„Privacy by design“ mit Hilfe von Schutzprofilen (BSI-Profil) bei Einsatz intelligenter Messsysteme

Workshop „Der Entwurf des Messstellenbetriebsgesetzes“
04. September 2015

Dr. Michael Schmidt
RWE Metering GmbH, Mülheim

VORWEG GEHEN

Agenda

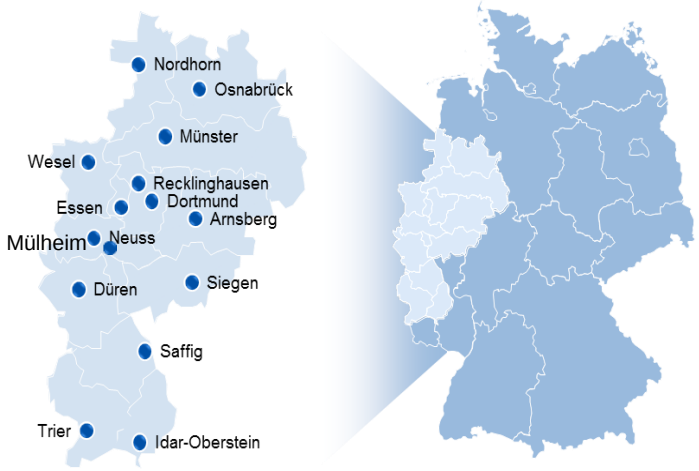
- Messsysteme und Schnittstellen
- Basisziele der IT-Sicherheit
- Normative Grundlagen
- Geschichte
- Common Criteria
- Schutzprofile
- Technische Richtlinien
  - Inhalte
  - Tarifanwendungsfälle
- Gateway
- Gateway Administrator
- PKI
- Herausforderungen
- Smart Metering in Europa

RWE Metering - größter deutscher Messdienstleister

Kennzahlen	
Umsatz	135 Mio. €
Mitarbeiter	550

Gemessene Energie ca.
100 TWh Strom
30 TWh Gas

Gerätebestände
ca. 5 Mio. Strom-, Gas-, Wasser- sowie Wärmezähler und sonstige Geräte



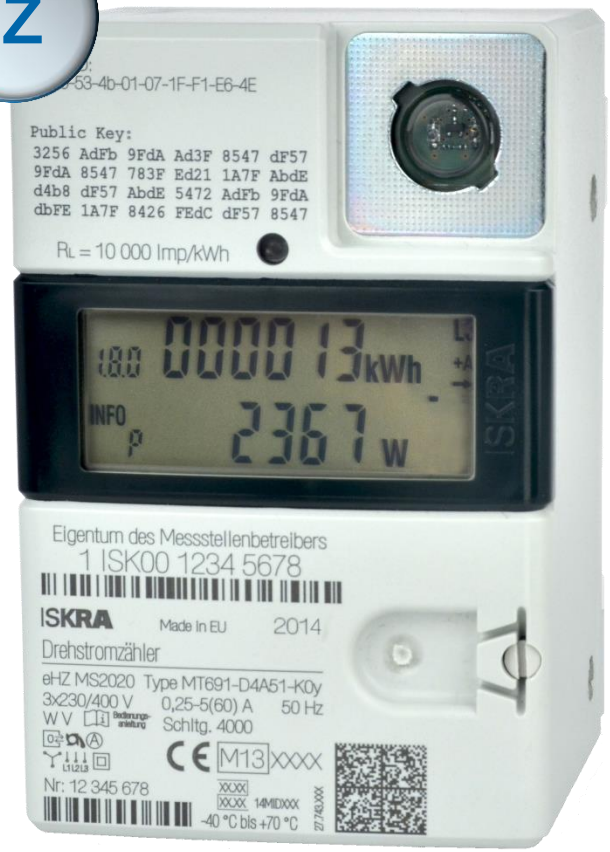
80 % - 95 %

FDL-Quote –100%→

Messstellenbetrieb	
Zählerwechsel	150.000 - 250.000
Stichprobenverlängerungen	1.070.000
	(Strom und Gas)
Messdienstleistung	
Ablesungen, Turnus	5.100.000
Ablesungen, aperiodisch	900.000
Fernauslesungen	125.000
Service	
Inkassogänge	150.000
Sperren/Entsperren	125.000
Leeranlagen-Recherche	140.000

