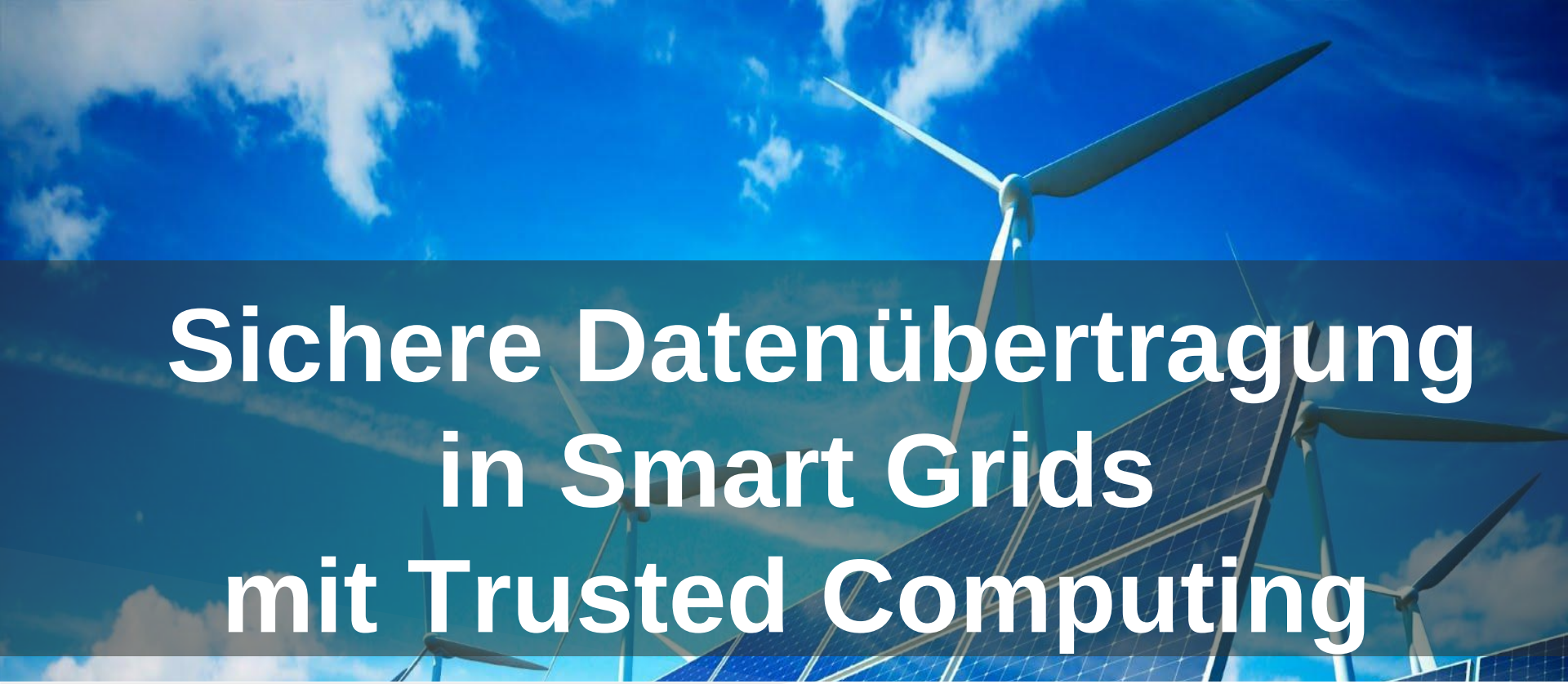


Sichere Datenübertragung in Smart Grids mit Trusted Computing

Prof. Dr. Richard Sethmann, Olav Hoffmann, Simon Busch

Institut für Informatik und Automation (IIA) der Hochschule Bremen

HOCHSCHULE BREMEN
UNIVERSITY OF APPLIED SCIENCES

Motivation und Zielsetzung

- Energienetze der Zukunft (Smart Grids)
  - Steuerung der Smart Grids über moderne IKT - Systeme
- System- und Sicherheitskonzept für Sichere Datenübertragung
  - Berücksichtigung der BSI Richtlinien
- Sicherstellung der Integrät in potentiell nicht vertrauenswürdiger Umgebung
  - Trusted Computing Ansatz verfolgen

