TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "IT-Sicherheit im Smart Grid"

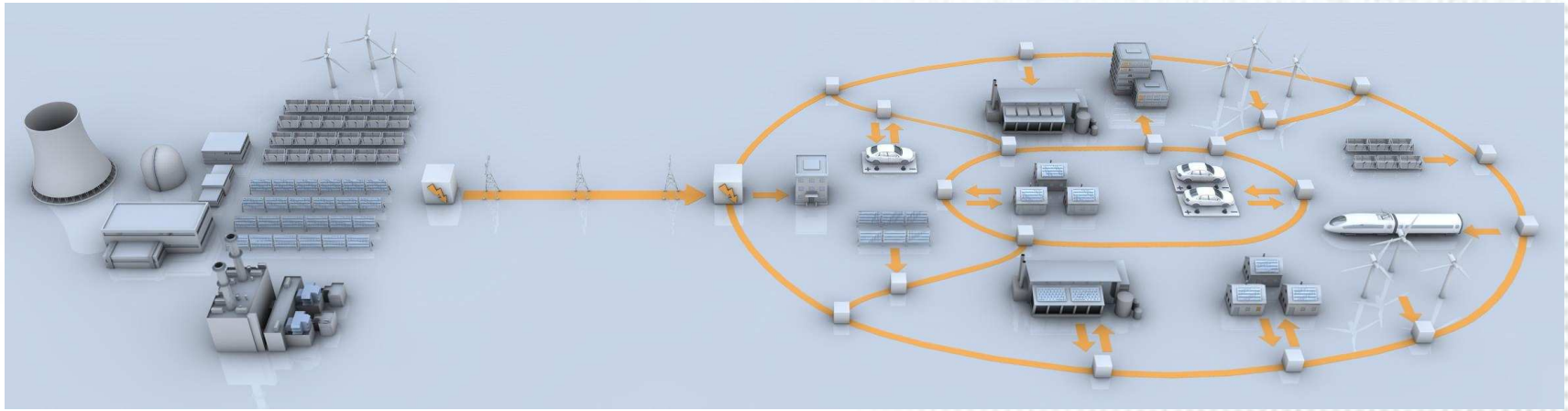
Berlin, 31.05.2011

Bernd Kowalski
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Schutzprofile für intelligente Stromzähler

Herausforderung Smart Grid

- Zentrale und dezentrale Energieeinspeisung
- Lastmanagement im Verteilnetz
- Flexible Tarifierung
- Sichere Informationsverarbeitung für Verbrauchs- und Steuerdaten



Quelle: Infineon

Politische Ziele

- Europaweite Ziele bis zum Jahr 2020:
  - 20 % Anteil an erneuerbaren Energien
  - 20 % weniger Treibhausgasemissionen als 1990
  - 20 % mehr Energieeffizienz durch Verbrauchssteuerung

- Vorbereitung der Elektromobilität
  (bis zum Jahr **2020 eine Million E-Fahrzeuge in D**)

- Mehr **Wettbewerb** unter den Energieerzeugern und Verteilnetzbetreibern

- Aufbau einer **sicheren IT-Infrastruktur** zur Steuerung der Energienetze und ihrer Endeinrichtungen

- Gewährleistung von **Datenschutz und Datensicherheit nach deutschem Standard** mit gesetzlicher Verankerung

- Schaffung einer frühzeitigen **Weltmarktposition für innovative IT-Produkte deutscher Industrieunternehmen** in diesem Sektor der Energiewirtschaft

Notwendigkeit des Smart Meter im Smart Grid

- Smart Meter sind notwendig, um eine **bedarfs- und angebotsgerechtes Lastmanagement/Energieverteilung** auch im Verteilnetz zu ermöglichen.
- Smart Grids benötigen Smart Meter als Instrument zum **Abruf und zur Weiterleitung von Verbrauchs- und Steuerdaten**.
- Das Smart Meter verarbeitet damit **sensible Daten** zur Steuerung des Netzes, der Verbraucher und dezentralen Stromerzeugern sowie **personenbezogene Daten der Verbraucher**.
- Daher müssen Smart Meter **besonders hohen Sicherheitsanforderungen** genügen.