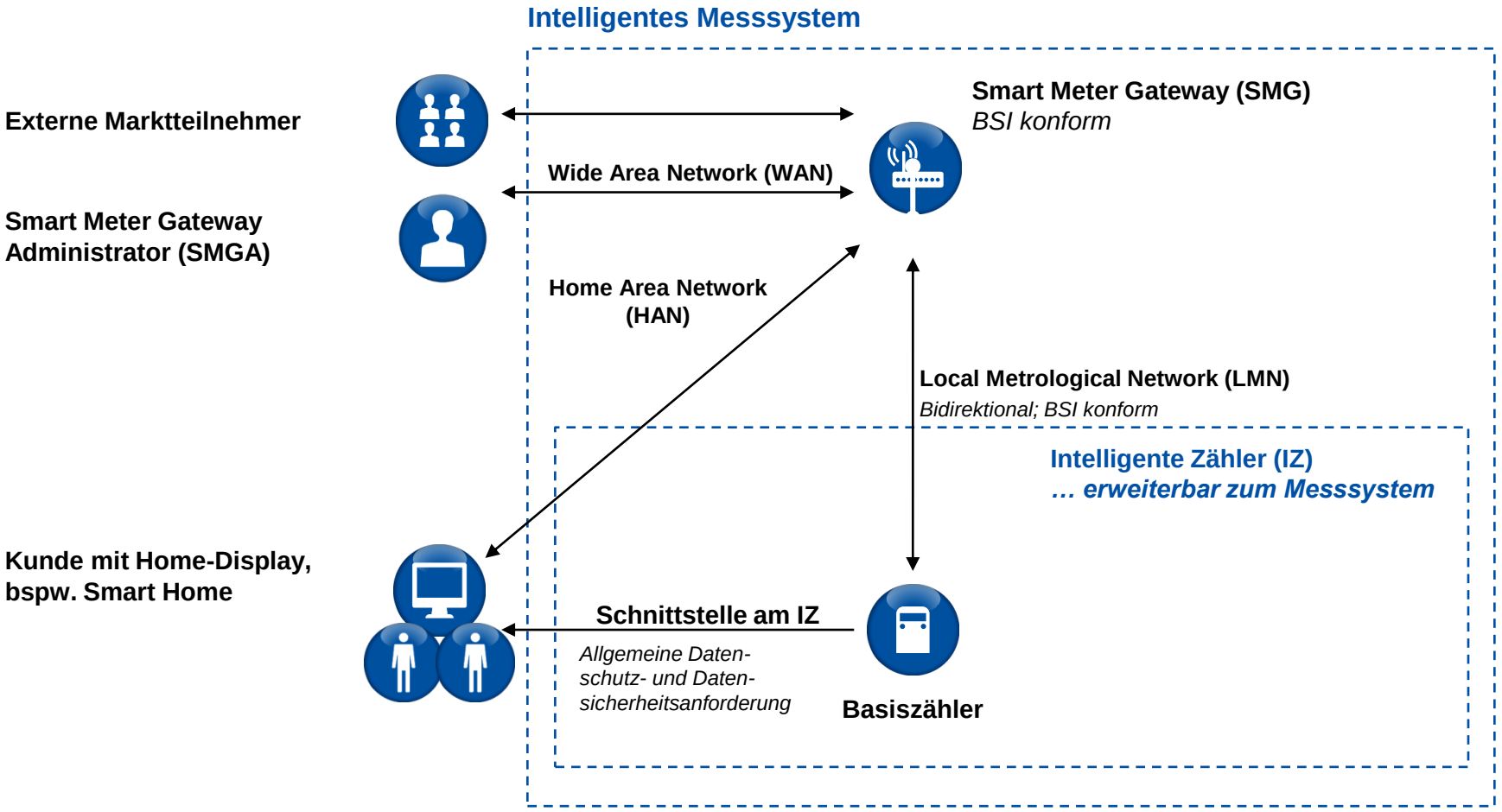
Das intelligente Messsystem
Einsatz im Labor