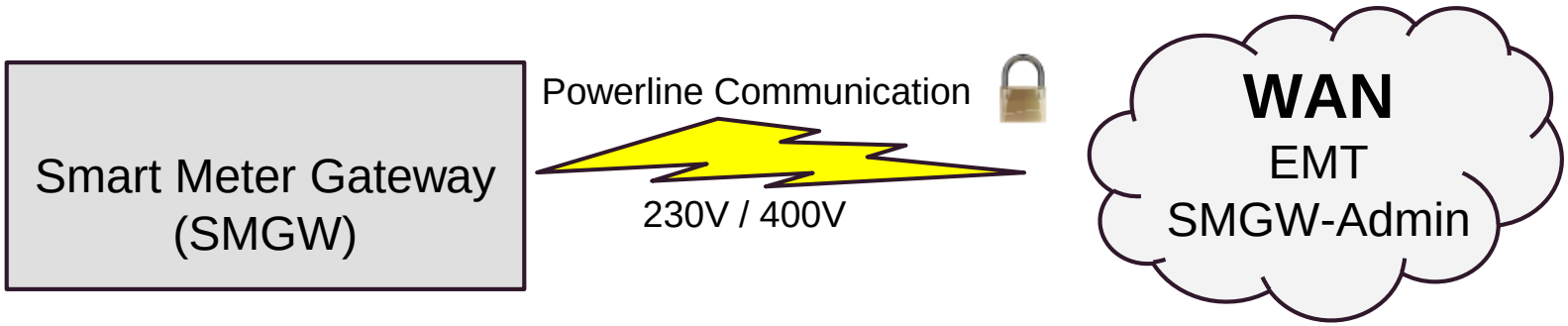
Agenda

- Systemumgebung
- Technische Richtlinie (TR) des BSI
- Sicherheitskonzept
- Demonstrator

