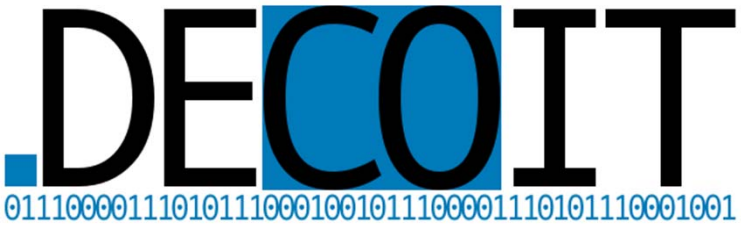


Absicherung von Smart-Meter-Umgebungen mit Trusted Computing

Prof. Dr. Kai-Oliver Detken[1], Carl-Heinz Genzel[2]

[1] DECOIT GmbH, Fahrenheitstraße 9, D-28359 Bremen
[2] Hochschule Bremen, Flughafenallee 10, D-28199 Bremen

Inhalt

1. Motivation
2. Das SPIDER-Projekt
3. Smart-Metering-Szenario
4. Trusted Computing
5. Bewertung der Schutzverfahren
6. Anwendung der Schutzverfahren
7. Fazit und Ausblick

Motivation

Intelligente Energienetze

- Regulierung schwankender dezentraler Energieerzeugung
- Berücksichtigung variierender Interessen
- Transparenz für Endverbraucher
- Erfüllung gesetzlicher Vorgaben (deutsches EnWG §21-Gesetz)

Herausforderung für Sicherheit (intelligent ≠ sicher)

- Kritische Infrastrukturen müssen abgesichert werden können
- Personengebundene Daten müssen geschützt werden
- Herstellen von Vertrauen durch Sicherheitsmechanismen
- BSI definiert Sicherheitsanforderungen und Spezifikationen für kritische Infrastrukturen