Anforderungen an IT-Sicherheit und Datenschutz von Smart Metern

- **Verfügbarkeit, Integrität** und **Vertraulichkeit** der an die Messstellendienstleister übermittelten **Verbrauchs- und Einspeisedaten**
- **Gewährleistung der Versorgungssicherheit**
  Ausschluss negativer Rückwirkung vereinzelter oder massenhafter Fehlfunktionen wie auch gezielter Manipulationen von Smart Metern auf die Versorgungssicherheit
- **Manipulationssicherer Betrieb der Smart Meter**
  in ungesicherter Umgebung (Hausflur)
- **Datenschutzanforderungen**
  Verhinderung der Erstellung und Weitergabe von Verbraucherprofilen gemäß gesetzl. Vorgaben / Einstellungen des Kunden
- **Steuerung der Zugriffskontrolle je nach Rolle**
  der Marktteilnehmer, z. B.: Verbraucher, Netzbetreiber, Stromlieferant

**Zertifizierung der IT-Sicherheit für Smart Meter nötig,
um ein hohes, staatlich kontrolliertes Sicherheitsniveau herzustellen.**

Inhalte und Struktur eines Schutzprofils

- Abgrenzung, Einsatzumgebung
- Bedrohungen
- Sicherheitsziele
- Requirements/Sicherheitsfunktionen
- Generische Natur eines PP
- Implementierung flexibel

Inhalte der Technischen Richtlinie

- Systemarchitektur
- PKI
- Kommunikationsprotokolle
- Kryptographische Vorgaben
- Zugriffs- und Berechtigungsprofile

Erwartungen an ein Gateway Schutzprofil (GW-PP)

- **Erfüllung unterschiedlicher Sicherheitsvorgaben**
  - Generische Sicherheitsfunktionen für Key-Processing, Auth., Ener., Sign., etc.
  - Datenschutz
  - Netzsicherheit
  - Eichrecht

- **Abdeckung spezieller Marktbedürfnisse**
  - Nachvollziehbare Umsetzung der Sicherheitsvorgaben nach internat. Standard
  - Unterstützung weiterer Funktionalitäten (Gas, Wasser, etc.)
  - Basis für den weiteren Ausbau der Infrastrukturen in diesem Bereich

Primäre Sicherheitsziele

- **Schutz der Netze (O.Firewall, O.SeparateIF)**
  - Trennung der Netze WAN, MAN und HAN
  - Schutz des Gateways vor Bedrohungen aus dem WAN
  - Getrennte Schnittstellen für die verschiedenen Netze

- **Sichere Behandlung von Messdaten (O.Meter)**
  - Empfang der Verbrauchsdaten von den Zählern
  - Aufarbeitung der Daten/Tarifierung
  - Versand/Empfang der Daten an/von zentralen Dienstleistern
  - Abbildung der Rollen der Marktteilnehmer auf Zugriffskontrollprofile

Logging (O.Log)

Das Gateway führt eine Reihe von Logdateien zu verschiedenen Zwecken:

- Systemlog zur Information des Administrators
  - Informationen über den Zustand des Systems für den Administrator
- Consumer-Log zur Information des Verbrauchers
  - Informationen über Informationsflüsse
  - Informationen über aktuelle Zugriffskontrollprofile
- Billing-Log zur Information des Verbrauchers
  - abrechnungsrelevante Daten

Sicherheitsziele zum Schutz des Gateways

- **Kryptographie (O.Crypt)**
  - Bereitstellung zuverlässiger kryptografischer Funktionen zur Absicherung von Kommunikationsflüssen
  - Verwendung eines Sicherheitsmoduls
    - Speicherung von Schlüsseln
    - Asymmetrische Kryptografie
    - Bereitstellung von Zufallszahlen

- **Schutz der Sicherheitsfunktionen (O.Protect) durch**:
    - Speicheraufbereitung
    - Selbstests
    - Fail-Safe Funktionalität
    - Detektion physischer Manipulationen