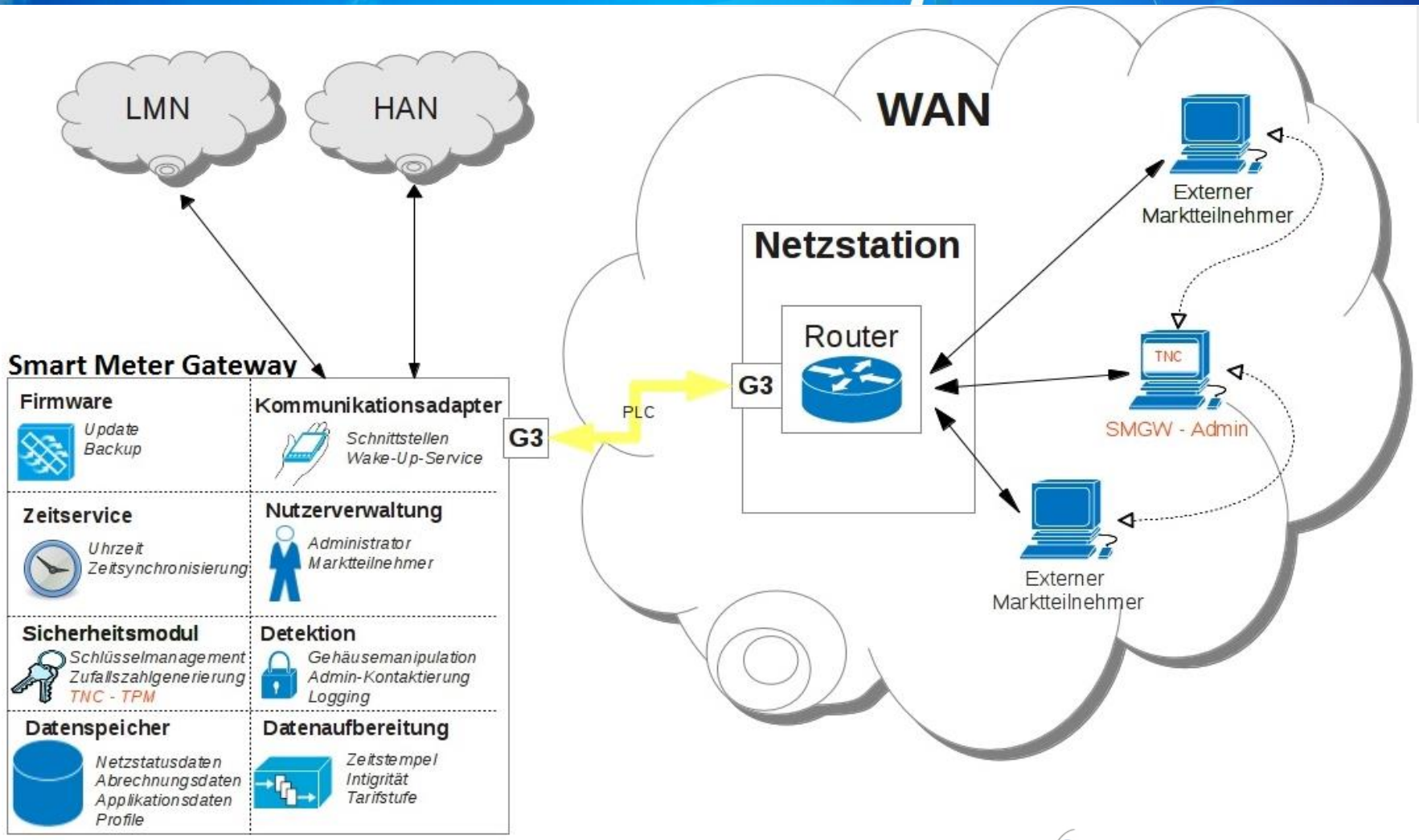
Systemumgebung

Systemumgebung

- Smart Meter Gateway (z. B. im Keller)
- Powerline Communication zur Netzstation
- Wide Aera Network zum SMGW-Admin bzw. Externen Marktteilnehmer (EMT)

