Absicherung von Smart-Meter-Umgebungen mit Trusted Computing

Prof. Dr. Kai-Oliver Detken[1] · Carl-Heinz Genzel[2]· Olav Hoffmann[2]· Prof. Dr. Richard Sethmann[2]

[1]DECOIT GmbH, Fahrenheitstr. 9, D-28359 Bremen
detken@decoit.de

[2]Hochschule Bremen, Flughafenallee 10, D-28199 Bremen
carl-heinz.genzel/olav.hoffmann/sethmann@hs-bremen.de

Zusammenfassung

Die sichere Datenübertragung zwischen den Steuerkomponenten zukünftiger, intelligenter Energienetze ist zwingend notwendig, um die Anforderungen an die Stabilität und Sicherheit erfüllen zu können. Hierfür wurden Sicherheitsvorgaben von dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bezug auf eine zentrale Kommunikationseinheit zur Sicherung intelligenter Energienetze, das sog. Smart Meter Gateway (SMGW), entwickelt. Das SPIDER-Projekt des BMWi berücksichtigt diese Vorgaben bei der Entwicklung ihres SMGW und erhöht den Integritätsschutz, indem es Elemente aus dem Ansatz Trusted Computing (TC) von der Trusted Computing Group (TCG) integriert. Aufbauend auf Trusted Boot wird ein Secure-Boot-Verfahren angewendet und eine laufende Integritätsmessung über die Trusted Network Connect (TNC) Architektur realisiert. Dadurch ist die Integrität einer SMGW-Komponente aus der Ferne erkenn- und kontrollierbar, wodurch man sich nicht auf eine Verplombung des Gehäuses verlassen muss. Dieser Ansatz geht damit einen Schritt weiter, als die bisherige BSI-Spezifikationen es vorsehen.

1 Einleitung

Die steigende Einbindung schwankender und dezentraler Energieerzeuger bei gleichzeitiger Wahrung der Netzstabilität erfordert die Etablierung intelligent steuerbarerer Energienetze. Weiterhin gilt es, verschiedene Externe Marktteilnehmern (EMT) mit ihren Interessen im Energienetz zu berücksichtigen [Bu13f]:

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 deshalb maßgebend von einer sicheren Datenübertragung zwischen den o.g. Teilnehmern sowie den eingesetzten Steuerkomponenten ab. Das Bundesamt für Informationssicherheit (BSI) hat in diesem Umfeld eine Architektur definiert, die neben den eigentlichen intelligenten Messsystemen eine lokale Kommunikationseinheit, das sog. Smart Meter Gateway (SMGW), zum Schutz dieser Messsysteme und deren Messdaten vorsieht.

Aufbauend auf diesen Vorgaben, wurden im Rahmen des BMWi-Forschungsprojektes „**S**ichere **P**owerl**i**ne-**D**atenkommunikation im intelligenten **E**ne**r**gienetz“ (SPIDER) Trusted-Computing-Lösungen diskutiert, die den Sicherheitsgrad einer SMGW-Umgebung weiter erhöhen sollen [Sp14]. Ziel ist es, das zentrale SMGW mit einer zusätzlichen Integritätsmessung auszustatten, um Manipulationen jeglicher Art erkennen zu können. Dies wird immer wichtiger, wenn man bedenkt, dass die gesammelten Daten über das Internet gesichert abgefragt werden sollen und dabei die Fälschungssicherheit gewährleistet sein muss.

Aus diesem Grund wurden im Konsortium der Einsatz eines Trusted Platform Modules (TPM) und die Umsetzung von Trusted Network Connect (TNC) der Trusted Computing Group (TCG) zur sicheren Kommunikation zwischen SMGW und Gateway Administrator (GWA) diskutiert. Außerdem wurde die Implementierung eines vertrauenswürdigen Bootverfahrens betrachtet. [GSHD14]

2 Smart-Meter-Szenario

Die neuen Anforderungen an Energienetze können nur durch die Koordination der Energieerzeugung und des Energieverbrauchs, in Verbindung mit einer sicheren Datenübertragung zwischen den Beteiligten, erreicht werden. In diesem Zusammenhang werden gemäß BSI zwei neue Komponenten in intelligenten Energienetzen benötigt, das Smart Meter (SM) als „intelligenter Zähler“ und das SMGW als zentrale abgesicherte Kommunikationseinheit. Sie bilden zusammen die Basis des Smart-Metering-Systems.

Die dargestellten Komponenten und Bereiche in Abbildung 1 sowie die entsprechenden Sicherheitsanforderungen in einem Smart-Metering-System werden durch Vorgaben des BSIs im Detail beschrieben (vgl. [Bu13a], [Bu13b], [Bu13d], [Bu13e]).

Das SMGW ist die zentrale Instanz in einem Smart-Metering-System. 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 gem. den Vorgaben des BSI (vgl. [Bu13a]) um folgende Netzbereiche:

1. **Local Metrological Network (LMN):** ein Netz zur lokalen Anbindung von Messgeräten (Strom-, Gas- oder Wasserzähler) der Endnutzer (Letztverbraucher, LV).
2. **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).

3. **Wide Area Network (WAN)**: ein Netz zur Anbindung des GWA für die SMGW-Verwaltung und autorisierter Dritter (EMT) zur Datenvermittlung.

