Sicherheitskonzept zum Schutz der Gateway-Integrität in Smart Grids

Carl-Heinz Genzel[1], Richard Sethmann[2], Olav Hoffmann[3], Kai-Oliver Detken[4]

[1,2 und 3] Hochschule Bremen, Flughafenallee 10, 28199 Bremen
[4] DECOIT GmbH, Fahrenheitstraße 9, 28359 Bremen

Inhalt

Motivation

HOCHSCHULE BREMEN
UNIVERSITY OF APPLIED SCIENCES

.DECOIT

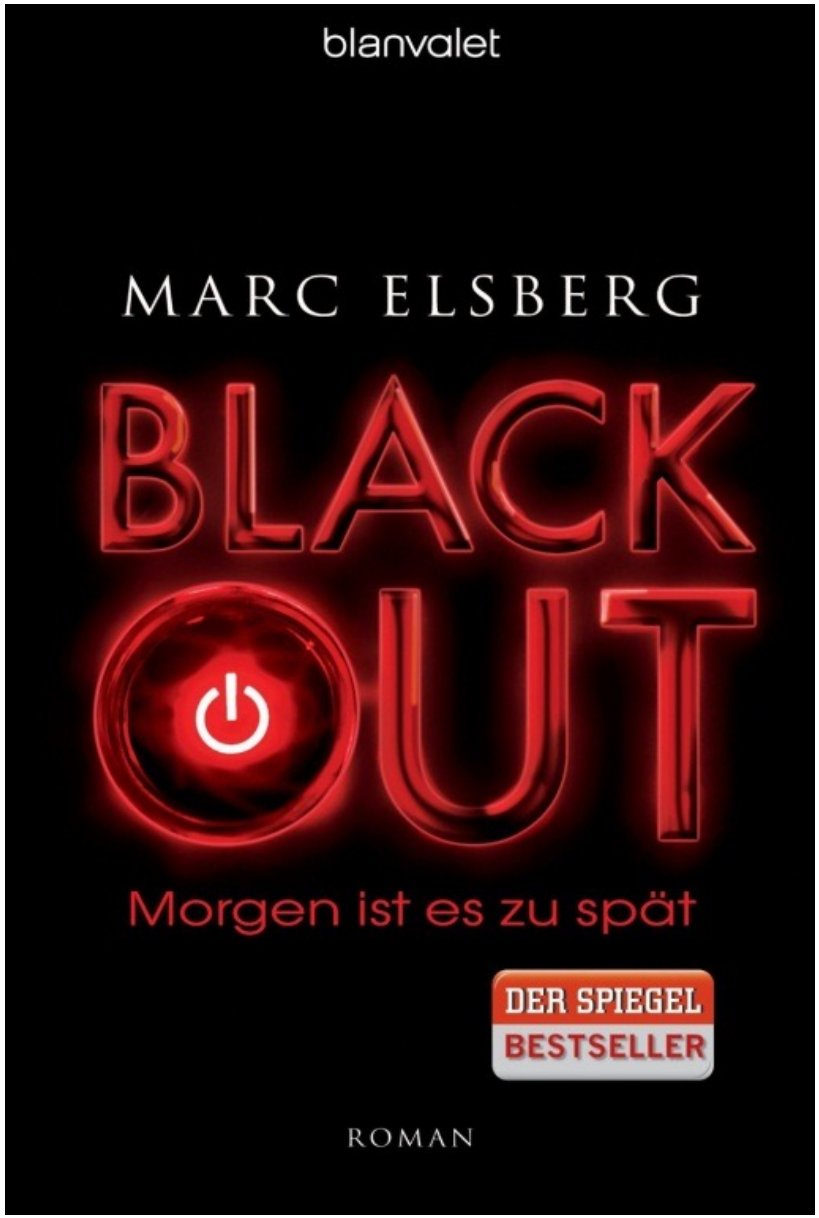
Energiemarkt im Wandel

- Schwankende dezentrale Energieerzeugung vs. Netzstabilität
- Berücksichtigung variierender Interessen
- Intelligent geregelte Energienetze notwendig
- EnWG §21 fordert intelligente Systeme

