DECOIT®

01110000111010111000100101110000111010111000 1001

Integritätsmessung von Smart Meter Gateways

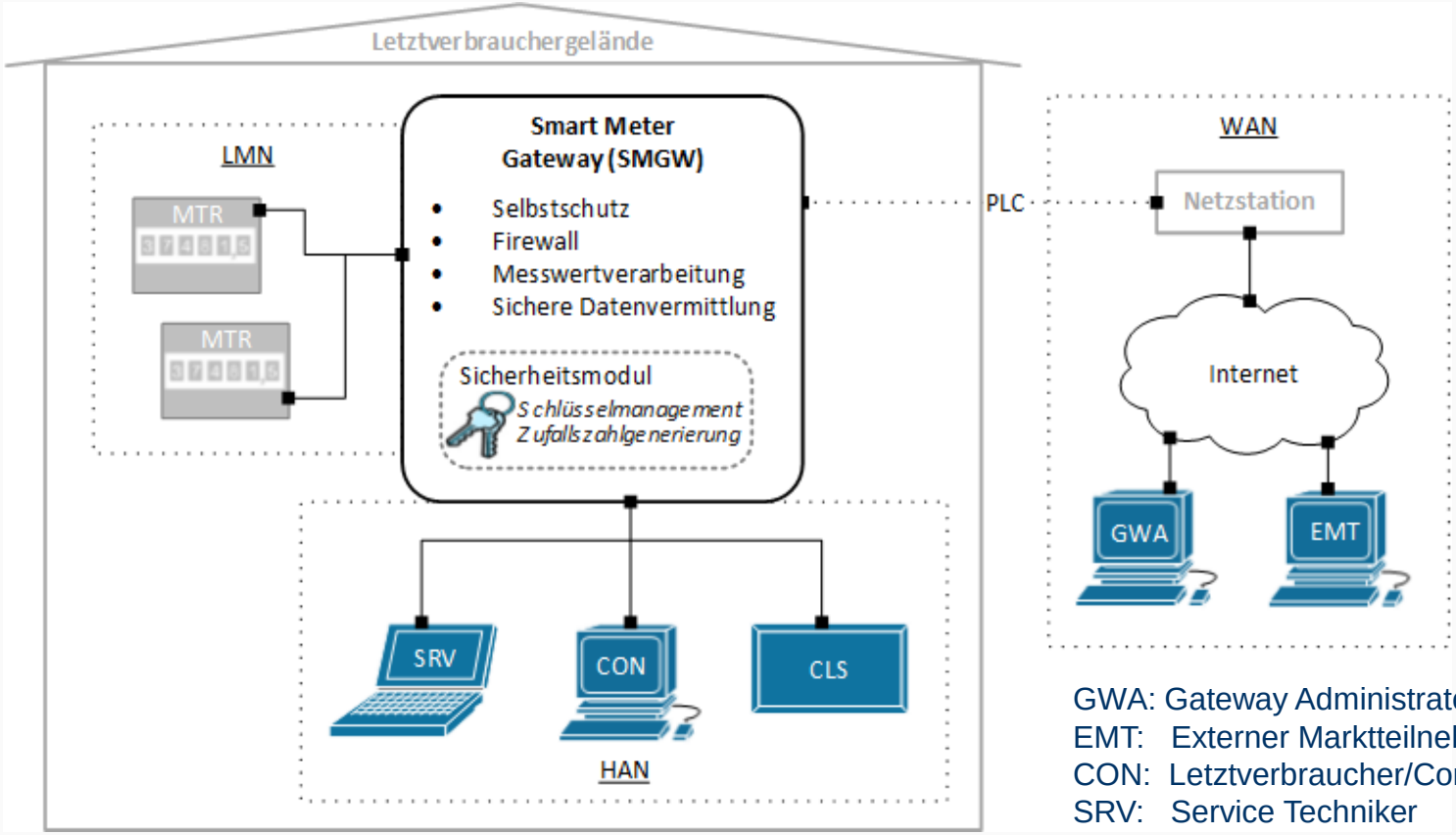
Kai-Oliver Detken · Marcel Jahnke · Malte Humann

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
detken@decoit.de

Agenda

- Einführung in die Sicherheitsarchitektur von Smart Meters
- Vorstellung des BMWi-Projekts SPIDER
- Integritätskonzept mit Trusted Computing
- Smart Meter Gateway: vom F&E-Prototypen zum Produkt
- Testbed-Ergebnisse
- Zusammenfassung