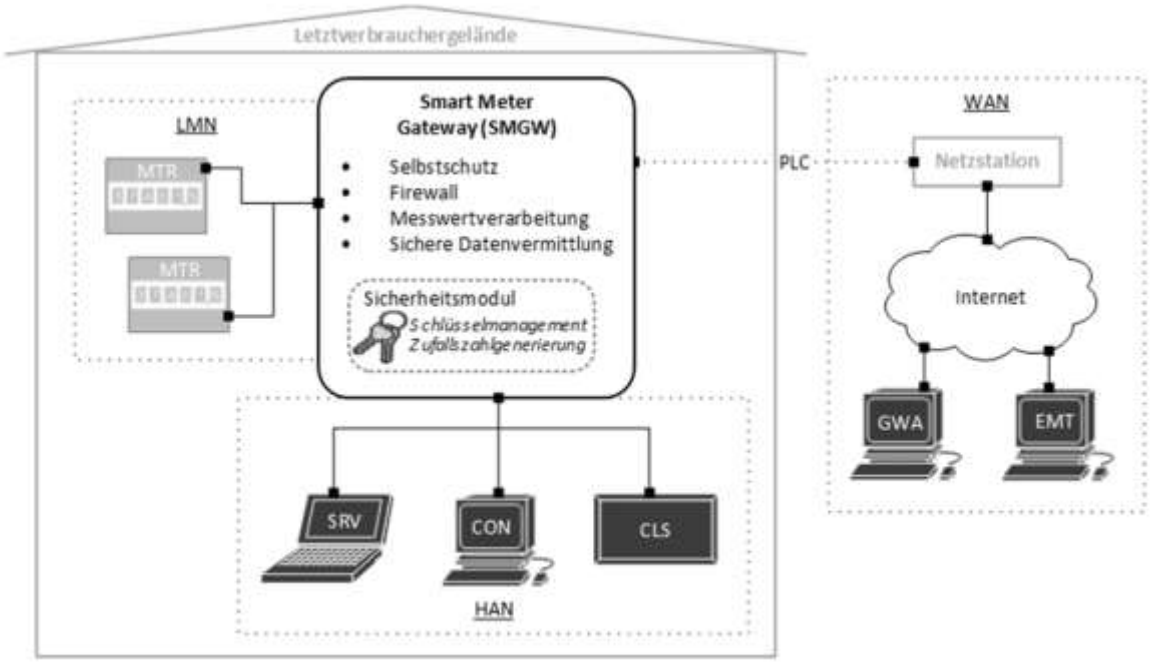

Abb. 1: SMGW und benachbarte Netze mit Teilnehmern

Das SMGW erfüllt außerdem die Funktion einer Firewall zur Separierung dieser Netze und deren Teilnehmer. Neben dieser logischen Trennung sind die Schnittstellen im SMGW zusätzlich physisch voneinander getrennt. [Bu13a]

Ein Security-Modul innerhalb des SMGWs stellt kryptographische Operationen für die sichere Speicherung und Übertragung von Daten zur Verfügung. Zu den Funktionen zählen unter anderem [Bu13b]:

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

Das SMGW empfängt über das angeschlossene LMN Messwerte von Smart Metern. Smart Meter unterscheiden sich von regulären Messsystemen insbesondere dadurch, dass sie eine kryptographisch gesicherte Kommunikation zum SMGW verwenden und die Übermittlung von Messwerten durch das SMGW steuerbar ist. [Bu13a]

Um eine möglichst einfache Integration des Smart-Meter-Systems zu ermöglichen, werden zusätzliche Komponenten zur Anbindung des SMGWs an das Weitverkehrsnetz verwendet. Jedes SMGW kommuniziert mit Hilfe der G3-Power-Line-Communication (PLC) Technologie über die „Letzte Meile“ des lokalen Stromnetzes mit der nächsten Netzstation. Erst in der Netzstation wird die Kommunikation in ein vorhandenes Weitverkehrsnetz eingeleitet. [SHB13]

Welche Daten in das Weitverkehrsnetz kommuniziert werden dürfen, ist ebenfalls durch das BSI in den entsprechenden Richtlinien geregelt. In diesem Zusammenhang definiert das BSI Eigentumsverhältnisse in Bezug auf die einzelnen Rollen. Der Letztverbraucher, als natürliche oder juristische Person, ist Eigentümer der Messwerte und davon abgeleiteter Daten seiner Messsysteme. Ein EMT ist Interessent und Nutzer dieser Daten, sie ermöglichen ihm die Durchführung der Bilanzierung, Tarifierung und Netzzustandserfassung. Der GWA hat im Allgemeinen keinen Zugriff auf diese Form der Daten. Er hat im Gegenzug Zugriff auf systemrelevante Daten wie Konfigurationsdaten, System- und Eichtechnische-Logs. Der Service-Techniker hat eine Diagnosefunktion und darf daher systemrelevante Daten auslesen, sie aber im Gegensatz zum GWA nicht speichern. Der Zugriff auf das SMGW ist jedem Teilnehmer nur über das ihm zugeordnete Netz (siehe Abbildung 1) gestattet [Bu13a]. [GSHD14]

3 Bewertung geeigneter Schutzverfahren

Um die Integrität der SMGW-Komponente zu erhöhen, wurde von Anfang an über den Einsatz von Trusted Computing nachgedacht. Dabei wurde als erstes das Verfahren selbst untersucht und die Einsatzmöglichkeiten mit den BSI-Spezifikationen verglichen, um ein eigenes Sicherheitskonzept zu definieren und abschließend ein Secure-Boot-Verfahren umzusetzen.