Intelligent ≠ Sicher

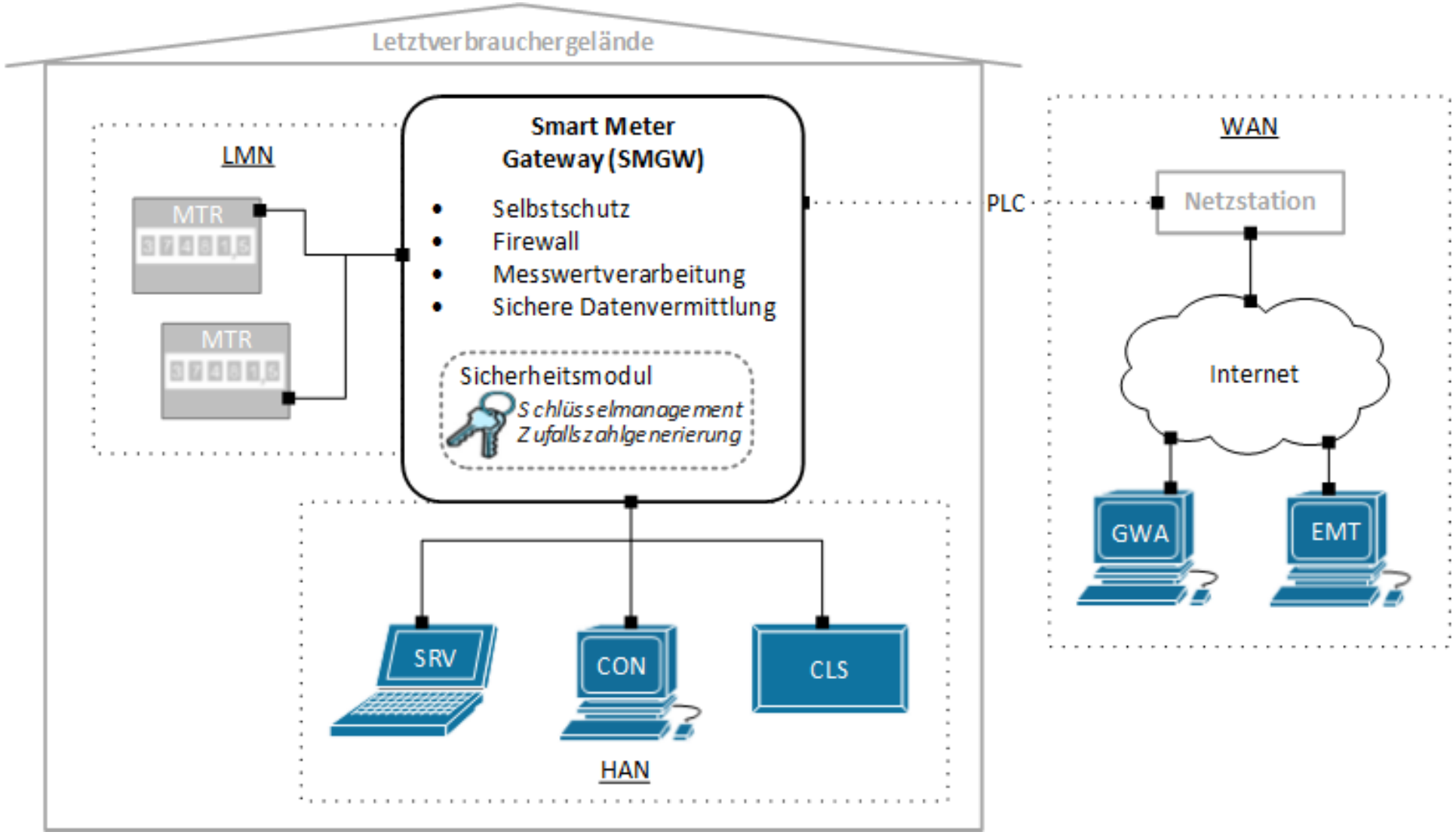
- Kritische Infrastruktur sichern
- Personengebundene Daten schützen
- Vertrauen schaffen