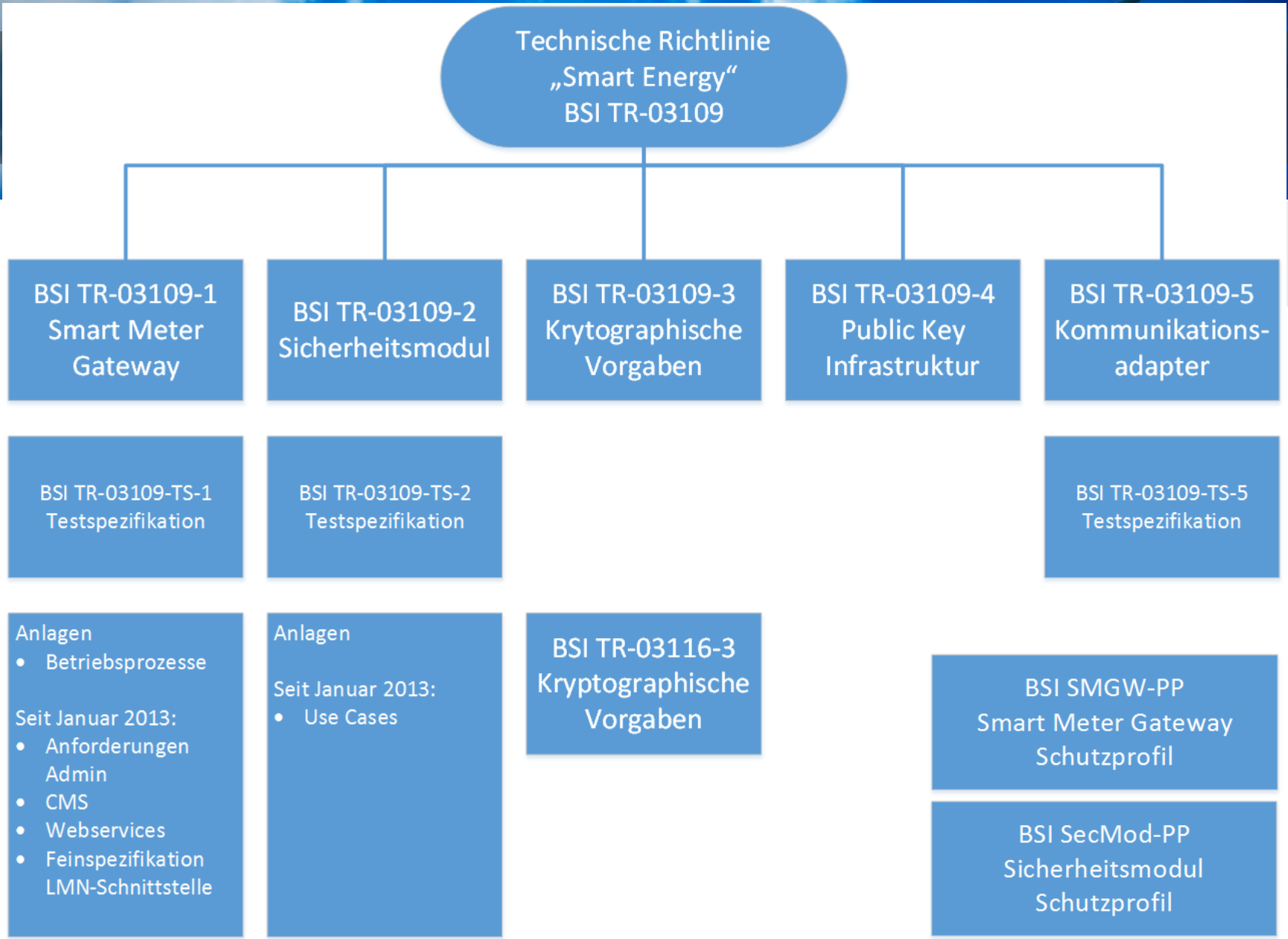


Systemumgebung



Technische Richtlinie des BSI

Bundesamt für Sicherheit in der Informationstechnik



BSI TR-03109, Dokumentenübersicht der berücksichtigten TR des BSI [Bund12a]