3.1 Trusted Computing (TC)

Trusted Computing (TC) ist eine Technik, die von der Trusted Computing Group (TCG) spezifiziert wurde und die Kontrolle von Hard- und Softwarekomponenten ermöglicht. Die TCG ist eine von der Industrie betriebene Standardisierungsorganisation, die Spezifikationen für TC-Techniken entwickelt. Ziel der TCG ist es, einen offenen, herstellerunabhängigen Standard für TC-Bausteine und Software-Schnittstellen zu spezifizieren. Der Begriff „Trust“ wird dabei so definiert, dass es bestimmte Erwartungen an ein Gerät oder eine Software gibt, die sich für einen bestimmten Zweck nach einer vordefinierten Art und Weise verhalten. Durch die Offenheit der Standards und eine breite Unterstützung wichtiger Hersteller für IT-Sicherheitsprodukte wurde TC in SPIDER zur weiteren Untersuchung ausgewählt. [TCG14]

Mit Hilfe von TC kann bei Rechnersystemplattformen wirkungsvoll nachgewiesen werden, dass die Basis eines Gerätes noch nicht kompromittiert worden ist. Das bedeutet, Veränderungen an der IT-Plattform können erkannt werden. Hierdurch lassen sich unter anderem externe Software-Angriffe, als auch Veränderungen der Konfiguration, Sicherheitslücken oder schadhafte Anwendungsprogramme ausmachen. TC wurde inzwischen zum Teil durch die IETF in Form von RFCs standardisiert. Die folgenden Beschreibungen beziehen sich, wie die RFCs, auf die Definitionen der TCG.

Die Spezifikationen der TCG können in verschiedene Arbeitsgruppen unterteilt werden. Ein Schwerpunkt ist sicherlich das Trusted Platform Module (TPM), inkl. der Sicherheitselemente, wie dem Core-Root-of-Trust-for-Measurement (CRTM), dem TPM Software Stack (TSS) und dem Trusted Boot (vgl. [Detk12]). Diese Sicherheitselemente sind in der Trusted Network Connect (TNC) Architektur wiederzufinden (vgl. [DDN10]), die eine Erweiterung der bisherigen Sicherheitsprotokolle darstellt, da sie zusätzlich Informationen über die eingesetzten Policys und Plattform-Zustände bereithält. TNC definiert außerdem ein Konzept von Metadata Access Points (MAP), bei dem erweiterte Monitoring-Mechanismen zum Einsatz kommen, damit eine kontinuierliche Überwachung von Infrastrukturen in Echtzeit ermöglicht werden

kann (vgl. [DSBW12]). Weitere Gruppen beschäftigen sich mit PC-Clients, Infrastruktur und Server-Systemen. Best-Practice-Angaben werden zudem regelmäßig definiert [TCG12].

3.2 STRIDE-Ansatz

Im Rahmen des Forschungsprojektes SPIDER wurden die Bedrohungen durch den STRIDE-Ansatz analysiert (vgl. [SHB13]). STRIDE steht für **S**(poofing), **T**(ampering), **R**(epudiation), **I**(nformation disclosure), **D**(enial of service) und **E**(levation of privilege) und ermöglicht die Identifizierung von gefährdeten Sicherheitseigenschaften durch die Zuordnung erkannter Bedrohungen. Aufbauend auf diese Bedrohungsanalyse wurden Gegenmaßnahmen aus den TC-Standards und den BSI Vorgaben bezogen auf die genannten Sicherheitseigenschaften in Tabelle 1 gegenübergestellt.

Tab. 1: Bedrohungen und Sicherheitseigenschaften

Bedrohung	Sicherheits-eigenschaft	Trusted Computing	BSI
Spoofing (Täuschung)	Authentifizie-rung	TPM (Identität), TNC (Au-thentifizierung)	Security-Modul (Identi-tät, Authentifizierung)
Tampering (Datenmanipulation)	Integrität	TPM (Identität, Signatur), TNC (sichere Kommunikati-on, Integritätskontrolle)	Security-Modul (Identi-tät, Signatur), SMGW (Verschlüsselung, Selbst-tests)
Repudiation (Nichtanerkennung)	Nichtabstreit-barkeit	TPM (Identität, Signatur), TNC (Sichere Kommunika-tion)	Security-Modul (Identi-tät, Signatur), SMGW (Daten- und Transport-verschlüsselung)
Information Disclosure (Informationsenthüllung)	Vertraulichkeit	TPM (Datenverschlüsse-lung), TNC (Sichere Kom-munikation)	SMGW (Daten- und Transportverschlüsse-lung)
Denial of Service (Dienstverweigerung)	Verfügbarkeit	keine Angaben	SMGW (priorisierte Bu-siness Logik)
Elevation of Privilege (Rechteerweiterungen)	Autorisierung	TPM (eingeschränkter Be-fehlssatz), TNC (Rechtepro-file)	Security-Modul (einge-schränkter Befehlssatz), SMGW (Rollen-basierte Rechte)

Dabei wird deutlich, dass sich eine Härtung gegen Spoofing und Tampering durch beide Konzepte mit Hilfe von Verschlüsselung und Signaturen erreichen lässt. Zeitstempel können zudem eingesetzt werden. Zusätzlich bieten beide Standards die Möglichkeit den Systemzustand zu evaluieren, zum einen mit sog. Selbsttest und zum anderen mit Hilfe einer sog. Integritätskontrolle.

