DECOIT®

# Absicherung von Smart-Meter-Umgebungen

## Vom Prototyp zum Produkt


Prof. Dr. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
detken@decoit.de

# Portfolio der DECOIT GmbH

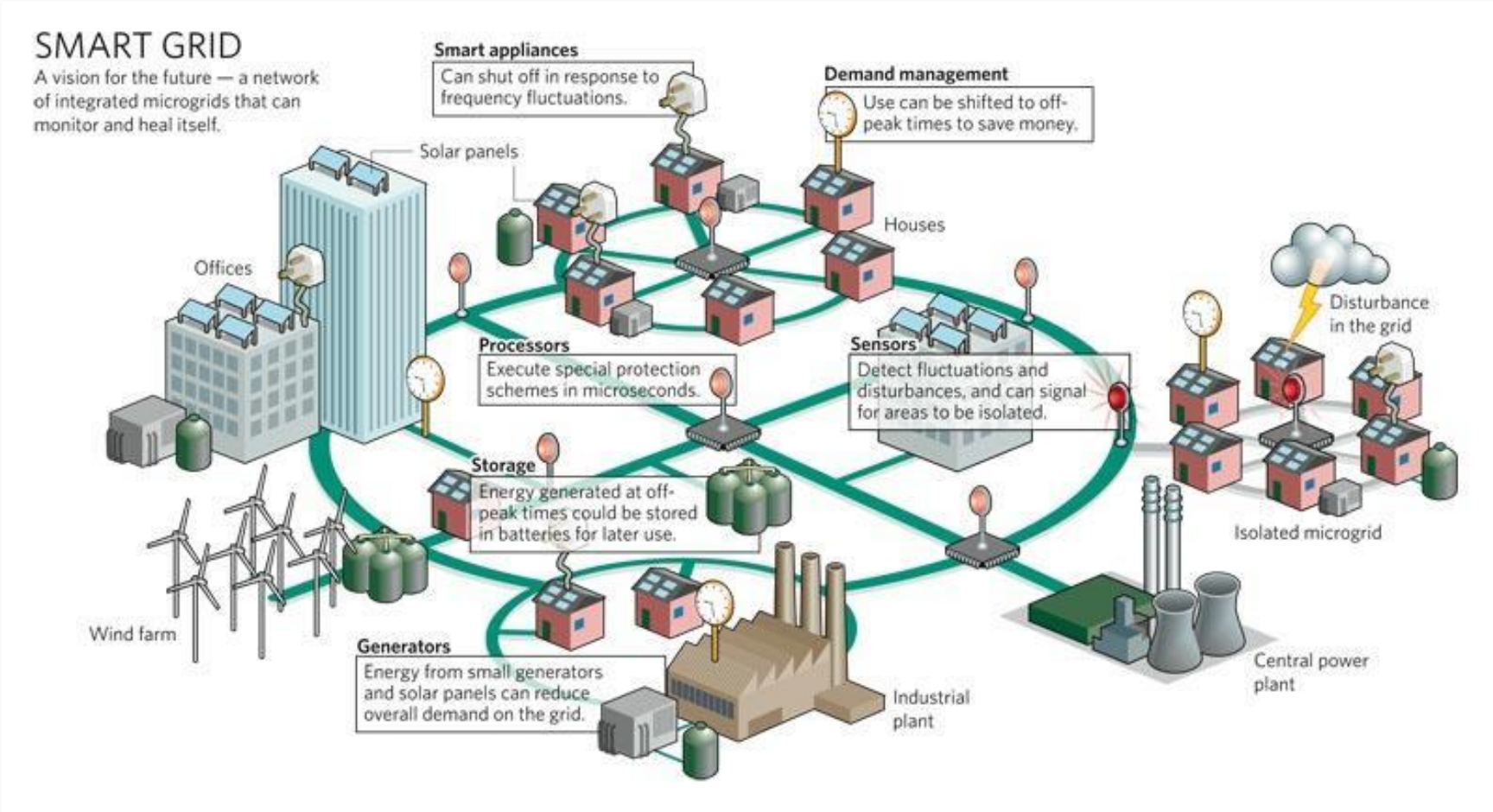
- Gründung am 01.01.2001
- Seit 2003: Sitz im Technologiepark an der Universität Bremen
- Fokus: Herstellerneutrale, ganzheitliche Beratung von IT-Lösungen
- Zielsetzung: akademische Lösungsansätze in kommerzielle Marktprodukte/Lösungen umsetzen
  - Consulting: ganzheitliche/herstellerneutrale Beratung
  - Systemmanagement: Planung, Umsetzung und Support von Hersteller- und Open-Source-Lösungen
  - Software-Entwicklung: Entwickeln von Individuallösungen und Produkten mit hohem Innovationscharakter
  - Forschungsprojekte: entwickeln innovativer IT-Lösungen
- Heute: Full-Service-Anbieter im IT-Umfeld
- Enge Kooperationen zu Herstellern, Anbietern und Hochschulen