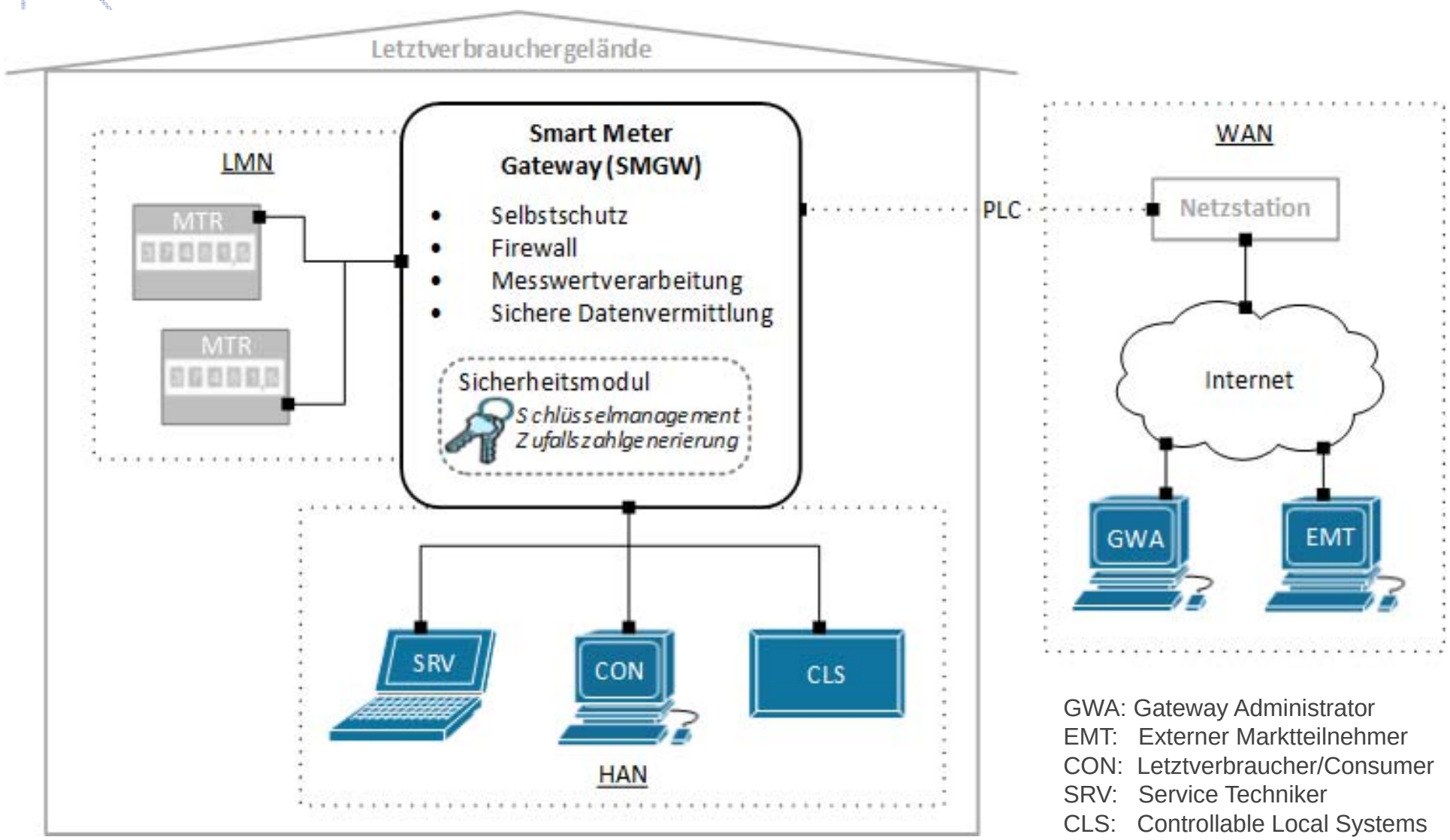
SPIDER-Projekt

- Sichere Powerline-Datenkommunikation im intelligenten Energienetz (SPIDER)
  - 2-Jahre-Projekt vom ZIM (BMWi)
  - Zeitdauer: 1. März 2013 bis 28. Februar 2015 (Verlängerung um drei Monate wird angestrebt)
  - Budget: 1,2 Millionen Euro
  - Projektziel: Entwicklung eines Smart Meter Gateway (SMGW) 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

Bundesministerium für Wirtschaft und Technologie

ZIM Zentrales Innovationsprogramm Mittelstand

Smart Meter Szenario (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

Smart Meter Szenario (2)

- **Local Metrological Network (LMN):** ein Netz zur lokalen Anbindung von Messgeräten (Strom-, Gas- oder Wasserzähler) der Endnutzer (Letztverbraucher, LV).
- **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).
- **Wide Area Network (WAN)**: ein Netz zur Anbindung des GWA für die SMGW-Verwaltung und autorisierter Dritter (EMT) zur Datenvermittlung

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 RFCs 5792, 5793, 6876, 7171 übernommen

TC-Spezifikationen

Trusted Platform Modul (TPM)

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

Trusted Network Connect (TNC)

- Systemintegritätsvalidierung entfernter Systeme (Remote Attestation)
- Authentifizierung und/oder Monitoring

STRIDE-Bewertung (1)

Spoofing (Authentifizierung)

- Verschlüsselung und Signaturen, Zeitstempel
- TC = TNC, TPM / BSI = Sicherheitsmodul

Tampering (Integrität)

- Verschlüsselung und Signaturen, Zeitstempel
- Systemzustandsprüfung
- TC = TPM, TNC / BSI = Sicherheitsmodul, Selbsttest

(Non)-**R**epudiation (Nichtabstreitbarkeit)

- Feste Systemidentität
- TC = TPM, TNC / BSI = Sicherheitsmodul

STRIDE-Bewertung (2)

Information Disclosure (Vetraulichkeit)

- Daten-/Transportverschlüsselung (TLS für Transport)
- TC = TPM, TNC / BSI = Sicherheitsmodul

Denial of Service (Verfügbarkeit)

- TPM und TNC nicht relevant
- BSI: priorisierte Geschäftslogik notwendig

Elevation of Privilege (Nichtabstreitbarkeit)

- Eingeschränkte Befehlssätze
- Rollen-/Profil-basierte Rechte
- TC = TPM, TNC / BSI = Sicherheitsmodul

Auffälligkeiten bei der Bewertung

Bundesamt für Sicherheit in der Informationstechnik

- Integration des Sicherheitsmoduls ist weniger stark
- Kein vertrauenswürdiges Bootverfahren spezifiziert
- Selbsttest ohne vertrauenswürdige Basis
- Selbsttest ohne Hardware (kein Root of Trust)