Die Repudiation bzw. Non-repudiation ist durch fest verankerte Identitäten in den, durch die Standards spezifizierten, Modulen erreichbar. Der Schutz vor „Information Disclosure“ wird mit Hilfe der TLS-Transportverschlüsselung und ergänzender Datenverschlüsselung realisiert. Für die Abwehr von Denial-of-Service-Angriffen spielen sowohl das Security-Modul, als auch

TPM oder TNC, keine besondere Rolle. An dieser Stelle müssen andere Maßnahmen getroffen werden, wie z. B. die durch das BSI geforderte niedrige Priorisierung des Wake-Up Service an der WAN-Schnittstelle durch das SMGW (vgl. [Bu13a]).

Elevation-of-Privilege, unter anderem durch vorhandene Schwachstellen (Exploits) auf dem SMGW, werden durch eingeschränkte Befehlssätze und rollen- oder profil-basierte Rechte in beiden Standards erschwert. An dieser Stelle sind allerdings vor allem Methoden zur Entwicklung hochwertiger, sicherer Software elementar.

Durch die jeweiligen Konzepte können die STRIDE-Bedrohungen im Wesentlichen verringert werden. Der Unterschied der Ansätze liegt dabei vor allem in der Verteilung der Funktionen auf beteiligte Systemkomponenten. Außerdem ist der Schutz vor Denial-of-Service Angriffen mit Trusted Computing allein nicht umsetzbar. Losgelöst von der allgemeinen Betrachtung funktionaler Gegenmaßnahmen beider Konzepte nach STRIDE, zeigt eine genauere Betrachtung einzelner technischer Komponenten hingegen deutlicher Unterschiede.

Neben der logischen Zugriffskontrolle ist ein TPM auch physikalisch so derart im System zu integrieren, dass es nicht einfach entfernt werden kann [TCG07]. Das BSI schreibt eine solche Integration für das Security-Modul im entsprechenden Protection Profile (PP) nicht direkt vor. Es geht jedoch davon aus, dass das Security-Modul innerhalb des SMGW liegt und denselben physischen Schutz durch die Gateway-Umgebung erhält, wie das Gateway selbst. Zusätzlich wird gefordert, dass das Security-Modul physischer Manipulation in Grenzen widerstehen kann [Bu13e]. Obwohl, das Öffnen des SMGW nicht unbemerkt geschehen darf [Bu13d], ist eine feste Integration nach TPM-Vorbild dennoch empfehlenswert, um die in **Fehler! Verweisquelle konnte nicht gefunden werden.** gezeigten Bedrohungen zu erschweren. Ohne eine solche Integration, besteht ein Restrisiko, die Identität eines SMGW physisch zu entfernen.

Eine wichtige Funktion im Trusted-Computing-Verfahren in Verbindung mit TPM und TNC, ist die in Tabelle 1 angedeutete Integritätsmessung des Systems und die davon abhängige Attestierung. Veränderungen der Software und Hardware, besonders im Zusammenhang von „Tampering“ und „Elevation of Privileges“, sind so während des Betriebs erkennbar [TCG07]. Eine Form der Integritätsmessung wird vom BSI gem. Tabelle 1 durch sog. Selbsttest vorgeschrieben, die die Integrität der Sicherheitsfunktionen und Daten verifizieren sollen ([Bu13d]). Genauere Informationen sind im Protection Profile (PP) festgelegt, wie die Tabelle 2 zeigt.

Tab. 2: Vorgaben des BSI zu Selbsttests des SMGW gem. CC [Bu13d]

Anforderungsbezeichner	Beschreibung
FPT_TST.1.1	The TSF shall run a suite of self-tests [during initial startup, at the request of a user and periodically during normal operation] to demonstrate the correct operation of [the TSF]
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of [TSF data]
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of [TSF].

Unabhängig von den STRIDE-Bedrohungen aus Tabelle 1 kann bei einer unbedachten Implementierung von Selbsttests, ohne eine vertrauenswürdige Basis, allerdings nicht auf die Ergebnisse der Tests vertraut werden. Im Trusted Computing wird mit Hilfe von Trusted Boot als vertrauenswürdiges Bootverfahren und dem TPM, eine Integritätsmessung beim Start des Sys-

tems realisiert. Durch die Verkettung der gemessenen Attribute in den einzelnen Phasen des Systemstarts, kann ein transitives Vertrauen erzeugt werden, dass die Integrität des Systems zur Startzeit prüfbar macht [TCG07]. Mit Hilfe der Prüfung der Messwert durch TNC können hierdurch Manipulationen (z.B. durch Fremdeinwirkung) an Hardware und Software erkannt werden, um Bedrohungen im Sinne von „Tampering“ erkennen zu können. Das BSI schreibt allerdings keine solche Vertrauensbeziehung vor.