Sicherheitsarchitektur von Smart Meters



WAN: Wide Area Network
HAN: Home Area Network
LMN: Local Metrological Network

GWA: Gateway Administrator
EMT: Externer Marktteilnehmer
CON: Letztverbraucher/Consumer
SRV: Service Techniker
CLS: Controllable Local Systems
MTR: Smart Meter
PLC: PowerLine Communication

Das SPIDER-Projekt

- Sichere Powerline-Datenkommunikation im intelligenten Energienetz (SPIDER)
  - 2-Jahre-Projekt vom ZIM (BMWi)
  - Zeitdauer: 1. März 2013 bis 31. Mai 2015
  - Projektziel: Entwicklung eines Smart Meter Gateway (SMGW) Prototypens mit anschließender BSI-Zertifizierung
- Partner:
  - Industrie: DECOIT GmbH, devolo AG (Projektleiter)
  - Hochschulen: Hochschule Bremen, Fraunhofer FOKUS, Universität Siegen
  - Assoziierte Partner: Maxim Intgrated, datenschutz cert sowie die Energie-Provider Vattenfall und RWE

Berücksichtigung externer Marktteilnehmer

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

SPIDER-Sicherheitsarchitektur

- Die Sicherheit und Stabilität zukünftiger, intelligenter Energienetze hängt maßgebend von einer sicheren Datenübertragung zwischen den Marktteilnehmern sowie den eingesetzten Steuerkomponenten ab!
- Das SMGW ist daher die zentrale Instanz eines Smart-Metering-Systems
  - Verlässliche Verarbeitung von Messwerten
  - Sichere Speicherung von Messdaten
  - Sichere Datenübertragung zwischen den Smart Metern und Teilnehmern
- Der GWA ist die einzige vertrauenswürdige Instanz innerhalb des intelligenten Messsystems
  - Konfiguration der SMGW-Komponente
  - Überwachung und Steuerung der SMGW-Komponente

SMGW-Eigenschaften (1)

- Das SMGW verbindet die Smart-Meter-Komponenten und Rollen über die angeschlossenen Netze miteinander
- 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 Messwerte 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

SMGW-Komponente im Hutschienenformat

SMGW-Eigenschaften (2)

- Zur sicheren Übermittlung der Daten zwischen den einzelnen Komponenten und Rollen werden asymmetrische und symmetrische Verschlüsselungsverfahren eingesetzt
- Hierbei wird zwischen Inhaltsdaten- und Transportverschlüsselung unterschieden
- Zur Verschlüsselung verwendet das SMGW ein Sicherheitsmodul:
  - Sichere Speicherung von Zertifikats- und Schlüsselmaterial
  - Schlüsselgenerierung und Schlüsselaushandlung auf Basis von Elliptischen Kurven
  - Erzeugung und Verifikation digitaler Signaturen
  - Zuverlässige Erzeugung von Zufallszahlen

SMGW-Komponente im Hutschienenformat

Einsatz von Trusted Computing

- 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!
- Diese Lücke kann der Ansatz Trusted Network Communications (TNC) der TCG schließen

Integritätskontrollen

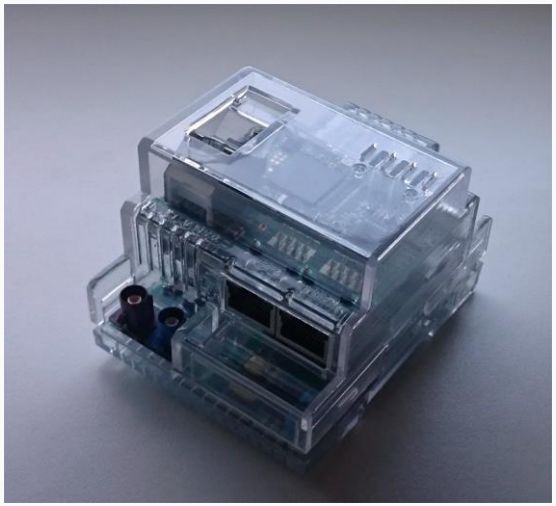
- Bei der Umsetzung im SPIDER-Projekt lassen sich drei Integritätskontrollen unterscheiden:
  - Die physikalische Integritätskontrolle kann durch Verplombung oder mechanischen Schutz umgesetzt werden
  - Zur Integritätskontrolle beim Bootvorgang wurde im SPIDER-Projekt ein sicheres Bootverfahren (Secure Boot) implementiert, bei dem einzelne Bootstrap-Module in einer Bootsequenz nacheinander geladen und ausgeführt werden
  - Die Integritätskontrolle im Betrieb soll nach BSI-Richtlinien durch einen Selbsttest umgesetzt werden. Dieser Selbsttest kann aber manipuliert worden sein, weshalb im SPIDER-Projekt der TNC-Ansatz als sinnvolle Ergänzung eingebracht wurde

