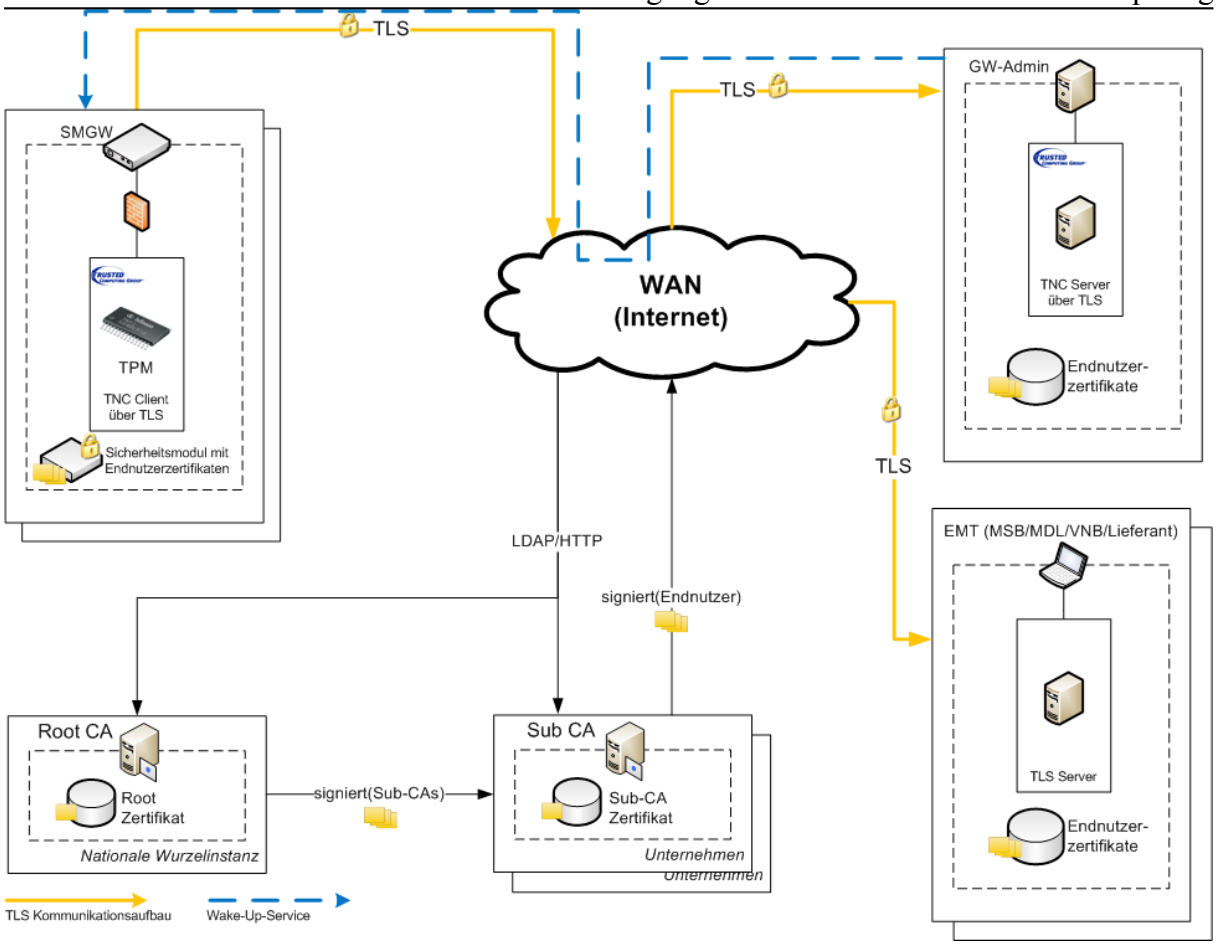

Abb. 5: Systemumgebung des Sicherheitskonzeptes

4.2 Anwendung des Trusted Computings

Abb. 6 zeigt das TNC-Schichtenmodell mit den relevanten Komponenten des Systemkonzepts. Die Rolle des ARs übernimmt das SMGW. Begründet ist dies dadurch, dass das Gerät permanent einem möglichen nicht autorisierten Zugriff unterliegt. Die abgeschirmte Umgebung eines Kellers (möglicher Einsatzort des SMGW) bietet alle Voraussetzungen, um in Ruhe Manipulationsversuche durchzuführen. Die Tatsache, dass zum aktuellen Zeitpunkt ein TPM, der Vertrauensanker, nur unter sehr hohem Aufwand manipuliert werden kann, prädestiniert die Anwendung des Konzeptes TNC. Auf der rechten Seite ist der PDP, der durch den SMGW-Admin ausgeübt wird, abgebildet. Dieser ist für die Prüfung der Integrität der Endgeräte, den SMGWs, zuständig. In einer geschützten Umgebung können hier alle Sicherungsmechanismen ablaufen. Die IMCs sammeln die Prüfwerte der relevanten Software Komponenten im SMGW. Die IMCs werden in TNC-Client-Server (TNCCS) Pakete verpackt und via TLS-Protokoll an den TNCS gesendet. Die empfangenen Prüfwerte werden mit Sollwerten, den IMVs, verglichen. Ebenfalls zu erwähnen ist die gesonderte Provisioning and Remediation (PaR)-Schicht. Diese ist als Isolationsschicht zu betrachten. Sollte eine Integritätsprüfung fehlschlagen, so kann ein möglicherweise kompromittiertes SMGW isoliert und gleichzeitig mit einer neuen Firm- oder Software versorgt werden.