iZ

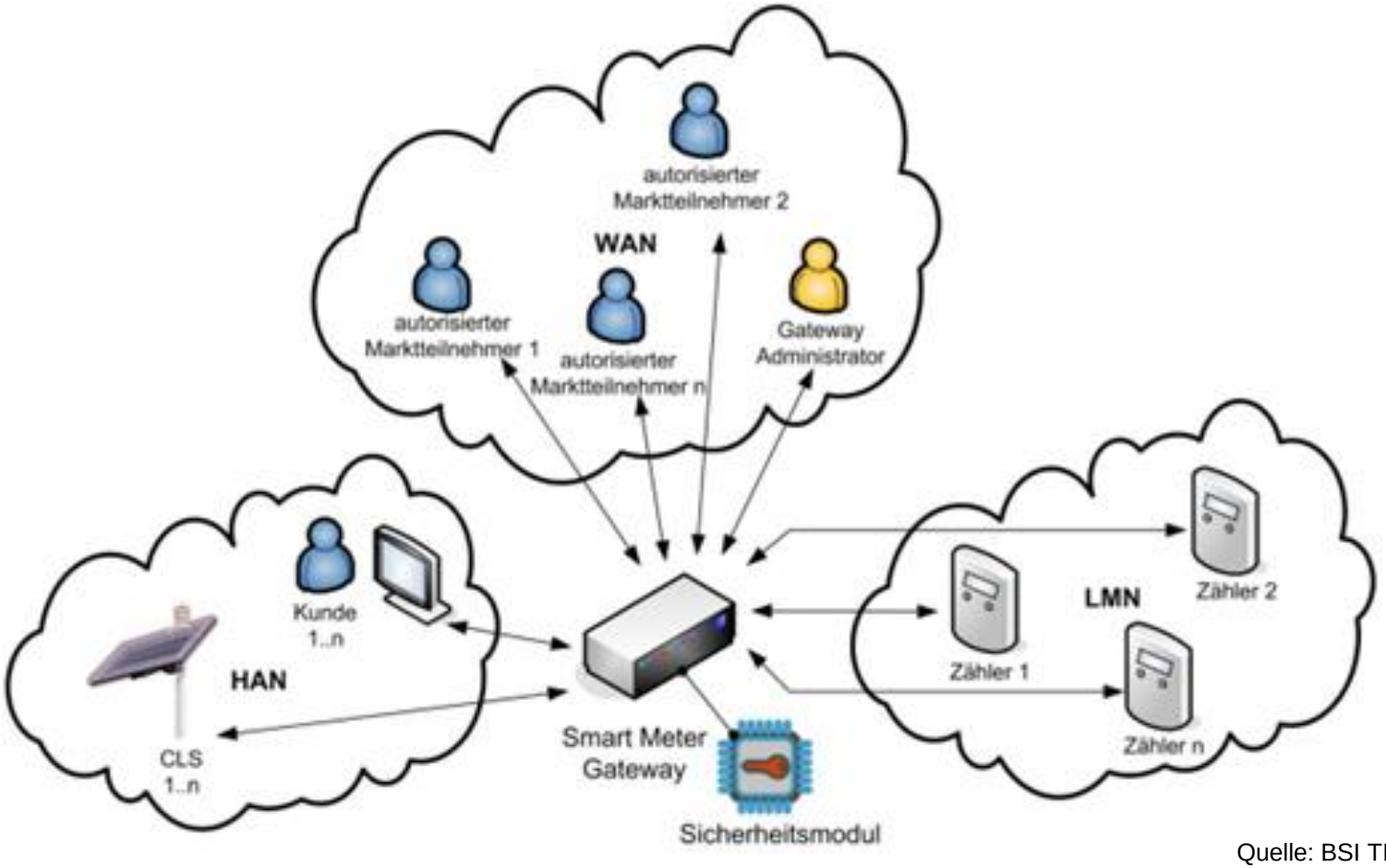


iM

Die Einführung von Smart Metern beinhaltet neben neuer Technologien auch neue Marktrollen im Zählerwesen



Das intelligente Messsystem
Smart Meter Gateway mit Schnittstellen



Quelle: BSI TR 03109-1

Basisschutzziele

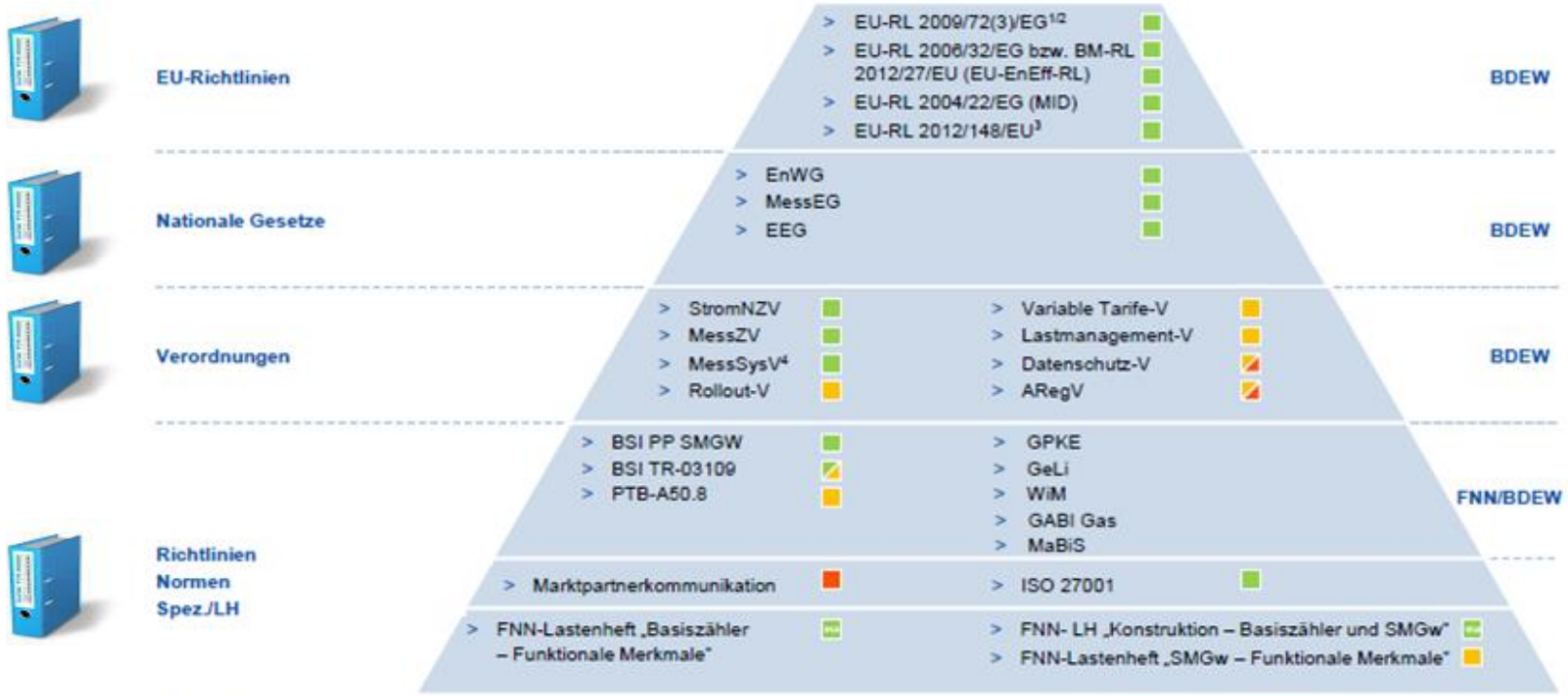
Security - Schutz vor Angriffen auf die Infrastruktur
Safety - Sicherstellung der Betriebssicherheit
Privacy - Datenschutz