Trusted-Computing-Verfahren der TCG

- Kryptographische Verfahren für BSI ungenügend
- Spezifizierte Befehlssatz des BSI nicht passend
- Keine Maßnahmen gegen Denial-of-Service

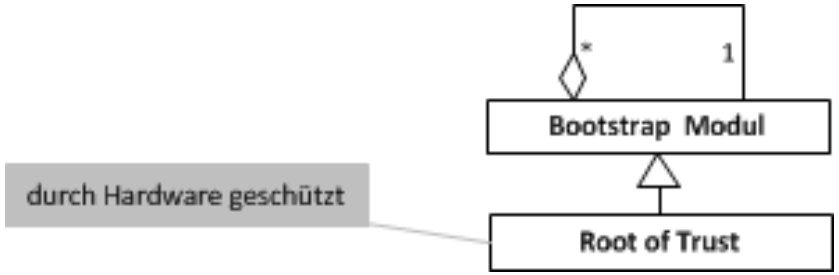
Schutzverfahren (1)

Aktuell ergeben sich zwei mögliche Szenarien

1. TNC, Security-Module und paralleler Einsatz eines TPM-Moduls in Version 1.2, inkl. Trusted Boot
   - Zusätzliche Kosten
   - Platzbedarf und Stromverbrauch der Hardware steigt

2. TNC, Security-Module und Implementierung des Secure-Boot-Verfahrens ohne TPM-Chip
   - Keine Integritätsmessung durch TPM
   - Integritätsmessung kann software-seitig erfolgen

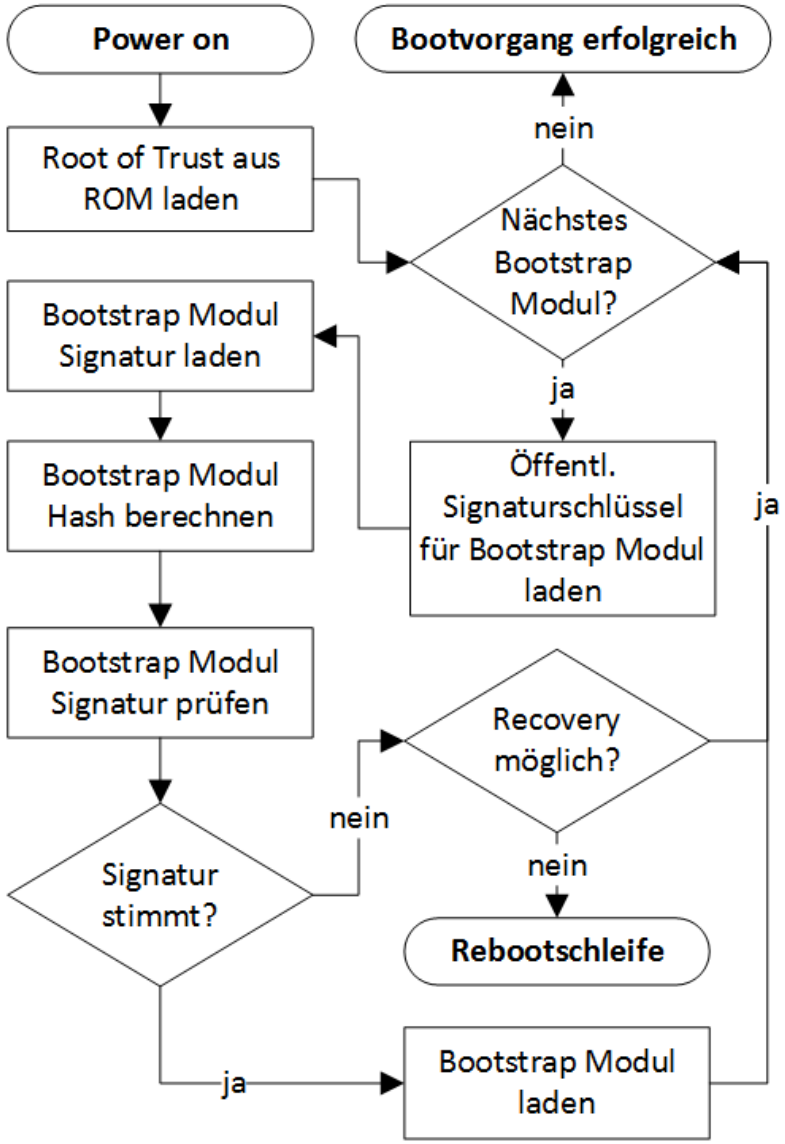
Schutzverfahren (2)