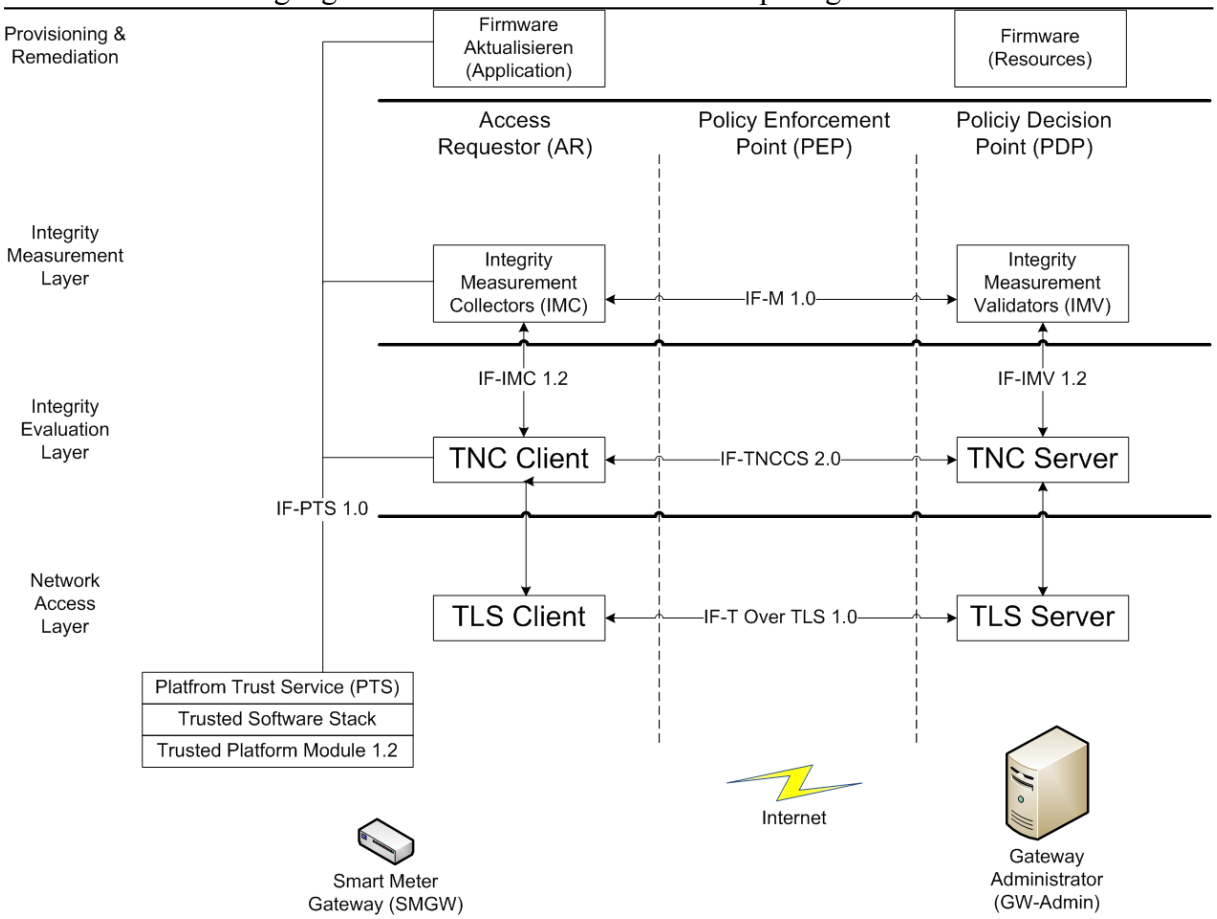

Abb. 6: TNC-Schichtenmodell mit relevanten Komponenten des Systemkonzepts (In Anlehnung an [TCGr12a, Seite 13], Abb. 2)

4.3 Abwehr der Bedrohungen

Durch das vorgestellte Sicherheitskonzept können die wesentlichen Bedrohungen abgewehrt werden. Tab. 1 zeigt die Bedrohungen mit den zugehörigen Sicherheitseigenschaften und die geeigneten Gegenmaßnahmen, die durch das Sicherheitskonzept realisiert werden.