→ Vertraulichkeit
Integrität
Verfügbarkeit

→ Authentizität
Verbindlichkeit
Autorisation

Normative Grundlagen

Überblick über wichtige Regelwerke… …und die Beteiligung in den Verbänden



[1] EU-RL für den Elektrizitätsbinnenmarkt
[2] EU-RL für den Erdgasbinnenmarkt
[3] Empfehlung (2012/45/EU) der Kommission von 9. März 2013 zu Vorbereitungen für die Einführung intelligenter Messsysteme
[4] Stand 07.10: EU-Notifizierungsverfahren abgeschlossen
Dr. Markus Gerdes, BTC Network Forum Energie 2013, 16.10.2013, Münster

Geschichte

- Bildung nationaler Standards durch Spionageabwehr und Militär – 1980
- Ausdehnung auf andere Bereiche z.B. Verwaltung und Wirtschaft
- „Demilitarisierung“
- 1991 Gründung BSI (vormals Abteilung BND)
- Supranationale Standards (CC) 1993 seit 1999 ISO Standard

Common Criteria

Zwischenstaatliches Abkommen und ISO Norm

7 Sicherheitslevel
Beschreibung von Funktionen und Sicherheiten
Methoden und Methodenvorgaben

Geschichte
Schutzbedarfsdefinitionen einzelner Staaten
USA, Kanada, Niederlande, Frankreich, Deutschland
durch Sicherheitsbehörden z.B. NSA und BND Abt. BSI
vereinheitlicht zu CC
Gegenseitige Anerkennung von Zertifizierungen (Level 1-4)
zus. Europäische Abkommen → Anerkennung höherer Level
Freiwillige oder verpflichtende Zertifizierung
z.B. § 21 e Abs. 4 EnWG

Prüfung nach CC ist ein formaler und aufwendiger Prozess

CC – Allgemeines Modell

Assets

- Informationen, Daten, Systeme u.a.