Ein TPM beinhaltet außerdem kryptographische Funktionen für die Verschlüsselung und eine sichere Kommunikation. Es kann aber das Security-Modul nicht ersetzen, da die aktuell auf dem Markt existierenden Chips nach TPM-Spezifikation 1.2 (vgl. [TCG11]) die Anforderungen an die kryptographischen Algorithmen des BSI nicht erfüllen. Aus diesem Grund ist der Einsatz eines TPM im aktuellen Prototyp alleine nicht möglich. Eine Verwendung von TPM 2.0 wäre alternativ denkbar, muss aber in Zukunft noch genauer untersucht werden, da diese Spezifikation zum Zeitpunkt dieser Veröffentlichung noch in Arbeit sich befindet.

Abgesehen von den kryptographischen Algorithmen können die Sicherheitsfunktionen eines TPMs zur Integritätsmessung in Verbindung mit TNC dennoch zu einer Erhöhung der Sicherheit führen. Das SMGW und sein Security-Modul sind vor allem nach außen gut geschützt, so dass Eindringversuche bereits hinreichend schwierig sind. Dennoch ist die Manipulation von Hardware oder Software auf einem entsprechend hohen Niveau denkbar. Solche Manipulationen sind durch die vom BSI vorgegebenen Schutzmaßnahmen nur schwer bis gar nicht erkennbar. Durch die Integritätsmessung und Attestierung mit TPM und TNC können Hard- und Software-Manipulationen erkannt werden. Das reduziert die Möglichkeiten des Angreifers, ein SMGW dauerhaft zu übernehmen. Dieser Aspekt wird in den aktuellen Spezifikationen des BSI nur pauschalisiert betrachtet. Durch die Integritätskontrolle wird zusätzlich die Authentizität der übertragenen Daten gestärkt, da der Zustand des SMGWs, unabhängig von einer PKI-basierten Authentifizierung, überwacht wird. Das TNC-Konzept der TCG in Verbindung mit einem vertrauenswürdigen Bootverfahren stellt daher den stärksten Sicherheitsgewinn durch Trusted Computing im Vergleich zu den BSI-Vorgaben dar.

Ausgehend von den Erkenntnissen der Untersuchung aus Kapitel 4 wurde eine Vorgehensweise entwickelt, die auf den BSI-Vorgaben aufbaut und Komponenten aus dem TC integriert, um die Sicherheit eines SMGW durch die Überwachung seiner Integrität zu erhöhen. Daher lassen sich momentan zwei Lösungsmöglichkeiten an dieser Stelle realisieren:

a. Security Module und paralleler Einsatz eines TPM-Moduls in Version 1.2
b. Security Module und Implementierung des Secure-Boot-Verfahrens ohne TPM-Chip

Im SPIDER-Projekt wurde die letztgenannte Variante ausgewählt, da die Verwendung von zwei Sicherheitschips für ein späteres Produkt als zu teuer bewertet wurde und der Platz innerhalb des SMGW-Hutschienengehäuses stark limitiert ist.

3.3 Secure Boot

Vertrauenswürdige Bootverfahren werden in der Literatur in drei Kategorien unterteilt (vgl. [Sm05]), die jedoch zum Teil synonym verwendet werden:

a. **Trusted Boot:** Prüfung der Komponenten durch Analyse und Messung (im TC eingesetzt).

b. **Secure Boot:** Prüfung der Komponenten durch Analyse und Messung, inklusive festgelegter Aktionen bei negativem Prüfungsergebnis.

c. **Authenticated Boot:** Prüfung der Komponenten durch Analyse und Messung, abhängig von verschiedenen Szenarien. Festgelegte Aktionen bei negativem Prüfergebnis sind möglich. Die Szenarien beschreiben verschiedene valide Systemzustände.

Für die Sicherstellung der Basisintegrität eines SMGWs soll das Secure-Boot-Verfahren zum Einsatz kommen. Ein Secure-Boot-Verfahren kann, im Gegensatz zum Trusted-Boot-Verfahren, auch ohne TPM durch vorhandene Technologien wie einen Co-Prozessor oder der aktuell in ARM-CPUs vorhandenen Trustzone umgesetzt werden. Bei der Umsetzung wird das Secure Boot-Muster [LSW10] in Abbildung 2 angewandt.

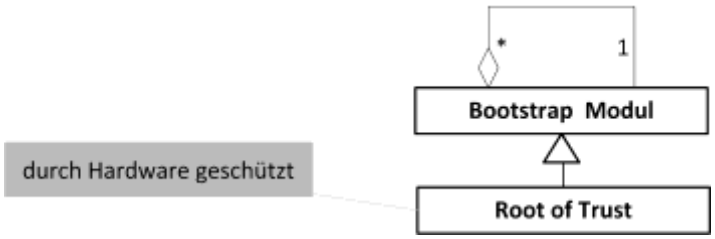

Abb. 2: Secure Boot-Pattern gem. [LSW10]

Der Bootprozess ist als eine Abfolge von Bootstrap-Modulen gestaltet, die miteinander verknüpft sind. Das Bootstrap-Modul „Root of Trust“ bildet den Ausgangspunkt (Basis) des Bootprozesses und ist als eigenständiges Hardware-Modul besonders geschützt. Daraus resultiert die in Abbildung 3 dargestellte Bootsequenz.