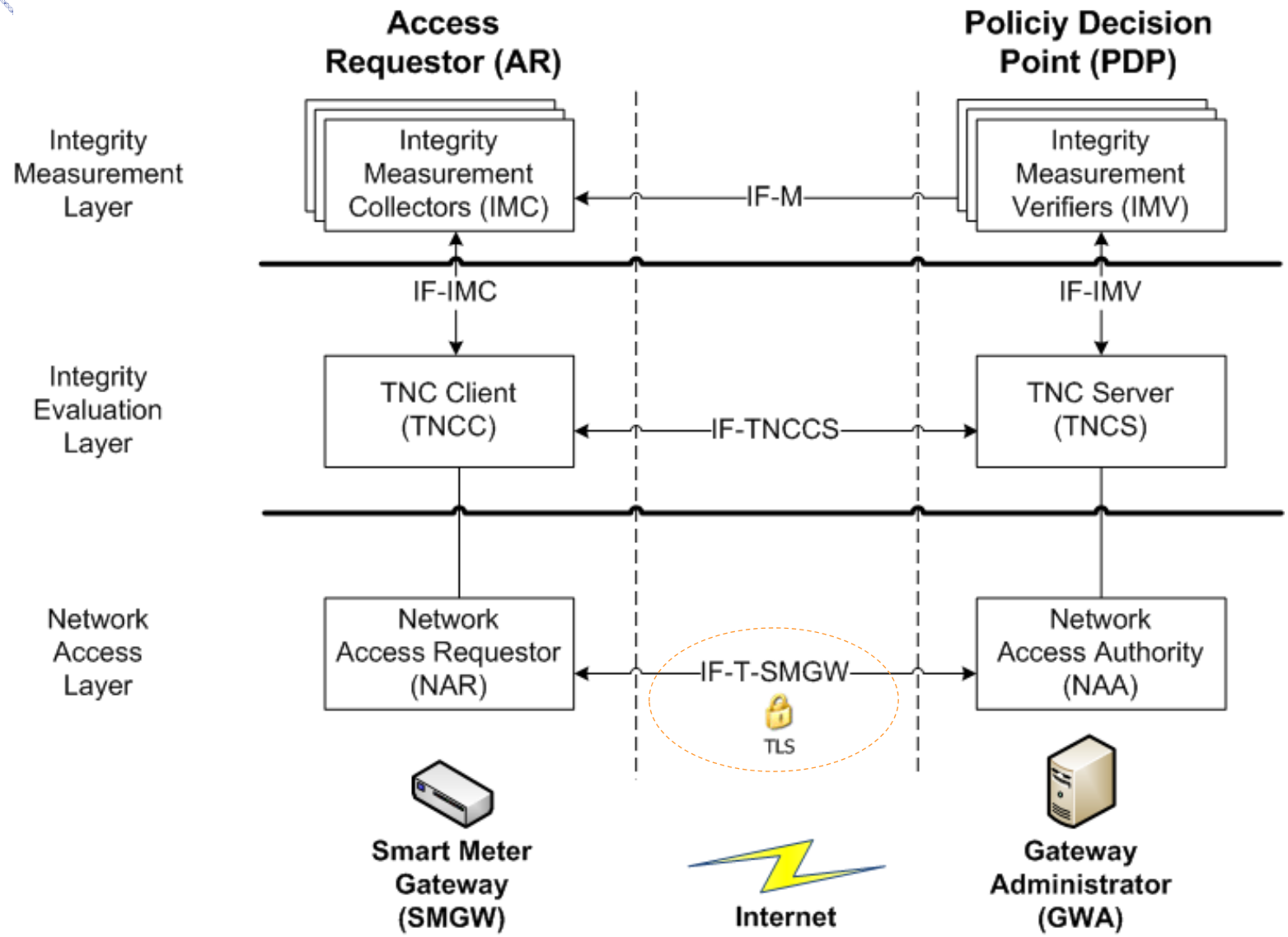
- Secure Boot Muster
  1. Secure Boot ermöglicht Prüfung und Reaktion (Hardware-Unterstützung z.B. durch ARM Trustzone)
  2. Root of Trust ist der Ausgangspunkt
  3. Definierte Vertrauenskette von Bootstrap-Modulen
  4. Andere Bootstrap-Module (z.B. Bootloader, Betriebssystem, Anwendung) werden nachgeladen