Bedrohungen

- Agent, feindliche Handlungen

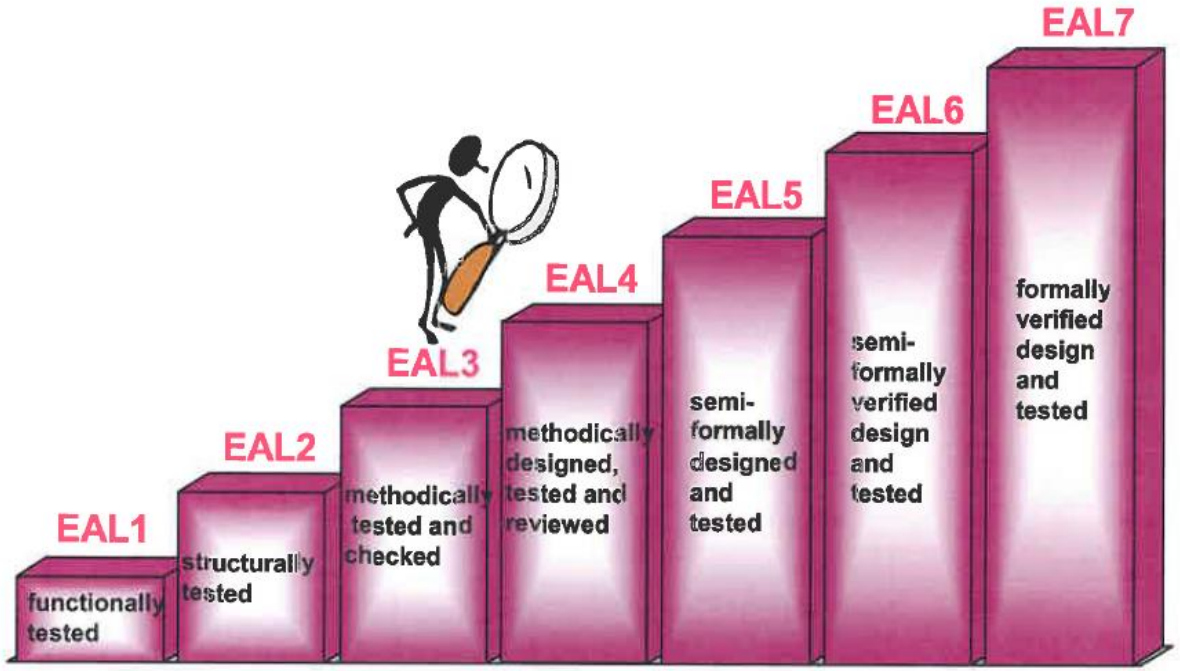
Gegenmaßnahmen

- Sicherheitsmechanismen zum Schutz von Assets
- Sicherheitsmaßnahmen in der Asset Umgebung

Assurance

- Vertrauen in Umfang und Wirksamkeit der Gegenmaßnahmen
  durch PP-Evaluation
  TOE-Evaluation
  Design, Verletzlichkeitsprüfung
  ggf. Vor-Ort-Besuche

CC - Evaluation Assurance Level (EAL)



Schutzprofil – Protection Profile

PP Gateway
PP Sicherheitsmodul

Basiert auf Common Criteria
Umfang und Schutzlevel richten sich nach dem Anwendungsbereich z.B. private versus öffentliche oder militärische Archivierungssysteme

- Angriffsszenarien und –punkte werden ermittelt, Schadensmöglichkeiten und –umfänge, Folgeschäden
- PP sind grds. technikneutral

Schutzprofil (PP)

Welche Schutzmechanismen braucht ein Produkt (SW/HW)?
Entscheidend ist der Einsatzbereich, z.B.:

Bürokommunikation
- Privat
- Kleingewerbe
- EVU, Bank
- Öff-Verwaltung
- Bundestag, Militär, BK

Prozesskommunikation
- Privat
- EVU
- Militär

Aus CC wird erforderliche (Funktionalität) und Qualität, d.h. Umfang und Prüftiefe ermittelt.
BSI ermittelt PP und zertifiziert Produkte die PP erreichen.

Rechtsnatur: Grds. unverbindliche Empfehlungen, es sei denn Bedarfsanwender bestimmt etwas anderes.

Aufbau PP

- Einleitung
- TOE – das Gateway
- Konformitätserklärungen
- Sicherheitsprobleme
  -- Beteiligte
  -- Gegenstand (Assets)
  -- Annahmen
  -- Bedrohungen
  -- Organisatorische Sicherheit
  (Zugriffsrechte, Dokumentation)
- Sicherheitsziele
  -- Gateway
  -- Umwelt und Beteiligte
- Maßnahmen und Sicherheitserfordernisse (an den Schnittstellen)

PP Smart Meter Gateway

- Bedrohungen
- Veränderungen lokaler Daten
- Veränderungen via WAN
- Veränderung SMGW-Zeit
- Offenlegung von Daten lokal (IF_MTR_GW)
- Offenlegung auf der WAN-Strecke
- Übernahme Kontrolle von SMGW, Zähler oder CLS
- Zugriff auf gespeicherte Daten
- Zugriff auf nicht mehr benötigte Daten
- Verletzung der Vertraulichkeit (Privacy)

Maßnahmen

- Sicherheitsmodul (eigenes PP)
  für (vereinfacht) PKI
- Diverse Log-Dateien und Zugriffsregelungen
- Firewallfunktion des SMGW
- Getrennte physische Schnittstellen
- Verschleierung
- Schutz der Kommunikation, sichere Speicherung, Pseudonymisierung
- Kryptographischer Schutz der Schnittstellen
  z.B. durch Zertifikate
- Zeitstempel und sichere Zeitsynchronisation (mit PTB)
- Vorgaben für Lagerhaltung, Aufhängung, Bedienungsanleitung für MSB u.a.
- u.a.