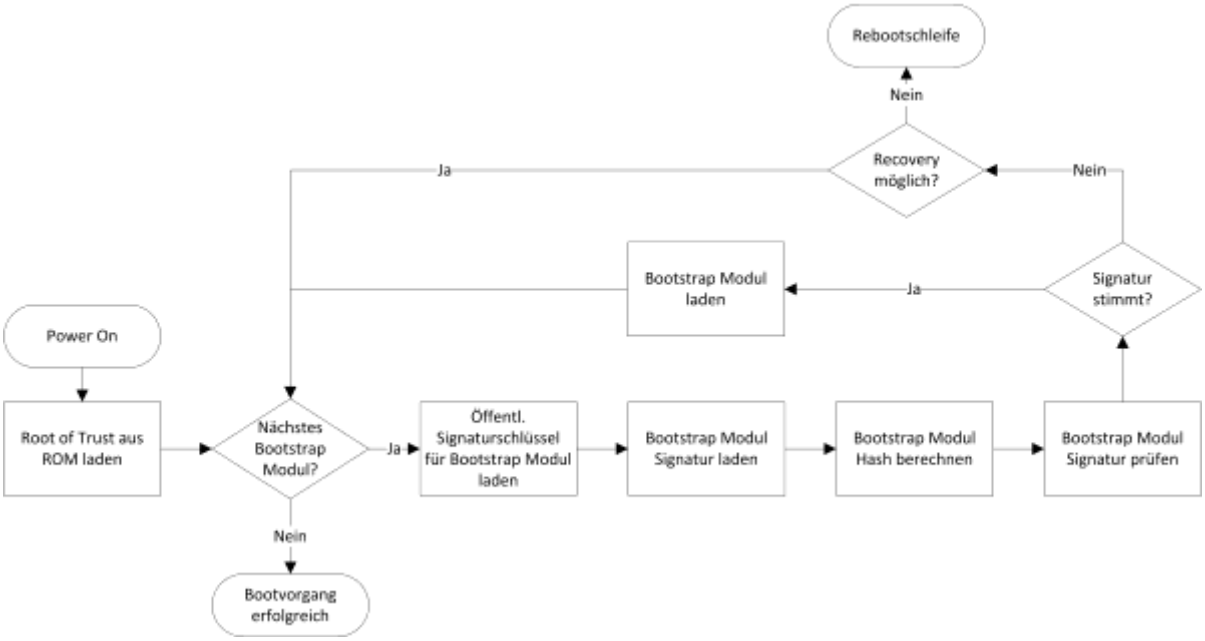

Abb. 3: Secure-Boot-Verfahren

Nach dem Einschalten eines SMGWs wird zuerst das System des „Root of Trust“ aus dem Hardware-ROM geladen. Das System hat eine Referenz zum eigentlichen Bootloader (Bootstrap Modul N) und besitzt zudem eine Signatur, die den Soll-Zustand des Bootloaders

beschreibt sowie den für die Verifizierung der Signatur benötigten öffentlichen Schlüssel. Bevor das System den Bootloader lädt, wird der Ist-Zustand des Bootloaders mit der Soll-Signatur verglichen. Nur wenn die Prüfung positiv ist, wird der Bootloader geladen und die Kontrolle im Bootprozess an ihn übergeben. Der Bootloader prüft daraufhin die Hardware-Integrität (z.B. Zustand des „Tamper-Resistant-Grid“) und das Betriebssystem (Bootstrap Modul N+1) auf dieselbe Weise mit Hilfe von Signaturen der Soll-Zustände. Das Betriebssystem kann wiederum einzelne Applikationen (Bootstrap Modul N+M) prüfen.

Schlägt eine Prüfung fehl, wird der Bootvorgang unterbrochen und das System geht in einen Fehlerzustand, gekennzeichnet durch einen dauerhaften Reboot, sofern es nicht auf eine vertrauenswürdige Betriebsstufe (Recovery Möglichkeit) zurückfallen kann. Hierzu dient eine Backup-Partition mit einem Duplikat der SMGW-Firmware. Sollte eine Prüfung erst oberhalb des Bootloaders fehlschlagen, ist es möglich, mit Hilfe des Bootloaders die Backup-Partition für die weitere Bootsequenz zu verwenden. Erst wenn auch die Bootstrap Module auf dieser Partition nicht ihren jeweiligen Soll-Zuständen entsprechen, bleibt das System in dem beschriebenen Fehlerzustand. Somit kann sichergestellt werden, dass es nur dann zum Betrieb eines SMGWs kommt, wenn der Initialzustand vertrauenswürdig ist. [GSHD14]

3.4 Trusted Network Connect (TNC)

In Kapitel 4 wurde festgestellt, dass die Integritätskontrolle durch den Einsatz von TNC einen signifikanten Sicherheitsgewinn darstellt. Davon ausgehend, dass die TNC-Architektur als erweiterbare Architektur beschrieben ist, kann TNC im Allgemeinen am SMGW eingesetzt werden. Der Fokus bei der Umsetzung von TNC liegt in der Ergänzung der BSI-Vorgaben durch die Integritätssicherung, während die Authentifizierung nach bestehenden BSI-Vorgaben realisiert wird. Abbildung 4 zeigt das SMGW als Network Access Requestor (NAR) und den GWA als Network Access Authority (NAA). Wie bereits in Kapitel 4 dargestellt ist ein aktueller TPM-Chip gemäß Spezifikation 1.2 nicht allein verwendbar. Zudem hat eine wirtschaftliche Prüfung ergeben, dass die Module beider Standards nicht parallel eingesetzt werden können. Aus diesem Grund wird im Rahmen der Realisierung ein Integrity Measurement Collector (IMC) entwickelt, der ohne ein TPM eingesetzt werden kann.