Secure-Boot-Ablauf

- Bootprozess
  1. Bootstrap-Modul suchen
  2. Öffentlichen Signaturschlüssel zu Modul suchen
  3. Definierte Signatur zum Modul suchen
  4. Bootstrap-Modul analysieren (Hash berechnen)
  5. Signatur und Hash vergleichen
  6. Wenn korrekt, laden
- Recovery = Partition mit alternativer Firmware (Resultat aus Update)
  1. Bootloader muss dazu valide sein
  2. Sonst sicherer Zustand (Reboot-Schleife)

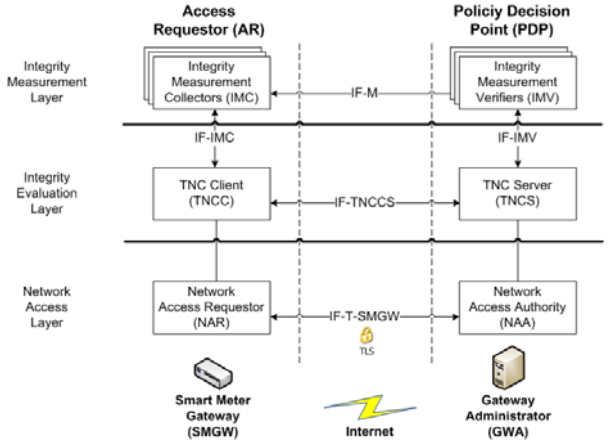


TNC-Architektur (1)



TNC-Architektur (2)

- Das SMGW fungiert als Network Access Requestor (NAR)
- Das GWA arbeitet als Network Access Authority (NAA)
- 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
- Eine TNC-Bibliotheken ist zur Realisierung vorhanden, jedoch aktuell nicht ausreichend (TNCCS 2.0)
- Alle Komponenten sind jedoch standardisiert
- IMC und IMV müssen durch den SMGW-Hersteller geliefert werden



TNC-Architektur (3)

- Besonderheit: IF-T-SMGW-Schnittstelle
  1. Für die Übertragung der Integritätsmesswerte vom SMGW zum GWA zur Verifizierung der Integrität sind derzeit keine Standards vorgesehen
  2. Vorhandene TNC-Standards passen nicht auf die BSI-Anforderung
  3. Gemäß TCG sind neue Standards für einzelnen Schnittstellen aber möglich
  4. BSI definierten Webservice für Alarm und Ereignismeldungen (wird im Projekt erst einmal verwendet)
- Erweiterung der TNC-Spezifikation
  1. Erweiterung der bestehenden Spezifikation wird aktuell erarbeitet
  2. Diese Erweiterung soll in den Standardisierungsprozess eingebettet werden
  3. Durch die TCG-Mitgliedschaft der DECOIT GmbH kann diese Möglichkeit direkt in der entsprechenden Arbeitsgruppe diskutiert werden

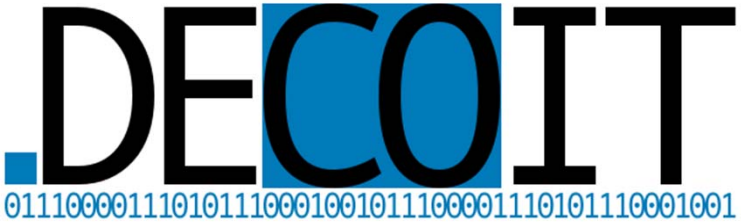
Fazit und Ausblick

Fazit

- Integritätsmessung und Attestierung ist möglich mit TC
  - Erhöhung der SMGW-Sicherheit
  - Verbesserung der Datenauthentizität
- Secure Boot ermöglicht vertrauenswürdige Systemprüfung

Ausblick

- Standardisierung der IF-T-SMGW-Schnittstelle ist in Arbeit
- Monitoring mit TNC Metadata Access Point (MAP) ermöglicht die Einbettung von SIEM-Lösungen in Smart Grids
- TPM 2.0 als Sicherheitsmodul verwenden



Vielen Dank für Ihre Aufmerksamkeit

Quellen

[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

Quellen

[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