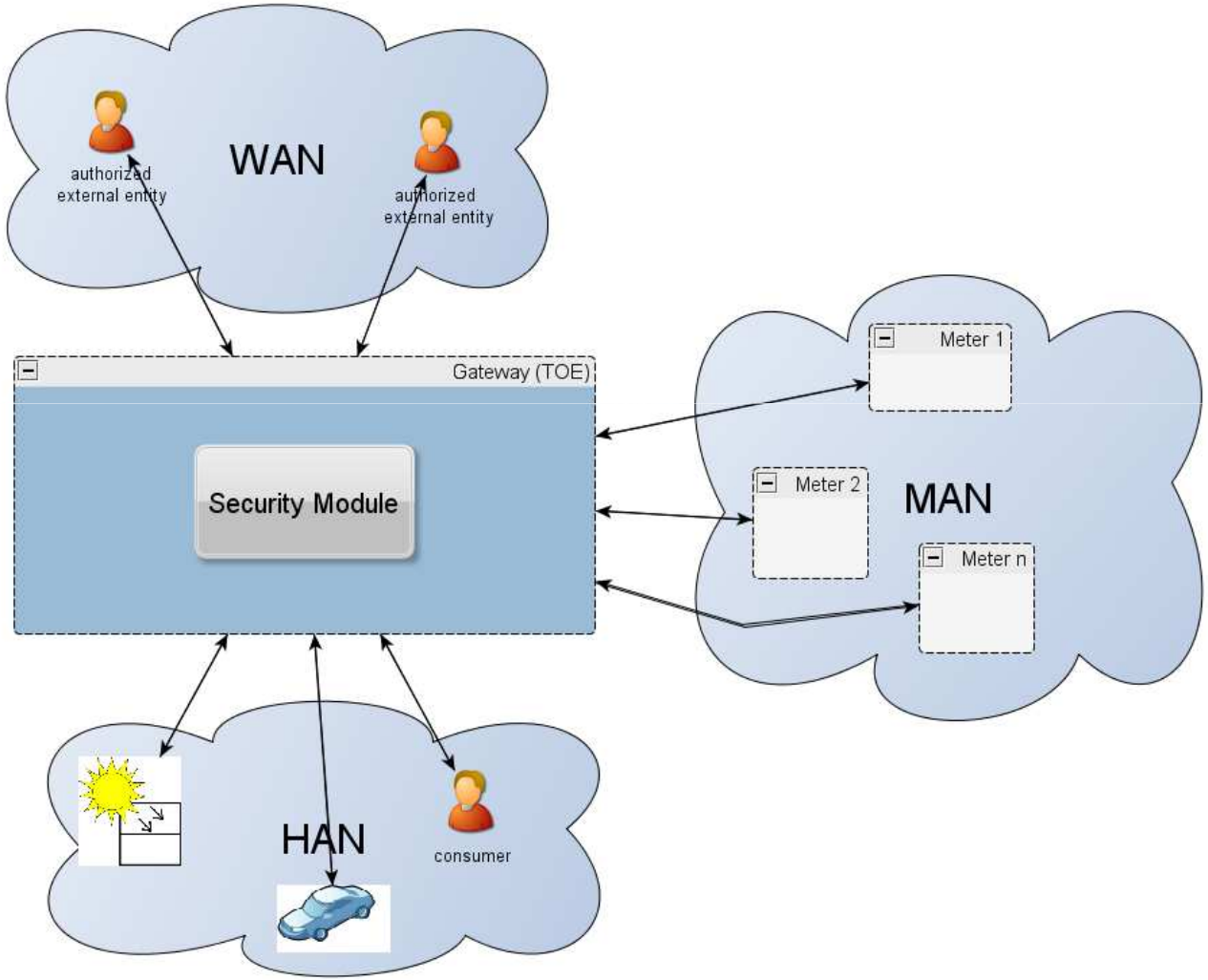
Sicherheitsziel zur Verhinderung der Verkehrsflussanalyse

- **Verschleierung (O.Conceal)**
  - Durch Verschlüsselung
  - Ggf. durch zusätzliche Phantomverbindungen