Integritätskonzept

- Der GWA nutzt im SPIDER-Projekt für die Überwachung der Integrität eines SMGW den TNC-Ansatz
  - Es werden Messwerte empfangen und geprüft
  - Das SMGW protokolliert den Ablauf der Integritätsprüfung
- Das GWA soll mehrere SMGWs unterschiedlicher Hersteller verwalten bzw. überwachen können:
  - Alle Hersteller nutzen die gleiche/feste Anzahl von Attributen, die gemessen (IMC) und überprüft (IMV) werden können
  - Jeder Hersteller stellt eine spezialisierte IMV bereit, die die Integrität eines SMGW überprüfen kann

Smart Meter Gateway: vom F&E-Prototypen zum Produkt

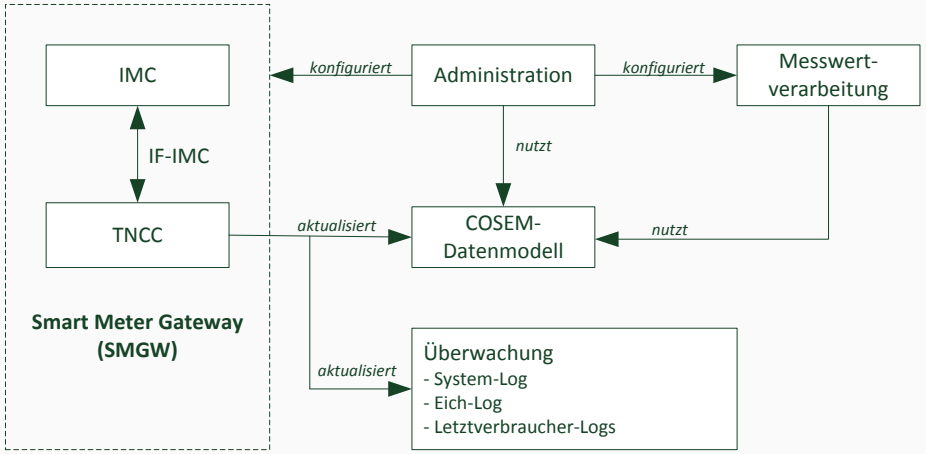
- Ein erster Prototyp wurde innerhalb des SPIDER-Projektes entwickelt
- Das Chassis des Prototyps bestand aus zwei Komponenten, die sich nach dem Zusammenfügen nicht mehr schadlos öffnen ließen (Plomben-Ansatz)
- Der TNC-Ansatz wurde optional integriert, so dass er auch deaktiviert werden kann
- Ein aktivieren/deaktivieren muss in den Logbüchern gespeichert werden
- Ein One-Meter-Szenario wurde erst einmal angestrebt (Anbindung eines einzelnen Smart Meters mit unterschiedlichen Use Cases)



Hardware-Prototyp von SPIDER

TNC-Integration im SMGW

- Das SMGW enthält den TNC-Client (TNCC), während das GWA den TNC-Server (TNCS) besitzt
- Die Administration des SMGW geschieht über eine RESTful-Webservice-Schnittstelle
- Der TNC-Ansatz überwacht
  - Systemlogs
  - Eichlogs
  - Letztverbraucherlogs



Testbed-Ergebnisse

- Im SPIDER-Projekt sind diverse Tests durchgeführt worden, um die Interoperabilität zu unterschiedlichen GWA-Anbietern sicherstellen und Sicherheitsmechanismen überprüfen zu können:
  - Aushandlung der Roadmap
  - Festlegung der Infrastruktur
  - Durchführung der Interoperabilitätstests
  - Dokumentation der Ergebnisse
- Die Testläufe des SMGW wurden auf Anwendungsebene durchgeführt
- Als Voraussetzung für die Testfällte und Use Cases galten grundsätzlich die Anforderungen an die Infrastruktur

Testumgebung

SMGW-VM

192.168.10.30/24

SMGW

Server-Services	Port
Wake-Up-Service	8085

Client-Services	Port
WKS1: Management	-
WKS3: Info-Report	-
WKS4: NTP-https	-
WKS6: TNC	-