Die Abwehr gegen Spoofing und Tampering lässt sich sehr gut durch den Einsatz des TPM-Chips, des TNC-Ansatzes und der TLS-Verschlüsselung erreichen. Hiermit ist sichergestellt, dass das SMGW nicht manipuliert wurde.

Die Repudiation bzw. Non-Repudiation lässt sich nur durch den Einsatz des TPM-Chips erreichen. Würde die Kommunikation nur über TLS verschlüsselt sein, dann könnte das SMGW manipuliert werden und somit das Schlüsselmaterial mit den Zertifikaten ausgetauscht werden. Die Abwehr gegen Information disclosure findet über die TLS-Verschlüsselung statt.

Ein Denial of Service Angriff kann von außen nur über ein Stören der PLC-Kommunikation oder über sehr häufiges Senden des Wake-Up-Signals erfolgen. Das Stören der PLC-Kommunikation kann nicht abgewehrt werden. Das häufige Senden des Wake-Up-Signals kann durch folgende Mechanismen abgemildert werden. Jedes Wake-Up-Signal ist mit der einzigartigen ID des SMGWs und einem aktuellen Zeitstempel (Timestamp) versehen (verhindert Replay-Attacken). Beide Daten werden mit dem privaten Schlüssel des SMGW-Admins signiert [Bund12b, Seite 34]. Weiterhin wird der Wake-Up-Service im SMGW mit geringen Ressourcen abgearbeitet.

Elevation of privilege bedeutet, dass Schwachstellen (Exploits) auf dem SMGW vorhanden sind. Diesem kann durch sichere Software-Entwicklung und Testen während des Entwicklungsprozesses entgegengewirkt werden. Falls doch eine Schwachstelle in der SMGW-Software enthalten sein sollte, dann kann diese Lücke über ein Firmware Update geschlossen werden.

Tab. 1: Bedrohungen, Sicherheitseigenschaften und Gegenmaßnahmen [MSDN13]

Bedrohung	Sicherheitseigenschaft	Gegenmaßnahme
Spoofing (Vortäuschung)	Authentifizierung	TPM-Chip, TNC-Kommunikation und TLS mit clientseitiger Authentifizierung
Tampering (Verfälschung)	Integrität	TPM-Chip und TNC-Kommunikation
Repudiation (Ablehnung)	Annahme/Akzeptanz von Daten	TPM-Chip
Information disclosure (Informationsenthüllung)	Vertraulichkeit	TLS-Verschlüsselung
Denial of service (Dos) (Dienstverweigerung) • DoS PLC-Verbindung • DoS Wake-Up-Signal	Verfügbarkeit	• Für einen DoS der PLC-Verbind. gibt es keine Gegenmaßnahme • Timestamp und geringe Priorisierung der Wake-Up-Signal-Verarbeitung auf dem SMGW
Elevation of privilege (Erlangung von Berechtigungen)	Autorisierung	Sichere Software-Entwicklung und Firmware Updates

5 Umsetzung im Demonstrator

Das vorgestellte Sicherheitskonzept wird über die Umsetzung in einem Demonstrator validiert. Der Demonstrator verwendet dabei folgende Basistechnologien des Systemkonzepts: PLC, TLS, TNC und TPM.

In der Topologie des Demonstrators in Abb. 7 werden ein SMGW, ein EMT und ein SMGW-Admin über die PLC-Technologie verbunden. Das SMGW generiert Messwerte, wie sie von einem realen SM geliefert würden und soll diese an den EMT übertragen. Damit der EMT sicherstellen kann, dass das SMGW nicht kompromittiert wurde, baut das SMGW eine Vertrauenskette auf und verwendet die daraufhin im TPM (integriert in einem Notebook) gespeicherten Werte, um sich per TNC beim SMGW-Admin anzumelden. Wurde das SMGW manipuliert wird dies durch den SMGW-Admin festgestellt. Alle Daten werden im Demonstrator verschlüsselt übertragen. Die Darstellung der Verbindungsdetails und Daten erfolgt über eine grafische Oberfläche, welche die ablaufenden Prozesse zur besseren Nachvollziehbarkeit verlangsamt darstellt.

Der SMGW-Admin übernimmt im Demonstrator die Rolle des TNCS und überprüft das angeschlossene SMGW auf seine Unversehrtheit. Der EMT empfängt die Messwerte vom SMGW und stellt diese dar. Zusätzlich kann der EMT eine Verbindung zum SMGW-Admin aufbauen, um dort anzufragen, ob das SMGW unversehrt ist.