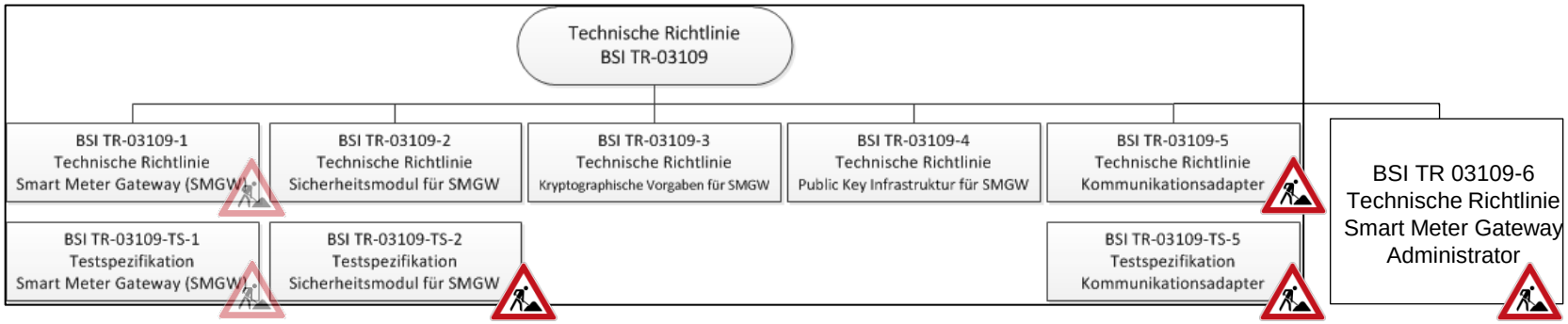
Sicherung der Schnittstellen

- Durch Vorgabe der Protokoll-(stacks)
- Durch TLS- Kommunikationskanäle, d.h.
  -- beidseitige Authentisierung mittels Zertifikaten durch Sender und Empfänger
  -- Verschlüsselung
  (detaillierte, komplexe Vorgaben in TR)

Technische Richtlinien

- Rechtsnatur siehe PP
- Geben Maßnahmen vor, wie PP umgesetzt werden muss oder ggf. kann
- Beschreiben Prozesse und Schutzanforderungen an die Prozesse und Werkzeuge (Asset)
- Sind i.d.R. technologieoffen
- Sorgen ggf. für Interoperabilität z.B. Protokollvorgaben
- Beschreiben PKI
- Beschreiben Schnittstellen
- Regeln u.a.
  - Testspezifikationen
  - Schnittstellen
  - Funktionen
  - Interoperabilität

Die Technische Richtlinie (BSI TR 03109)*



*) Basierend auf Quelle www.bsi.bund.de Smart Metering Systems

Version veröffentlicht, Fortschreibung angekündigt

Dokument z. Z. nicht vorhanden bzw. nicht allgemein veröffentlicht

Die Technische Richtlinie (BSI TR 03109)

1. **Basisrichtlinie**
2. **TR – 1 SMGW**
   - Es muss verschlüsselt werden
   - Interoperabilität
   - TAF
   - Information des Kunden (HAN-Schnittstelle, Display)
   - Selbstgenerierte Zertifikate gem. internationalen Normen
3. **TR – 2 Sicherheitsmodul**
   - Welches Stück Hardware vermittelt die Sicherheit – Kryptochip
4. **TR – 3 Kryptographische Vorgaben**
   - Wie wird verschlüsselt (Mathematik);
     Vorgabe Verfahren, z.B. asymmetrische Verschlüsselung
5. **TR – 4 PKI**
   - Wie komme ich an den Schlüssel und die Zertifikate?
     Spielregeln der Teilnehmer an PKI
6. **TR - 5 Kommunikationsadapter**
7. **TR - 6 Aufgaben, Rechte und Pflichten des SMGWA zurzeit in Bearbeitung**

Die Anwendungsfälle für die Tarifierung und Bilanzierung (TAF) gemäß TR 03109-1

- **TAF1: Datensparsame Tarife (nach § 40 (5) EnWG)**
- **TAF2: Zeitvariable Tarife (nach § 40 (5) EnWG)**
- **TAF3: Lastvariable Tarife**
- **TAF4: Verbrauchsvariable Tarife**
- **TAF5: Ereignisvariable Tarife**
- **TAF6: Abruf von Messwerten im Bedarfsfall**
- **TAF7: Zählerstandsgangmessung**
- **TAF8: Erfassung von Extremwerten für Leistung**
- **TAF9: Abruf der Ist-Einspeisung einer Erzeugungsanlage**
- **TAF10: Abruf von Netzzustandsdaten**
- **TAF11: Steuerung von unterbrechbaren Verbrauchseinrichtungen und Erzeugungsanlagen**
- **TAF12: Prepaid Tarif**
- **TAF13: Bereitstellung von Messwertsätzen zur Visualisierung für den Letztverbraucher über die WAN-Schnittstelle**

PP und TR-Reichweite beim Lebenszyklus des Gateways

- Entwicklung
- Produktion
- Vor-Personalisierung 1 (PKI-Vorbereitung Sicherheitsmodul)
- Vor-Personalisierung 2 und Integration Sicherheitsmodul
- Installation und Inbetriebnahme
- Personalisierung
- Betrieb
- Umfasst (ggf.) Vorschriften zur Dokumentation, zum Transport, Lager usw.