Technische Richtlinie des BSI

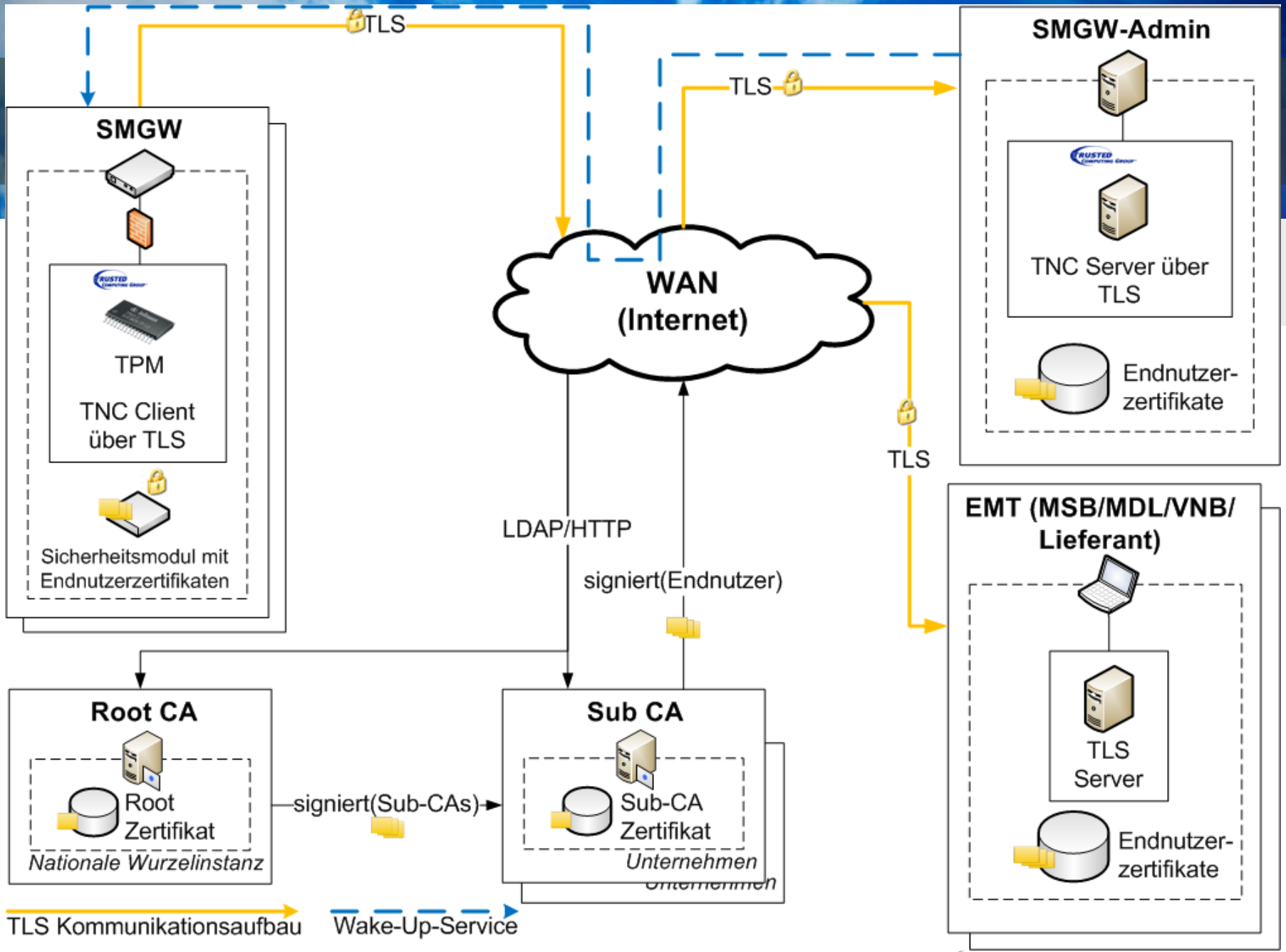
- Gesetz über die Elektrizitäts- und Gasversorgung (EnWG) - Energiewirtschaftsgesetz
  - §21e Abs. 2 Nr. 1 [EnWG05a]
  - §21i Abs. 1 Nr. 3 und Nr. 12 [EnWG05b]