Motivation



Quelle: Blanvalet Taschenbuch Verlag

Smart Metering Szenario



Bedrohungsanalyse

HOCHSCHULE BREMEN
UNIVERSITY OF APPLIED SCIENCES

.DECOIT

Bedrohungskategorien

- Ausspähung der Infrastruktur durch Datenaufdeckung
- Betrug und Störung durch Datenmanipulation
- Beeinträchtigung durch Systemmanipulation
- Bedrohungsgewichtung
  - Angreifer im WAN → Hohe Motivation
  - Angreifer im HAN → Geringere Motivation

STRIDE-Ansatz - weitere Analyse nach Sicherheitseigenschaften

- SMGW-Integrität durch das BSI nur pauschal betrachtet

Trusted Computing der Trusted Computing Group

- Trusted Platform Module (TPM)
  - Hardwarebasierte Identität (Hardware-Vertrauensanker, Root of Trust)
  - Integritätsmessung der Hard- und Software
  - Vertrauenswürdiges Bootverfahren (Trusted Boot)

- Trusted Network Connect (TNC)
  - Systemintegritätsvalidierung (Remote Attestation)
  - Authentifizierung und/oder Monitoring

Vergleich der TC-Technologie mit BSI-Anforderungen

Eigenschaft	**Trusted Computing**	**BSI**
Identität	TPM (fest integriert, phys. Schutz vor Manipulation, priv. Schlüssel)	Security Modul (fest integriert, phys. Schutz vor Manipulation, priv. Schlüssel)
Zustandsmessung	TPM (Messung von Systemattributen und sichere Speicherung)	Selbsttests (Prüfung sicherheitsrelevanter Funktionen und Daten)
Integritätsprüfung	TNC (Remote Attestation)	Selbsttests (Prüfung sicherheitsrelevanter Funktionen und Daten)
Vertrauenswürdige Basis	Trusted Boot (Messung der Systemintegrität zur Startzeit, siehe Zustandsmessung)	k.A.

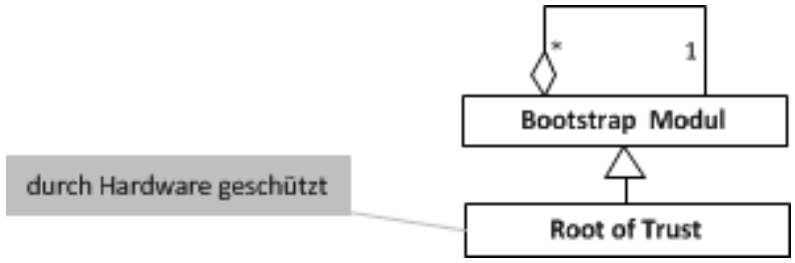
SMGW-Integrität

Sicherstellung der Hardware

- Passive Plombierung des Gehäuses
- Elektronischer Gehäuseöffnungssensor
- Tamper-Resistant-Grid für ausgesuchte Komponenten