DECOIT®

# Agenda

- Einführung in Smart-Grid-Netze
- Das SPIDER-Projekt
- Sicherheitsarchitektur für Smart-Meter-Umgebungen
- Einsatz von Trusted Computing
- Architektur des Trusted Network Connect (TNC)
- Einsatz von Open Source
- Umsetzung des Prototypen in ein Produkt
- Fazit

# Smart-Grid-Netze (1)




*https://smartgridtech.files.wordpress.com/2012/05/sg-nature.jpg*

# Smart-Grid-Netze (2)

- Intelligente Energienetze sind nach dem Energiewirtschaftsgesetz (EnWG) zukünftig gesetzlich vorgeschrieben
- Der Aufbau solcher Smart-Grid-Netze beinhaltet ebenfalls intelligente Messsysteme (Smart Meter)
- Energienetze entwickeln sich vom zentralen in ein dezentrales Energieversorgungssystem
- Smart-Meter-Komponenten müssen dementsprechend remote gesteuert werden können
- Dies wird über vorhandene globale Netze, wie das Internet, vorgenommen werden
- Diese Kritischen Infrastrukturen (KRITIS) sind dementsprechend gut gegen unerwünschte Außenwirkungen abzusichern

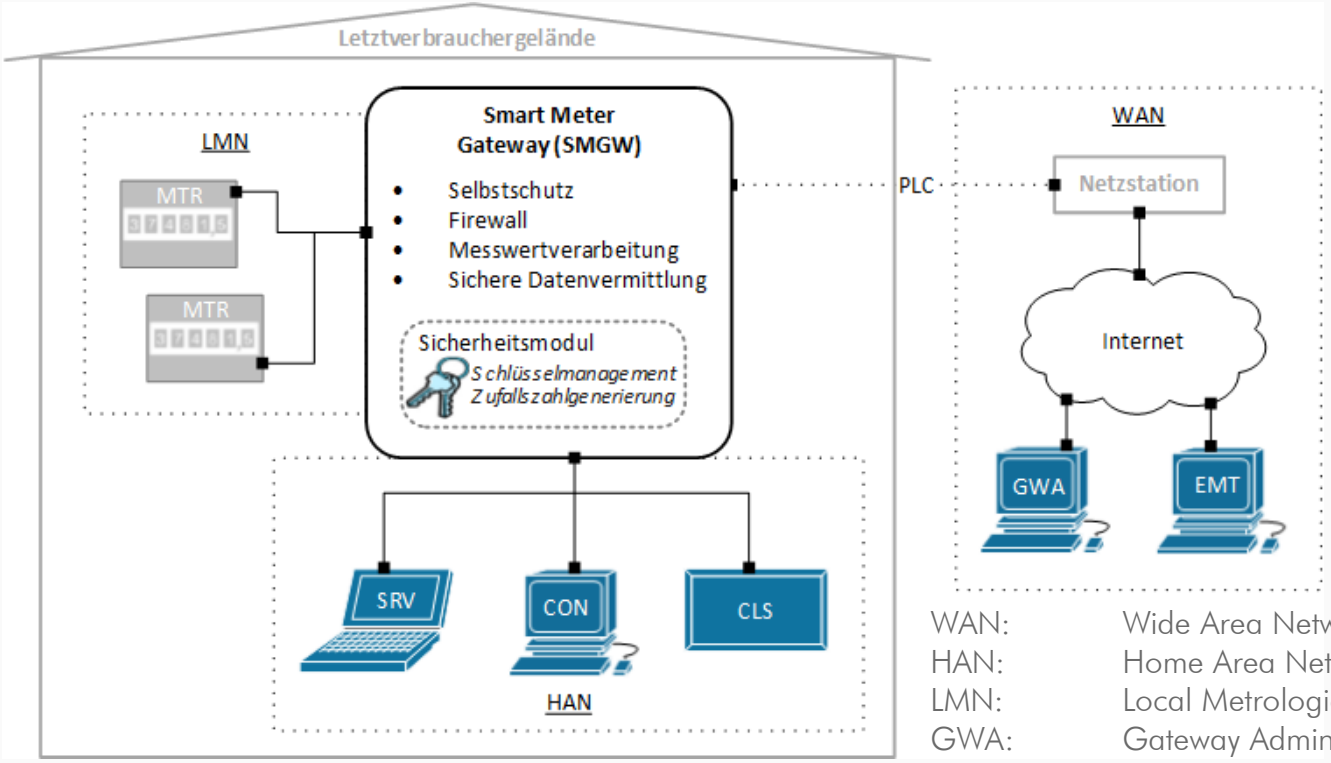
# Anforderungen die IT-Sicherheit

- Komponenten eines Smart Grids und IT-Systeme müssen in die Lage versetzt werden, Einbruchsversuche zu erkennen, zu melden und bereits autonom darauf zu reagieren
- Als Anforderungen an die IT-Sicherheit in Smart Grids muss daher folgendes gelten:
  - **Messung der Systemintegrität:** es muss erkennbar sein, ob Smart-Meter-Messungen vertraut werden kann oder nicht.
  - **Attestation:** eine starke Authentifizierung ist einzusetzen, um eine zertifizierte Aussage über die Integrität erhalten zu können.

# Das SPIDER-Projekt

- Sichere Powerline -Datenkommunikation im intelligenten Energienetz (SPIDER)