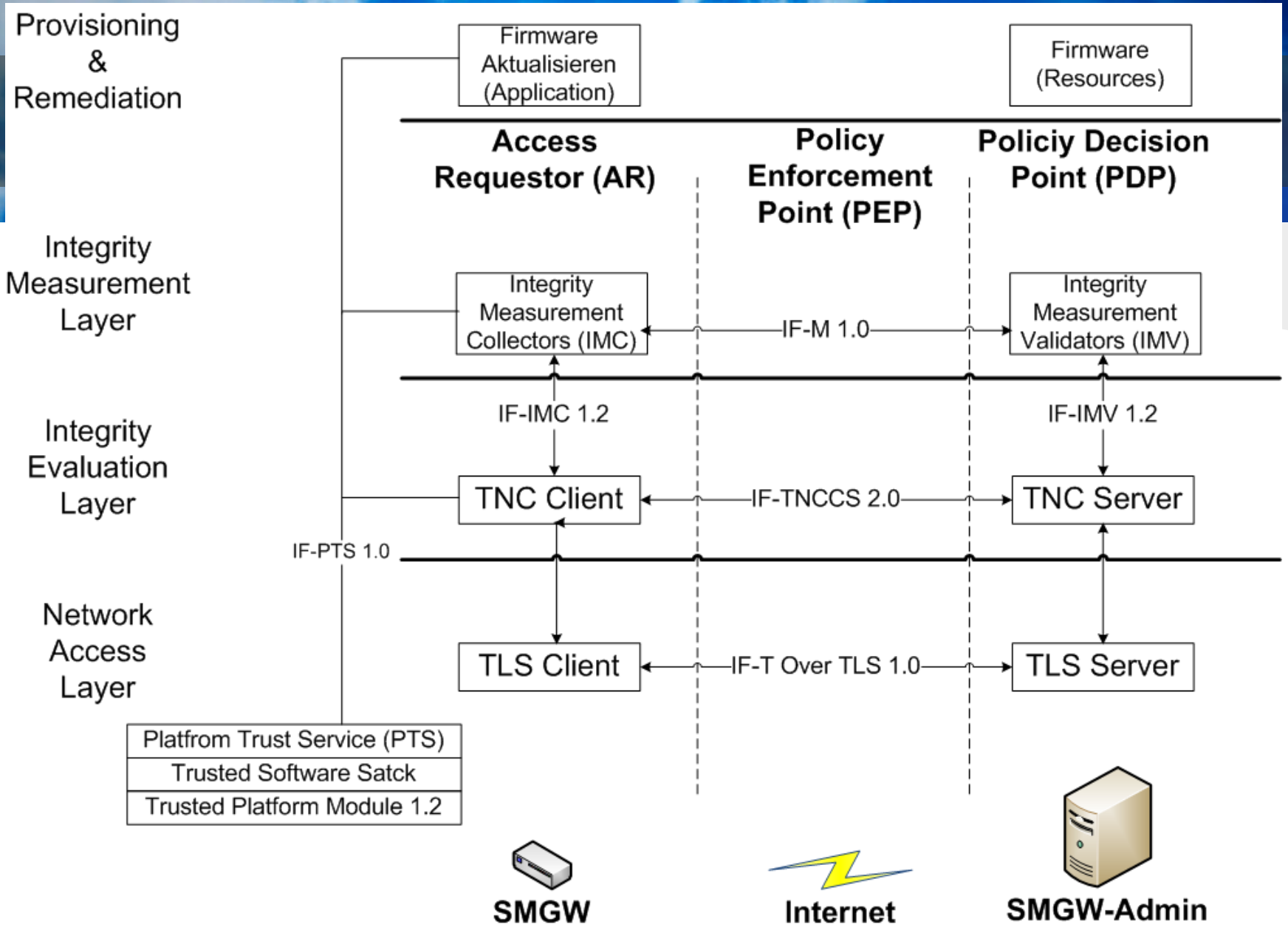
Sicherheitskonzept

Sicherheitskonzept

- Smart Meter Public Key Infrastructure (SM-PKI)
  - Authentizität durch hoheitlichen Vertrauensanker (Root CA)
  - Vertrauliche und integritätsgesichterte Kommunikation (TLS)

- Trusted Computing
  - Hardwaresicherheit durch Trusted Platform Module (TPM, Hardware-Vertrauensanker)
  - Integritätsmessung der Hard- und Software des SMGWs
  - Systemintegrität wird durch Trusted Network Connect (TNC) dem SMGW-Admin mitgeteilt (Remote Attestation)


TLS
SMGW
TPM
TNC Client über TLS
Sicherheitsmodul mit Endnutzerzertifikaten
WAN (Internet)
TLS
SMGW-Admin
TNC Server über TLS
Endnutzer-zertifikate
TLS
LDAP/HTTP
signiert(Endnutzer)
EMT (MSB/MDL/VNB/ Lieferant)
TLS Server
Endnutzer-zertifikate
Root CA
Root Zertifikat
Nationale Wurzelinstanz
signiert(Sub-CAs)
Sub CA
Sub-CA Zertifikat
Unternehmen
TLS Kommunikationsaufbau
Wake-Up-Service