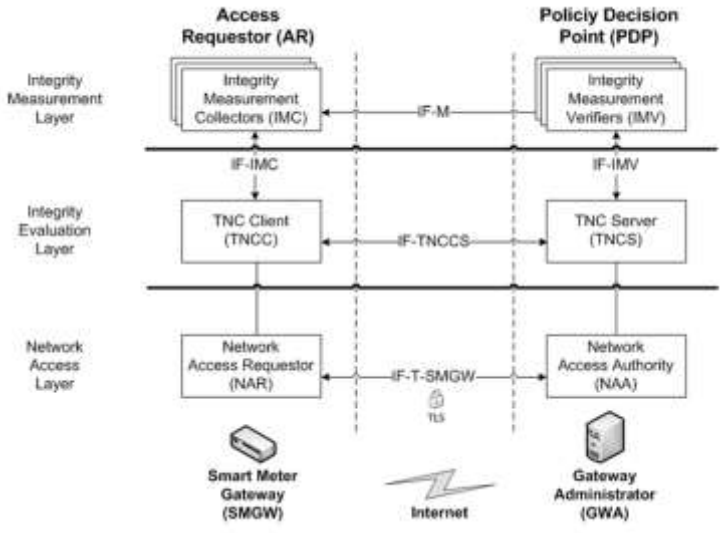

Abb. 4: TNC-Schichtenmodell mit relevanten Komponenten des Systemkonzepts

Der IMC wertet hierzu softwarebasiert Sicherheitsaspekte aus, die die Integrität des SMGWs messbar machen. Hierfür sind Hash-Summen vorgesehen, die periodisch über ausgesuchte Komponenten (z.B. eingesetzte Firmware-Komponenten, Konfigurationsdateien, Hardwarekomponenten) 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. Im Sinne von TNC übermittelt der IMC die Messwerte zur Attestierung an den Integrity Measurement Verifier (IMV), der sich auf der Seite des GWA befindet. Dementsprechend, wird auf der Seite des GWAs ein IMV umgesetzt, 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. Durch die softwarebasierte 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.

In Abbildung 4 wird der Vermittlungskanal zwischen NAA und NAR als IF-T-SMGW dargestellt, da an diesem Punkt keine bestehenden Spezifikationen der TCG für IF-T verwendet werden kann. Die Bezeichnung IF-T-SMGW verdeutlicht, dass an dieser Stelle eine neue Spezifikation notwendig ist, die noch nicht durch die TCG-Spezifikationen abgedeckt wird. Es wird an einem Vorschlag für die TCG innerhalb des Projektes gearbeitet. Für die Übertragung der Integritätsmesswerte vom SMGW zum GWA zur Verifizierung der Integrität, soll ein Webservice verwendet werden, der im Rahmen der BSI-Vorgaben für die Alarmierung und Ereignisvermittlung in Verbindung mit dem Systemzustand eines SMGWs eingesetzt wird. Alle weiteren Vorgaben zur Kommunikation über die WAN-Schnittstelle (vgl. [Bu13a]) haben dabei weiterhin Bestand. Um reguläre Ereignisse und Alarmierungen von TNC-Nachrichten zu unterscheiden, sollen letztere speziell gekennzeichnet werden. Dieses Vorgehen, ermöglicht die Interoperabilität zu nicht TNC-fähigen Endpunkten. TNC-Nachrichten sind dann für diese Endpunkte normale Ereignisse, während TNC-fähige Geräte die Nachrichten gesondert interpretieren können. Die darüber liegenden Ebenen sind vollständig in Software umgesetzt und von den BSI-Vorgaben kaum beeinflusst, daher können auch die vorhandenen Spezifikationen verwendet werden. [GSHD14]

4 Fazit

Die relevanten Aspekte zur Verbesserung des Sicherheitsgrades durch Trusted Computing sind die Integritätsmessung am SMGW und die damit verbundene Attestierung der Messwerte beim GWA in Verbindung mit TNC, da solche Überlegungen bei den aktuellen BSI-Spezifikationen bisher keine Rolle spielen. Es ist hierbei besonders wichtig die Integritätsmessung sicher durchzuführen, da sonst kein Vertrauen in die Messwerte möglich ist. Die Einbettung von Trusted-Computing-Mechanismen ohne TPM erfüllt diese Anforderung bereits, indem eine eindeutige Vertrauenskette erzeugt wird. Hierzu werden Integritätsmessungen während des Bootvorgangs (Secure Boot) sowie zur Laufzeit eingesetzt und die Messwerte zu den Hard- und Software-Komponenten manipulationssicher gespeichert.