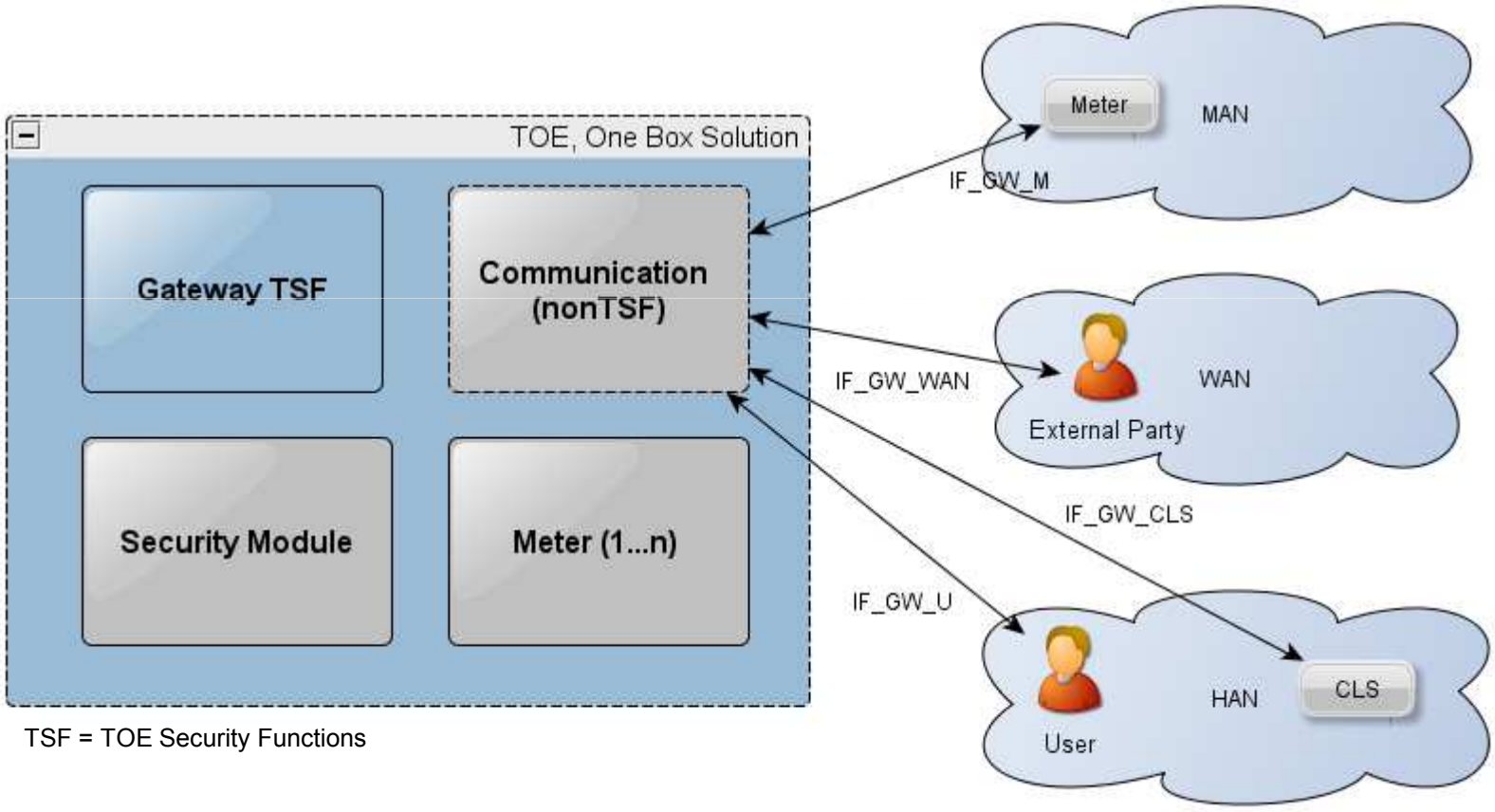
Sekundäre Sicherheitsziele

- **Managementfunktionen (O.Management)**
  - Management der implementierten Sicherheitsfunktionen
  - Beschränkung des Management-Zugangs für autorisierte Administratoren und bestimmte Schnittstellen
- **Zugriffskontrolle (O.Access)**
  - Beschränkung des Zugangs zu Informationen und Funktionen
- **Verlässliche Uhrzeit (O.Time)**
  - Bereitstellung einer verlässlichen Uhrzeit
  - Laufgenauigkeit der lokalen Uhr
  - Verlässliche Zeitquelle zur Synchronisation

Modulare Struktur des Smart Meter gemäß Protection Profile (V1.0)



Smart Meter Variante als Einboxlösung: Gateway + Security Module + Kommunikationsmodul + Meter