GWA-VM

192.168.10.10/24

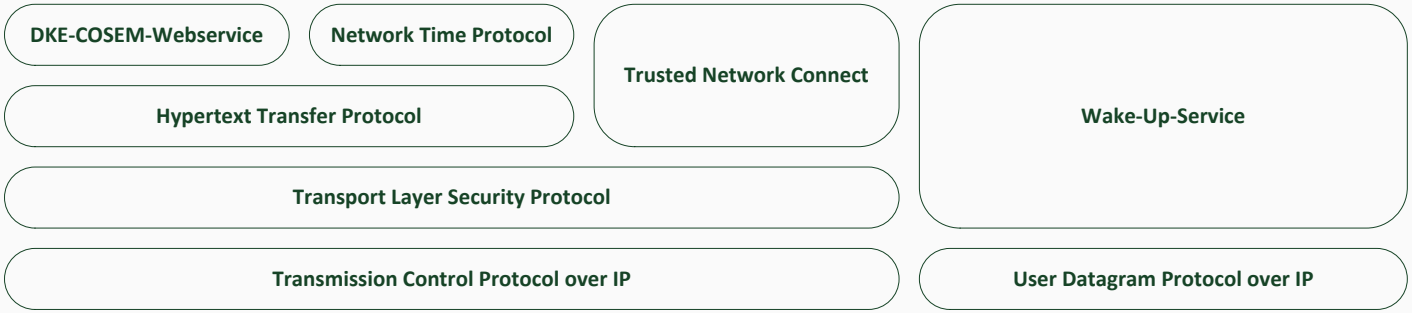
GWA

Server-Services	Port
WKS1: Management	8080
WKS4: NTP-https	30123
WKS6: TNC	30271

Client-Services	Port
Wake-Up-Service	-

EMT

Server-Services	Port
WKS3: Info-Report	30003



Absicherung der Inhalte/Kommunikation

- Für die sichere Kommunikation müssen auf beiden Endpunkten sowohl die Schlüsselmaterialien als auch die Zertifikate ausgetauscht werden
- Auf dem SMGW stehen Schlüsselmaterialien für die Inhaltsdatenverschlüsselung mit CMS sowie für die gesicherte Kommunikation mit TLS zur Verfügung
- Die BSI-Richtlinie unterteilt die kryptographischen Vorgaben bis und ab 2014:
  - Prototyp: NIST P-256 als Elliptische Kurve (bis 2014)
  - Produkt: BrainpoolP256r1 (ab 2015)

Testbed-Ergebnisse

- 8 Hersteller wurden insgesamt innerhalb der Projektlaufzeit getestet
  - Wake-Up-Service: funktionierte weitestgehend
  - TLS-Handshake: 6 von 8 Herstellern
  - Inhaltsdatenverschlüsselung mittels CMS: 6 von 8 Herstellern
  - COSEM-Webservice: 6 von 8 Herstellern
  - TNC: kein Hersteller unterstützte diesen Ansatz
- Interoperabilitätstests ergaben einen Mehrwert für alle Parteien, da frühzeitig Fehlverhalten erkannt werden konnte
- BSI-Richtlinien lassen sich unterschiedlich interpretieren, weshalb es auch zu Inkompatibilitäten kam
- Aktuell ist ein One-Meter-Szenario umgesetzt worden, welches in einem kleinen Feldtest erprobt wird
- Trusted Computing spielte bei anderen Herstellern keine Rolle

Zusammenfassung

- Im SPIDER-Projekt mussten mehrere Kompromisse bei der Entwicklung gemacht werden, da
  - die Partner sich in die Materie erst einarbeiten mussten,
  - die TR-Spezifikationen noch nicht fertiggestellt waren,
  - die Sicherheits- und TPM-Chips nicht gelieferten werden konnten,
  - die Ressourcen und die Zeit limitiert waren.
- Nach dem Projekt wurde aufgrund der guten Ergebnisse und der zu erwartenden Absatzmenge entschieden, den Prototypen zu einem Produkt weiter zu entwickeln
- Es bleibt aber nach wie vor ein weiter Weg von dem Prototyp zu einem zertifizierten Produkt, den der ursprüngliche Konsortialführer devolo AG stark unterschätzt hatte
- Derzeit werden daher verschiedene Strategien bei gefahren, um das Produkt fristgerecht fertigstellen zu können

Vielen Dank für Ihre Aufmerksamkeit!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

https://www.decoit.de
info@decoit.de