Die Informationssicherheit kann durch einen TPM-Chip allerdings noch weiter erhöht werden. Dieser kann aber nach derzeitigem Stand nicht ohne Security Module eingesetzt werden, da in der TPM-Spezifikation 1.2 die kryptographischen BSI-Anforderungen nicht erfüllt werden

können. Ob sich dies in der Spezifikation 2.0 ändern wird, muss abgewartet werden. Eine andere Lösung wäre es, den TPM-Chip nur zur Integritätsmessung zu verwenden und ein BSI-zertifiziertes Sicherheitsmodul die Authentifizierung und Verschlüsselung durchführen zu lassen. Dies bedeutet aber derzeit einen nicht zu unterschätzenden Mehraufwand.

Die Einbettung von Trusted Computing stellt aber in jedem Fall einen Mehrwert dar, um Smart-Grid-Infrastrukturen wirkungsvoll absichern zu können. Zukünftig kann der Einsatz eines Monitoring-Systems die Informationssicherheit in Smart-Grid-Umgebung weiter erhöhen. Das Protokoll Interface Metadata Access Point (IF-MAP) aus der TNC-Spezifikation definiert hierfür bereits Schnittstellen, die zur zentralen Informationssammlung eingesetzt werden können. Damit lassen sich solche sensitiven Systeme auch in Echtzeit kontinuierlich überprüfen.

5 Danksagung

Das SPIDER-Projekt (www.spider-smartmetergateway.de) ist ein gefördertes BMWi-Projekt mit einer Laufzeit von zwei Jahren, das im März 2013 seine Arbeiten begonnen hat. An dem Projekt sind 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 sind 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 diese Herangehensweise erst ermöglicht haben.

Literatur

[Bu13a] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems*. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2013.

[Bu13b] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie BSI TR-03109-2 Smart Meter Gateway Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls*. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2013.

[Bu13c] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie BSI TR-03109-4 Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways*. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2013.

[Bu13d] Bundesamt für Sicherheit in der Informationstechnik: *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2013

[Bu13e] Bundesamt für Sicherheit in der Informationstechnik: *Protection Profile for the Security-Module of a Smart Meter Gateway (Security-Module PP)*. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2013.

[Bu13f] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie BSI TR-03109-1 Anlage VI : Betriebsprozesse*. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2013.

[DDN10] Detken, Diederich, Nowak: *Vertrauenswürdiger mobiler Zugriff auf Unternehmensnetze im VOGUE-Projekt*. D.A.CH Security 2010: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, D.A.CH-Security Konferenz vom 21.-22. September, Herausgeber: Peter Schartner und Edgar Weippl, syssec Verlag, ISBN-13: 978-3-00-031441-4, Wien 2010

[Detk12] Kai-Oliver Detken: *Trusted Computing - Flopp oder Durchbruch des TPM-Chips?*. NET Verlagsservice GmbH, Woltersdorf 2012

[DSBW12] Detken, Scheuermann, Bente, Westerkamp: *Automatisches Erkennen mobiler Angriffe auf die IT-Infrastruktur*. D.A.CH Security 2012: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, Herausgeber: Peter Schartner und Jürgen Taeger, syssec Verlag, ISBN 978-3-00-039221-4, Konstanz 2012

[GSHD14] Genzel, Sethmann, Hoffmann, Detken: *Sicherheitskonzept zum Schutz der Gateway-Integrität in Smart-Grids*. Sicherheit 2014 - Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), GI-Edition, Herausgeber: Stefan Katzenbeisser, Volkmar Lotz, Edgar Weippl. Köllen Druck + Verlag GmbH, Bonn 2014

[ISO09] ISO/IEC: *ISO/IEC 11889-1 Information technology - Trusted Platform Module, Part 1: Overview*. ISO copyright office, Genf 2009

[Ki06] Kinney, S.: *Trusted platform module basics: using TPM in embedded systems*. Elsevier, Amsterdam [u.a] 2006

[LSW10] Löhr, H.; Sadeghi, A.-R.; Winandy, M: *Patterns for Secure Boot and Secure Storage in Computer Systems, Availability*. In IEEE: ARES '10 International Conference on Reliability, and Security, Krakow 2010

[SHB13] Sethmann, R.; Hoffmann, O.; Busch, S.: *Sichere Datenübertragung in Smart Grids mit Trusted Computing*. D.A.CH Security 2013: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, ISBN 978-3-00-042097-9, Hrsg. Peter Schartner u. Peter Trommler, syssec-Verlag, Nürnberg 2013

[Sm05] Smith, S. W: *Trusted Computing Platforms: Design and Applications*. Springer, New York 2005

[Sp14] SPIDER: *Sichere Powerline-Datenkommunikation im intelligenten Energienetz*. http://www.spider-smartmetergateway.de/, Nov. 2013; zuletzt aufgerufen am 11.06.14.

[TCG07] Trusted Computing Group: *TCG Specification Architecture Overview*. TCG PUBLISHED, Beaverton, 2007

[TCG11] Trusted Computing Group: *TPM Main - Part1 Design Principles*. 01 03 2011. Specification Version 1.2 Revision 116, 2011

[TCG12] Trusted Computing Group: *TCG Trusted Network Connect TNC Architecture for Interoperability*. Specification Version 1.5, Revision 3, 2012

[TCG14] Trusted Computing Group: *About TCG*. https://www.trustedcomputinggroup.org/about_tcg, Jun. 2014; zuletzt aufgerufen am 11.06.14