Gateway – Funktionen/Aufgaben

- Zentraler Datenspeicher
- (Teil)-übertragung nur an berechtigte EMT
  Grundsatz der Datensparsamkeit
- Tarifierung im GW verpflichtend (TAF)
- Zeitsynchronisation
- Logbücher
- Aufbau Datenkommunikation
  kein EMT kann eine Verbindung aufbauen
- Signatur (Authentizität und Integrität)
- Mandantenverwaltung
- Ver- und Entschlüsselung aller Daten
- Verbindungsaufbau

SMGW Administrator – Aufgaben

- Fordert Verbindungsaufbau durch Gateway an
- Kann Logbücher einsehen (nicht Kunden-Log)
- Organisiert mit Gateway Software Updates, Lieferantenwechsel, Tarifprofile
- Bietet TLS-Kanäle an
  - Ende-zu-Ende Verschlüsselung
  - Sicherung der Integrität und Authentizität

PKI

Public Key Infrastructure

= Asymmetrisches auf Zusammenspiel von öffentlichen und privaten Schlüsseln beruhendes Verschlüsselungs-verfahren

Zweck

- Sicherheit der Verschlüsselung (Methode)
- Sicherung der Integrität der Nachricht (Hash-Funktionen)
- Sicherstellung der Authentizität von Sender und Empfänger (Zertifikate)
- Sicherheit der Übertragung (TLS)

Root Certificate Authority (CA)

- Vertrauensanker der Sicherheit und Authentizität
- Zuständig BSI (durchgeführt T-Systems)
- Abgeleitet von Root CA ist Sub CA
- Betreiber: verschiedene zertifizierte Unternehmen
- Delegiert Aufgaben an Sub-CA Halter
- Risikostreuung und -minimierung

Herausforderungen im Smart Metering

- Definition und Umsetzung der HAN-Schnittstelle
- Integration der Steuerbox
- Telekommunikation

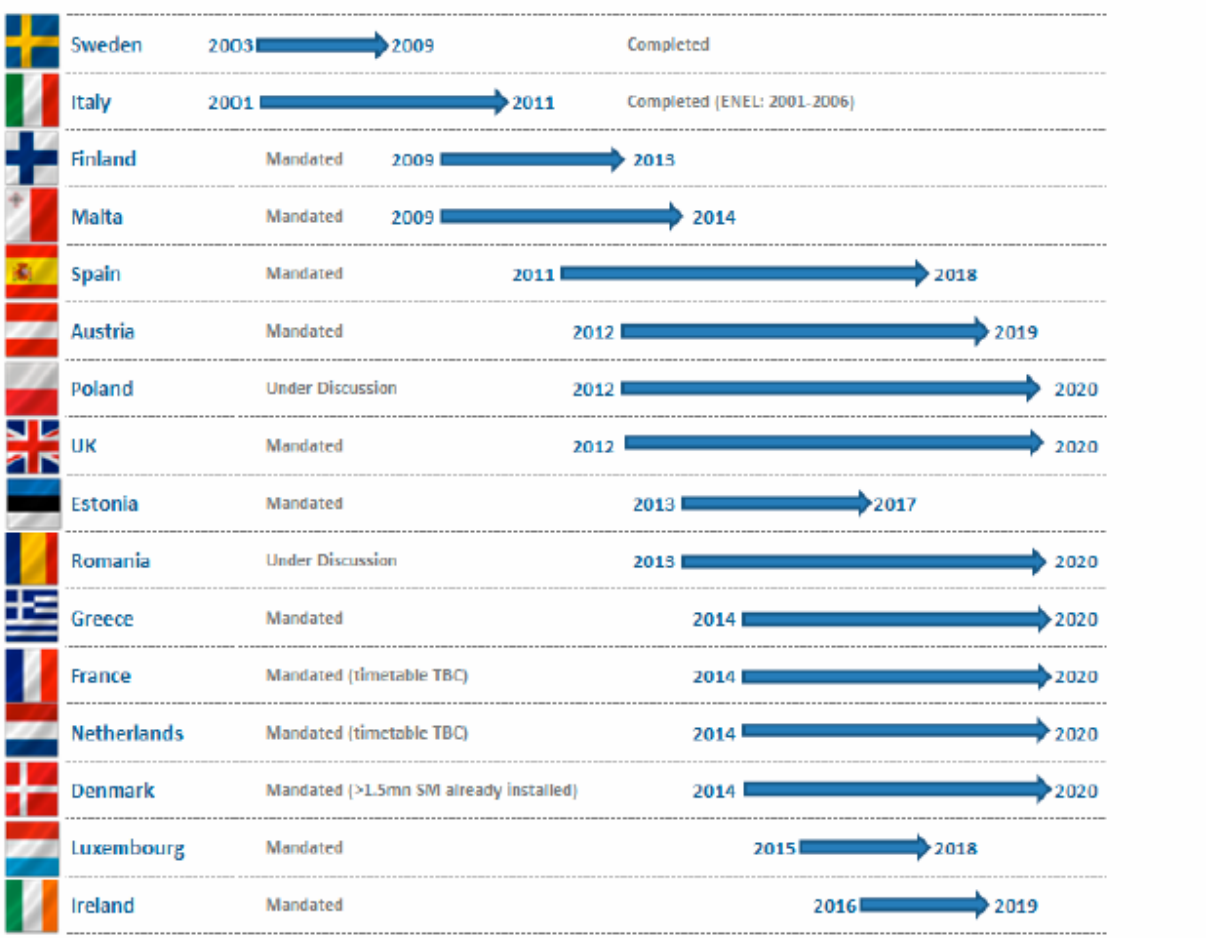
Smart Metering in Europa
Europa Roll-Out-Zahlen Ende 2014