  - Projektziel: Entwicklung eines Smart Meter Gateway (SMGW) mit anschließender BSI -Zertifizierung
  - Laufzeit: März 2013 bis Mai 2015
  - URL-Adresse: http://www.spider-smartmetergateway.de
  - 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
  - Seit August 2015 arbeiten die Partner devolo AG und DECOIT GmbH gemeinsam an einem SMGW-Produkt weiter

# Sicherheitsarchitektur (1)




| | |
|---|---|
| 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 |

# Sicherheitsarchitektur (2)

- Zur Verschlüsselung verwendet das SMGW ein Sicherheitsmodul, welches folgende Funktionen aufweist:
  - Sichere Speicherung von Zertifikats- und Schlüsselmaterial
  - Schlüsselgenerierung und Schlüsselaushandlung auf Basis von elliptischen Kurven
  - Erzeugung und Verifikation digitaler Signaturen
  - Zuverlässige Erzeugung von Zufallszahlen
- Durch die zentrale Rolle, die ein SMGW in einer Smart-Meter-Umgebung einnimmt, müssen spezielle Methoden zum Selbstschutz integriert sein
- Eine Integritätsüberprüfung fehlte bislang!

# Einsatz von Trusted Computing (1)

## Trusted Computing (TC)

- Hardware-basierte Identität (Hardware-Vertrauensanker, Root of Trust)
- Integritätsmessung der Hard- und Software
- Vertrauenswürdiges Bootverfahren (Trusted Boot)

## Trusted Computing Group (TCG)

- Organisationseinheit der Industrie
- Offene Standards zu Trusted Computing
  - teilweise durch IETF in RFC-5792, RFC-5793, RFC-6876 und RFC-7171 übernommen

# Einsatz von Trusted Computing (2)

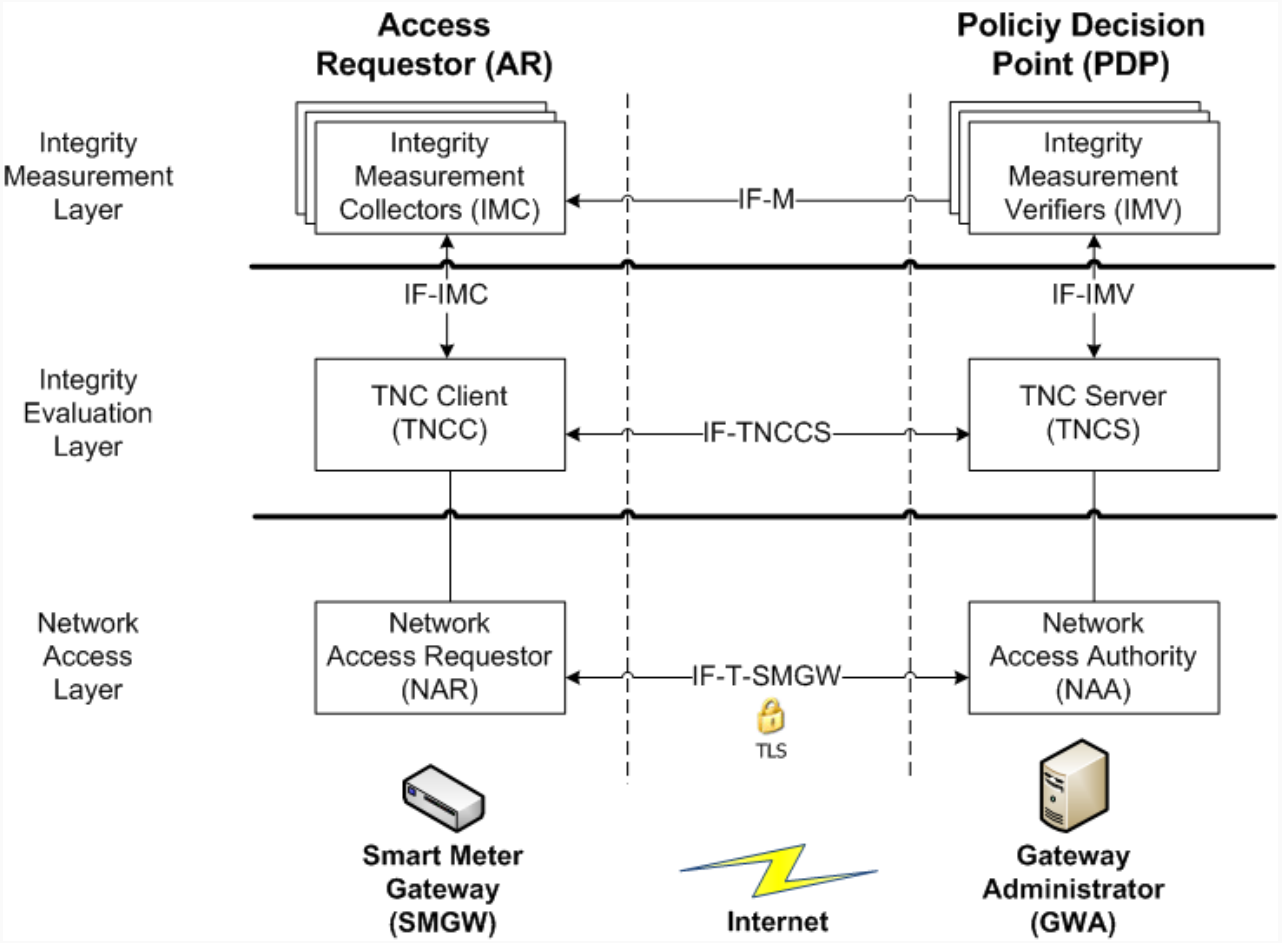
## Trusted Platform Modul (TPM)