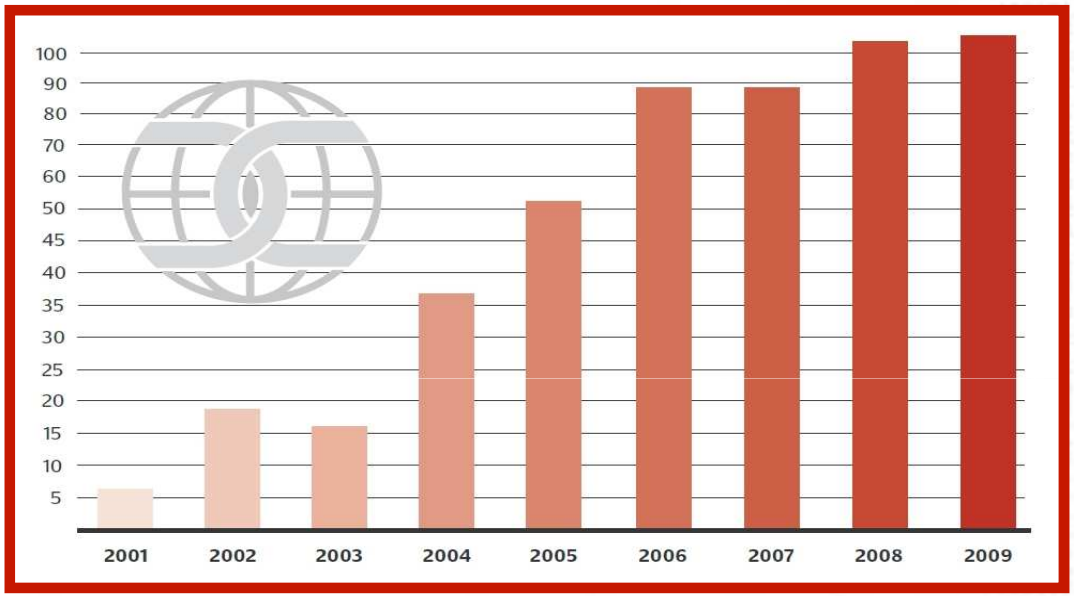


TSF = TOE Security Functions

Grundsatzentscheidungen nach der 2. Kommentierungsphase

- Technische Ansteuerbarkeit des Gateways aus dem WAN möglich.
- kein lokales Display im Gateway.

IT-Sicherheit bekommt im Smart Grid eine existenzielle Bedeutung



Bedeutung von Zertifizierungs-verfahren gewinnt angesichts der künftigen technologischen und gesellschaftlichen Entwicklung **eine wachsende regulative, innen-, industrie- und außenpolitische Bedeutung.**

Ausblick:

- IT-Marktführer lassen komplette Produktplattformen zertifizieren
- IT-Sicherheit wird integraler Bestandteil von Betriebssystemen u. Systemlösungen
- Zertifizierung wird zum Wettbewerbsmerkmal

Vorteile durch Zertifizierung

- **Nachweis der Wirksamkeit von Sicherheitseigenschaften** gegenüber Kunden
- **Verbesserung der Produktqualität** mit geprüfter „IT-Security“ als Qualitätsmerkmal
- **Staatliche Zertifizierungsstelle garantiert Neutralität** und **internationale Anerkennung** des Zertifikates, eine Herstellererklärung ist nicht ausreichend
- Nutzung des staatlichen Prüfsiegels fürs **Produktmarketing sowie Marktvorteil durch das anerkannte Prüfsiegel**
- **Entlastung des Herstellers**, da er nachvollziehbar seinen unternehmerischen Pflichten nachgekommen ist.
- **Etablierung eines speziellen Umsetzungsprozesses für im Wirkbetrieb erforderliche SW-Updates**, der zeitnahe Updates und eine ggf. nachgezogene Re-Zertifizierung erlaubt.