- 68 Mio. “Smart Electricity Meter” für EU28+2 (24%), Ziel 200 Mio. (2022)
- Beschleunigung in Osteuropa (Polen, Bulgarien, Slovakei, Estland)
- 30% Wachstum (8.4 Mio.) bei Lieferungen smarter Stromzähler (2015)
- Projektion für den europäischen Smart Meter Gesamtmarkt ergibt 25-30 Mio. Einheiten pro Jahr ab 2020
- Technologie-Upgrades für “alte Rollouts” (z.B. Italien) erwartet
- Deutschland: Pessimistischer Ausblick (regulatorische/technische Hürden)

Quelle: „Smart Metering in Europe, 11th edition“, Berg insight - summary

Smart Metering in Europa

Electricity Smart Meters Roll-Out Timeline in MS*



*) at least 80% coverage

Quelle: Europäische Kommission

Smart Metering in Europa
Rollout@RWE *

UK - RWE npower:
Marktmodell: Lieferant;
starke Verzögerung;
Gas+Strom kombiniert;
full-roll-out;
zentrale Datensammlung

PL – RWE STOEN
Marktmodell: Netzbetreiber;
Rollout gestartet
(Warschau); nur Strom;
Zusatzbonus

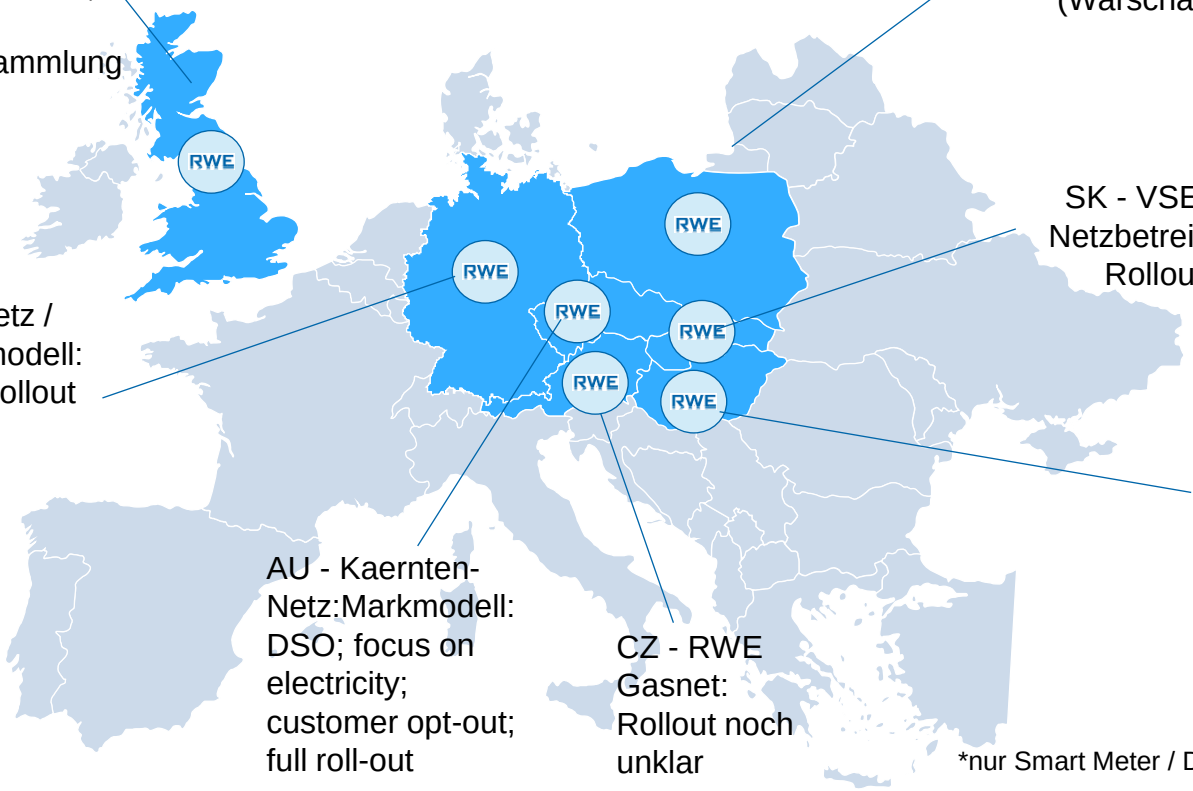
SK - VSE Marktmodell:
Netzbetreiber; selektiver
Rollout 4000 kW/h/a

D - RWE Westnetz /
Metering Marktmodell:
Netzbetreiber; Rollout
verzögert wg.
Datenschutz;
kein full-roll-out

HU - ELMÜ:
Rollout noch
unklar

AU - Kaernten-
Netz:Markmodell:
DSO; focus on
electricity;
customer opt-out;
full roll-out

CZ - RWE
Gasnet:
Rollout noch
unklar



*nur Smart Meter / Dienstleistungen