- Root of Trust / Hardware Trust Anker
- Systemidentität
- Integritätsmessung
- Trusted Boot


## Trusted Network Connect (TNC)

- Systemintegritätsvalidierung entfernter Systeme (Remote Attestation)
- Authentifizierung
- Monitoring

# TNC-Architektur für Smart Meter



# TNC-Architektur (2)

- Durch den TNC-Ansatz kann eine Remote Attestation vom SMGW-Administrator (GWA) zum SMGW durchgeführt werden
  - Der IMC sammelt Daten und vermittelt diese an den TNC-Client (TNCC)
  - Der TNC-Server (TNCS) vermittelt die Daten an den IMV
  - Der TNCS meldet bei fehlerhafter Validierung dies an den GWA
  - IMC und IMV müssen durch den SMGW-Hersteller geliefert werden
- Dadurch kann die Integrität der Hard- und Software elektronisch ermittelt werden

# Einsatz von Open Source

- Verwendung von Open-Source-Zutaten für die SMGW-Entwicklung
  - SQLite-Datenbank
  - Eclipse Link für Datenbankanbindung
  - Java für den SMGW-Quellcode
  - Jetty Webservice für RESTful-Schnittstelle
  - Jersey zum Parsen von XML für COSEM-Daten
  - Java-Bibliothek jTNC
- Abschließend wurde der Quellcode in eine einheitliche MIT License überführt

# Weiterentwicklung zum Produkt

- Die Firmen DECOIT GmbH und devolo AG entwickeln den SPIDER-Prototypen weiter
  - Sicherstellung der Interoperabilität mit GWA-Softwaresuiten sowie Basiszählern durch umfangreiche Interoperabilitätstests
  - Optimiert für die WAN-Kommunikation via G3-PLC
  - Inkrementelle Firmware-Updates
  - Sicherheitskonzept
    - Secure-Boot-Verfahren
    - Erkennung von Kompromittierung beim GWA
- Geplant in 2016: Feldtests und BSI-Zertifizierung


# Fazit

- Die Umstellung der Energienetze auf intelligente Messsysteme (Smart Meter) ist ein langwieriger Prozess
- Aufgrund der Nutzung öffentlicher Netzstrukturen wie dem Internet müssen hohe Sicherheitsvorkehrungen geschaffen werden
- Kritische Infrastrukturen (KRITIS) müssen dabei den höchsten Sicherheitsanforderungen genügen
- In Deutschland legte das BSI bereits die Messlatte für diese Anforderungen sehr hoch
- Die Implementierung von Trusted Computing erhöht nochmals diese Anforderungen und ermöglicht Integritätsmessungen vor und während des Betriebs
- Die Anerkennung durch das BSI ist die nächste Herausforderung

# Vielen Dank für Ihre Aufmerksamkeit!

**DECOIT GmbH**
Fahrenheitstraße 9
D-28359 Bremen

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