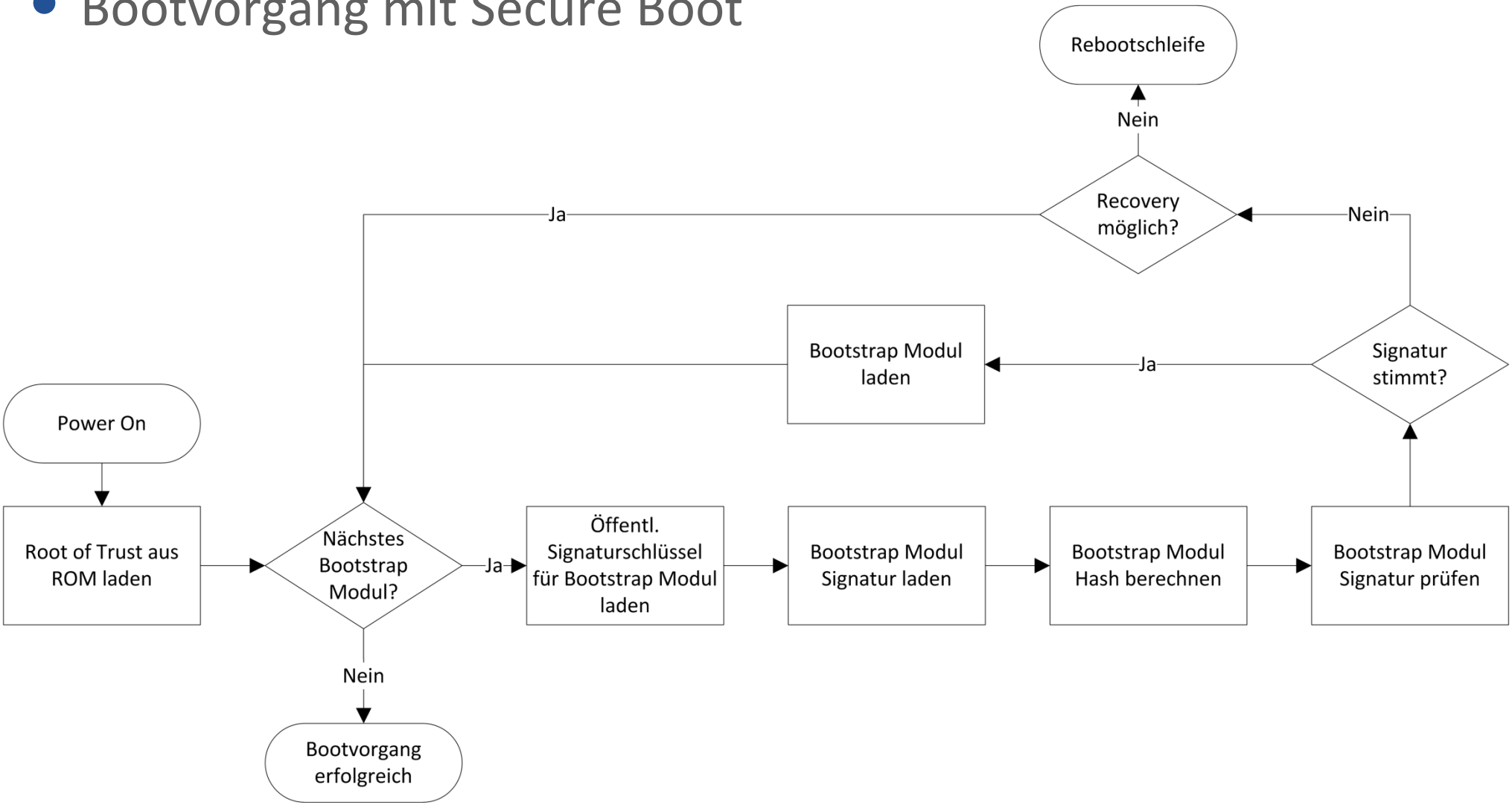
Sicherstellung der Basisintegrität

- Secure Boot und Root of Trust



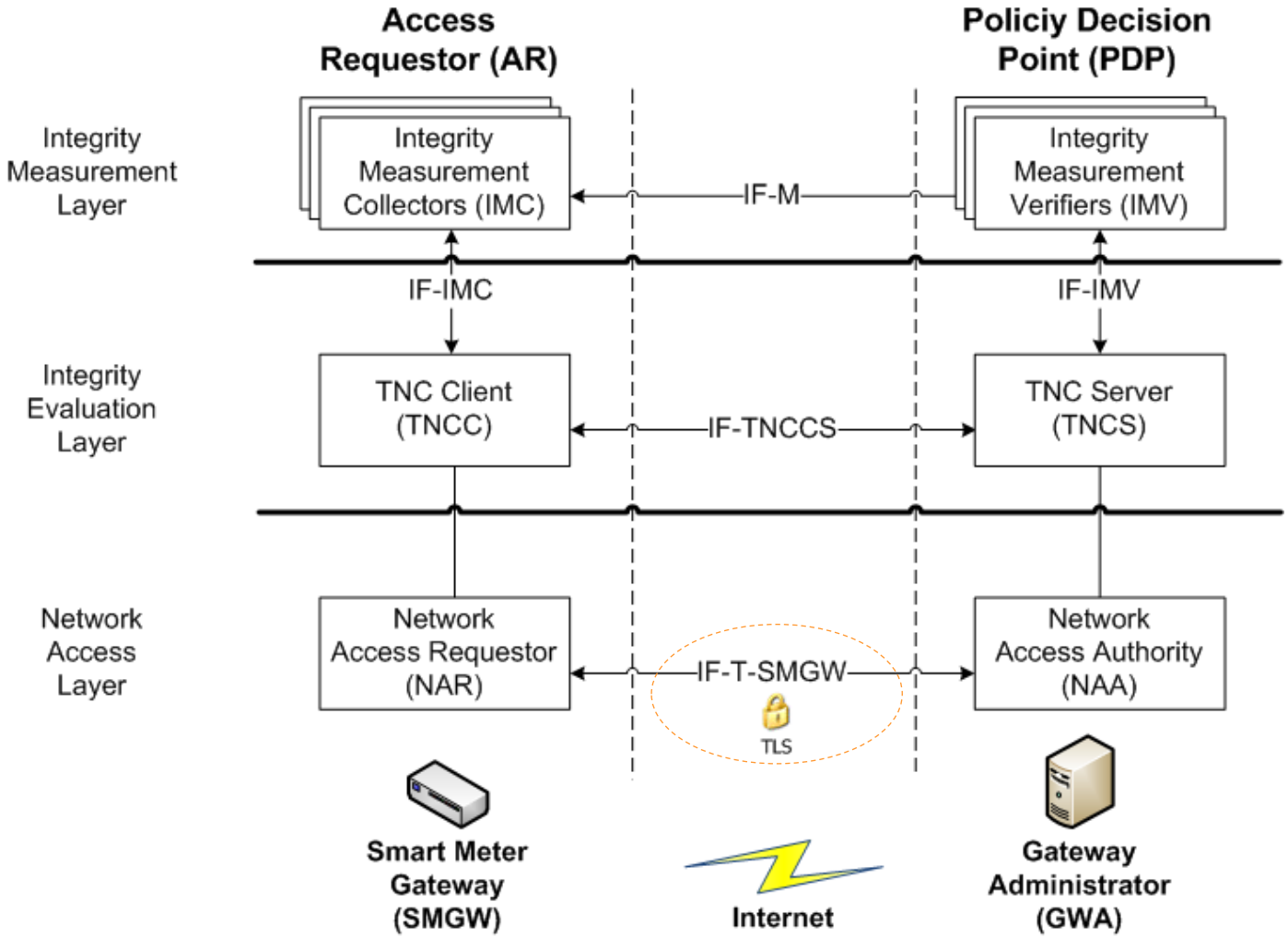
SMGW-Integrität

- Bootvorgang mit Secure Boot



SMGW-Integrität

Laufende Integritätsmessung (TNC)



Fazit und Ausblick

Fazit

- Integritätsmessung und Attestierung relevant
  - Erhöhung der SMGW Sicherheit
  - Verbesserung der Datenauthentizität
- Secure Boot ermöglicht Basisintegrität

Ausblick

- Standardisierung IF-T-SMGW Schnittstelle
- Monitoring mit TNC Metadata Access Point
- Zentrale Informationssammlung im Smart Grid mit Blick auf SIEM

Vielen Dank für die Aufmerksamkeit