Abb. 7: Topologie des Demonstrators

6 Fazit

Es wurde auf Basis der BSI-Richtlinien und des TCs ein umfassendes System- und Sicherheitskonzept für die Kommunikation in Smart Grids vorgestellt. Die strengen Vorgaben des BSI wurden in dem Sicherheitskonzept eingehalten. Hinzu kommt, dass der Ansatz des TCs erfolgreich mit den gestellten BSI-Anforderungen in Einklang gebracht werden konnte. Eine besonders positive Bewertung gilt der Tatsache, dass durch die Erweiterung mittels TNC die Sicherheit erheblich verbessert werden konnte. Der Fokus des BSIs liegt stets auf der Kommunikationssicherung und des Datenschutzes. TNC nutzt als Vertrauensanker das TPM, daher kann so auch die Integrität der Hard- und Software eines entfernten Gerätes, in diesem Fall die des SMGWs, geprüft werden (Remote Attestation). Ein wertvoller Vorteil, da stets ein physischer Zugriff durch Hausbesitzer und Mieter am SMGW möglich ist. Durch die Anforderungen des BSIs wird das SMGW sehr komplex. Insbesondere der kurze Lebenszyklus der Endnutzerzertifikate von zwei Jahren stellt eine Herausforderung für den praktischen Einsatz der SM-PKI dar. Die Machbarkeit dieses Sicherheitskonzeptes konnte schließlich im Demonstrator gezeigt werden.

Literatur

[BBF+13] C. Becker, S. Busch, H. Fellmann, K.-W. Heinrich, O. Hoffmann, J. Kahrs, N. Nesemann, J. Schröder, M. Schwitalla und S. Wend: Projektdokumentation des Masterprojektes - Sichere Datenübertragung in Energienetzen, Bremen 2013.

[Bund11] Bundesamt für Sicherheit in der Informationstechnik. Protection Profile for the Security Module of a Smart Metering System, 2011. Version 0.8.3

[Bund12a] Bundesamt für Sicherheit in der Informationstechnik. Das Trusted Platform Module (TPM). https://www.bsi.bund.de/DE/Themen/weitereThemen/SicherePlattformen/TrustedCompting/TrustedPlatformModuleTPM/TrustedPlatformModuleTPM/aufbaustruktur.html, zuletzt aufgerufen am 19.6.13

[Bund12b] Bundesamt für Sicherheit in der Informationstechnik. TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Mai 2012. Version 0.50

[Bund12c] Bundesamt für Sicherheit in der Informationstechnik. TR-03109 Smart Energy, Mai 2012. Version 0.50

[Bund12d] Bundesamt für Sicherheit in der Informationstechnik. TR-03109-4 Public Key Infrastruktur für Smart Meter Gateways, Mai 2012. Version 0.50

[Bund12e] Bundesamt für Sicherheit in der Informationstechnik. TR-03109-1 Anhang: Betriebsprozesse, Mai 2012. Version 0.50

[Bund12f] Bundesamt für Sicherheit in der Informationstechnik. TR- 03116-3 Kryptographische Vorgaben für die Infrastruktur von Messsystemen, 2012. Draft 20120525

[Bund13] Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html, zuletzt aufgerufen am 19.6.13

[DGBS08] K. O. Detken, S. Gitz, S. Bartsch, R. Sethmann: Trusted Network Connect – sicherer Zugang ins Unternehmensnetz. D•A•CH Security 2008, 24. und 25. Juni 2008, Technische Universität Berlin, Germany

[EnWG05a] § 21e EnWG - Allgemeine Anforderungen an Messsysteme zur Erfassung elektrischer Energie. http://www.gesetze-im-internet.de/enwg_2005/__21e.html, zuletzt aufgerufen am 19.6.13

[EnWG05b] § 21i EnWG - Rechtsverordnungen. http://www.gesetze-im-internet.de/enwg_2005/__21i.html, zuletzt aufgerufen am 19.6.13

[MSDN13] Microsoft. Threat Modeling Uncover Security Design Flaws Using The STRIDE Approach. http://msdn.microsoft.com/en-us/magazine/cc163519.aspx, Jan. 2013, zuletzt aufgerufen am 19.6.13

[NIST10a] National Institute of Standards and Technology. Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, 2010.

[NIST10b] National Institute of Standards and Technology. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, 2010.

[NIST12] National Institute of Standards and Technology. NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revision 3), 2012.

[TCGr12a] Trusted Computing Group. TCG Trusted Network Connect TNC Architecture for Interoperability, 2012. Revision 3

[VWEW01] VWEW Energieverlag GmbH. Powerline Communication (PLC): Telekommunikation über 50-Hz-Netze. VWEW Energieverlag GmbH, 1 Edition, 2001