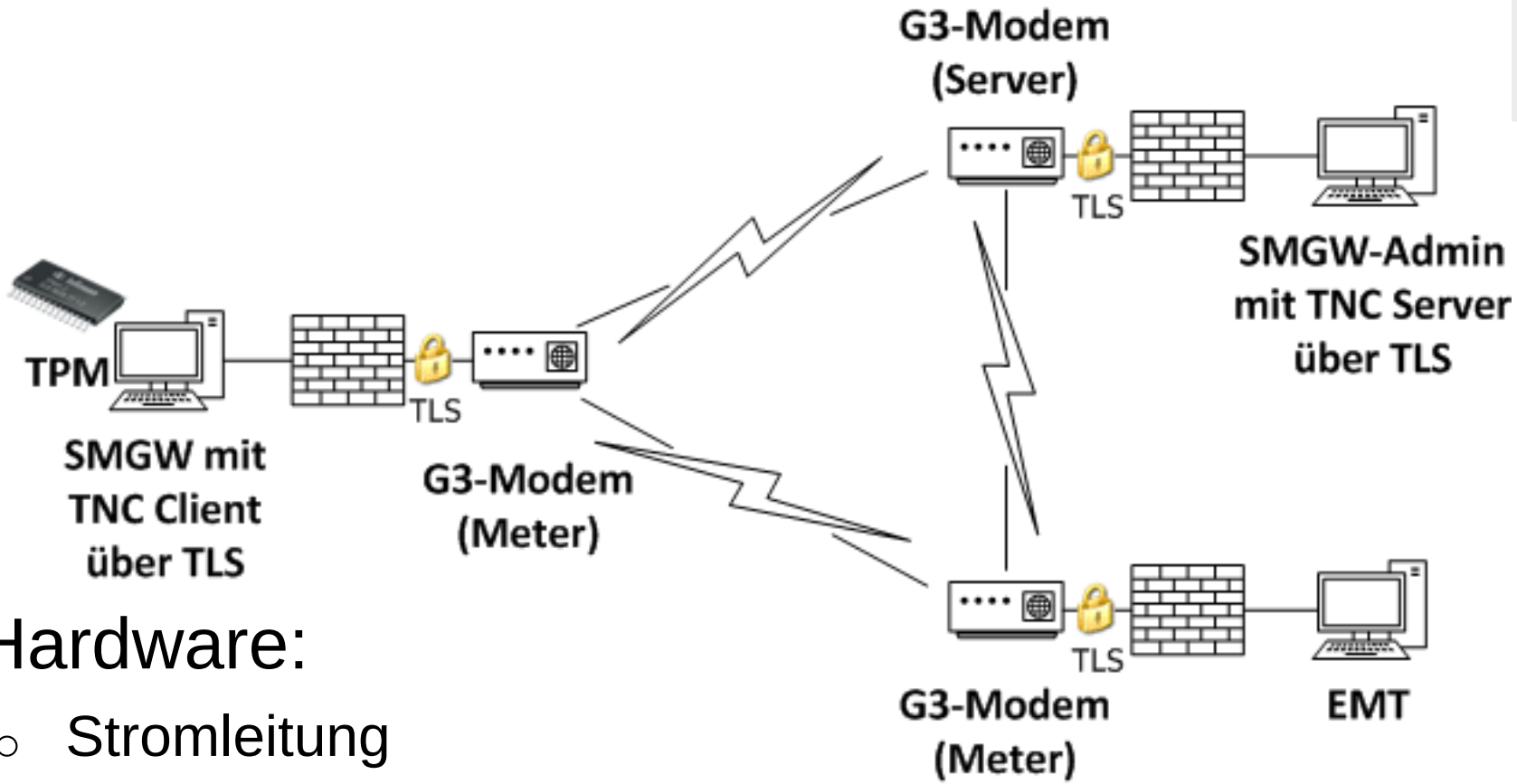
TNC-Schichtenmodell mit relevanten Komponenten des Systemkonzepts (In Anlehnung an [TCGr12a, Seite 13], Abb. 2)

Demonstrator

Demonstrator

- Intelligentes Verbrauchernetz: Abrechnungsdaten werden automatisiert an Stromanbieter geliefert
- Rollen
  - **Haushalt (Endabnehmer)** : bezieht Strom, zählt seinen Verbrauch, sendet seinen Verbrauch an den Anbieter
  - **Administrator:** verwaltet mehrere Haushalte und stellt deren Integrität sicher
  - **Externe Marktteilnehmer:** Empfang der Verbrauchsdaten des Endabnehmers

Demonstrator



Hardware:

- Stromleitung
- PLC-Modems der Firma Develo
- Darstellung der Rollen durch drei Laptops

Fazit

- Relevante Anforderungen des BSI im Systemkonzept umgesetzt
- Trusted Computing Ansatz mit TNC und TPM konform mit Technischer Richtlinie des BSI im Sicherheitskonzept umgesetzt
- Machbarkeit des Sicherheitskonzepts durch Demonstrator bewiesen

Ausblick

- Zukünftige Versionen der Technischen Richtlinie beachten
  - Aktueller Stand 18. März 2013 [Bund12b]
  - Anpassungen der kryptografischen Anforderungen in bestehenden Systemen aktualisieren
  - Herausforderung der zyklischen Erneuerung von Endnutzerzertifikaten

Quellen

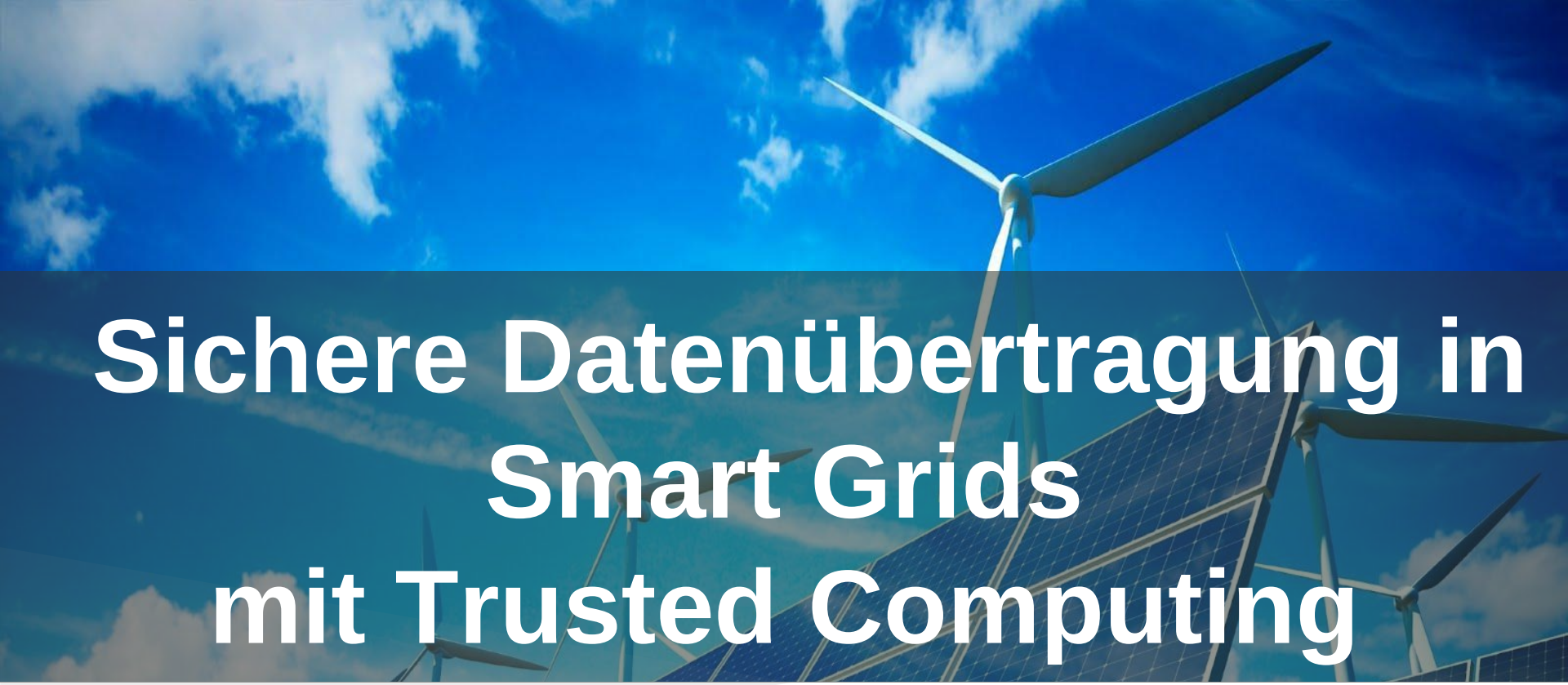
[Bund12a] Bundesamt für Sicherheit in der Informationstechnik. TR-03109 Smart Energy, Mai 2012. Version 0.50

[Bund12b] Bundesamt für Sicherheit in der Informationstechnik. TR-03109 Smart Energy, aktueller Stand der Technischen Richtlinie. https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html, zuletzt aufgerufen am 12.9.13

[EnWG05a] § 21e EnWG - Allgemeine Anforderungen an Messsysteme zur Erfassung elektrischer Energie. http://www.gesetze-im-internet.de/enwg_2005/__21e.html, zuletzt aufgerufen am 19.6.13

[EnWG05b] § 21i EnWG - Rechtsverordnungen. http://www.gesetze-iminternet.de/enwg_2005/__21i.html, zuletzt aufgerufen am 19.6.13

[TCGr12a] Trusted Computing Group. TCG Trusted Network Connect TNC Architecture for Interoperability, 2012. Revision 3



Sichere Datenübertragung in Smart Grids mit Trusted Computing

Vielen Dank für Ihre Aufmerksamkeit