CC-Zertifizierung
Weltweite Anerkennungsvereinbarung (CCRA) bis EAL 4

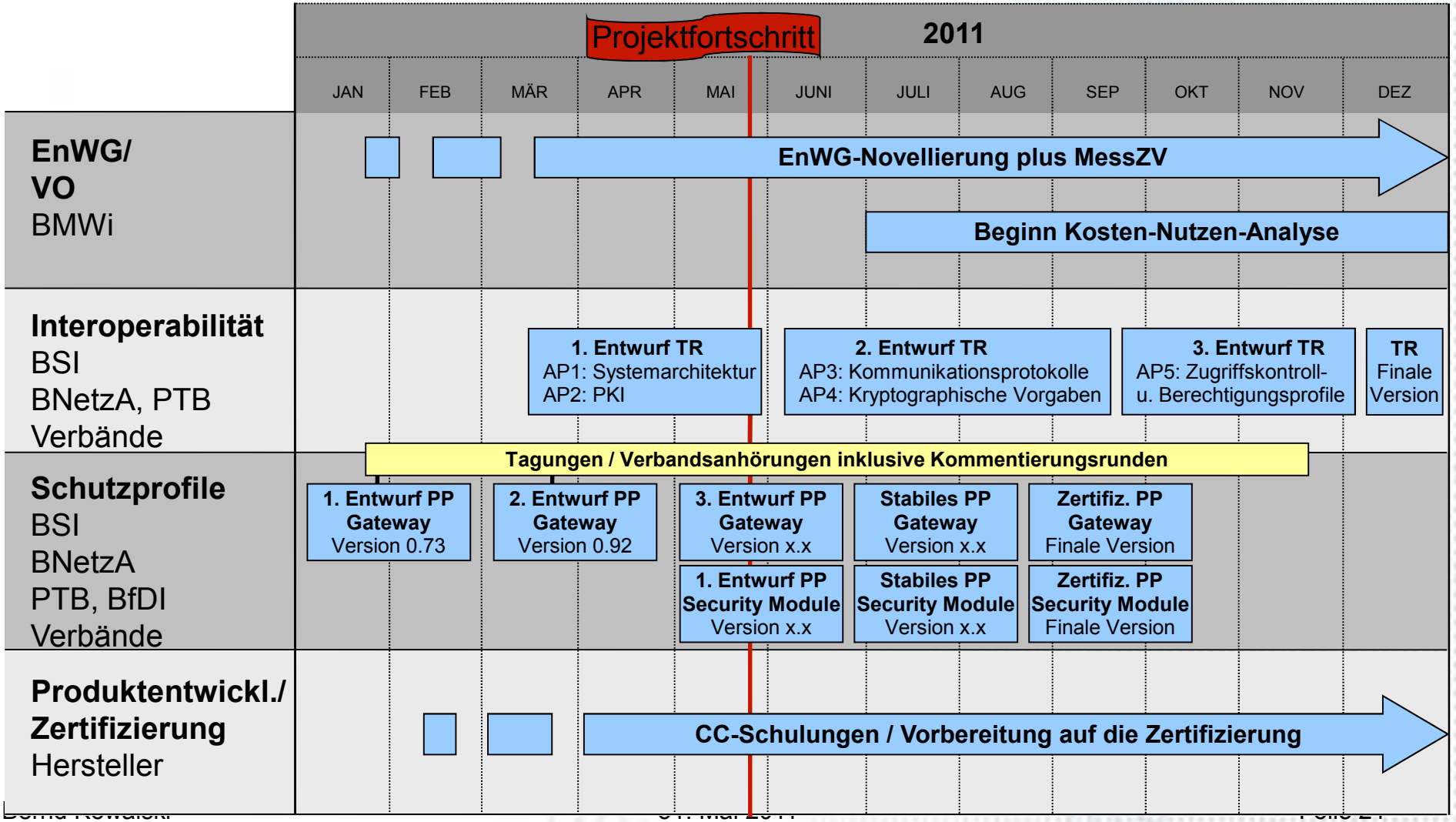
Anerkennende und zertifizierende Nationen		Anerkennende Nationen	
Australien/ Neuseeland	USA	Finnland	Griechenland
Kanada	Deutschland	Israel	Malaysia
Großbritannien	Frankreich	Dänemark	Ungarn
Norwegen	Niederlande	Tschechische Republik	Singapur
Japan	Spanien	Österreich	Pakistan
Schweden	Südkorea	Indien	
Italien	Türkei		

CC-Zertifizierung
Europäische Anerkennungsvereinbarung (SOGIS-MRA)

- Anerkennung von Common Criteria und ITSEC Zertifikaten
- Schließt alle Evaluationsstufen von EAL1 bis EAL7 ein (je nach "Technical Domain")

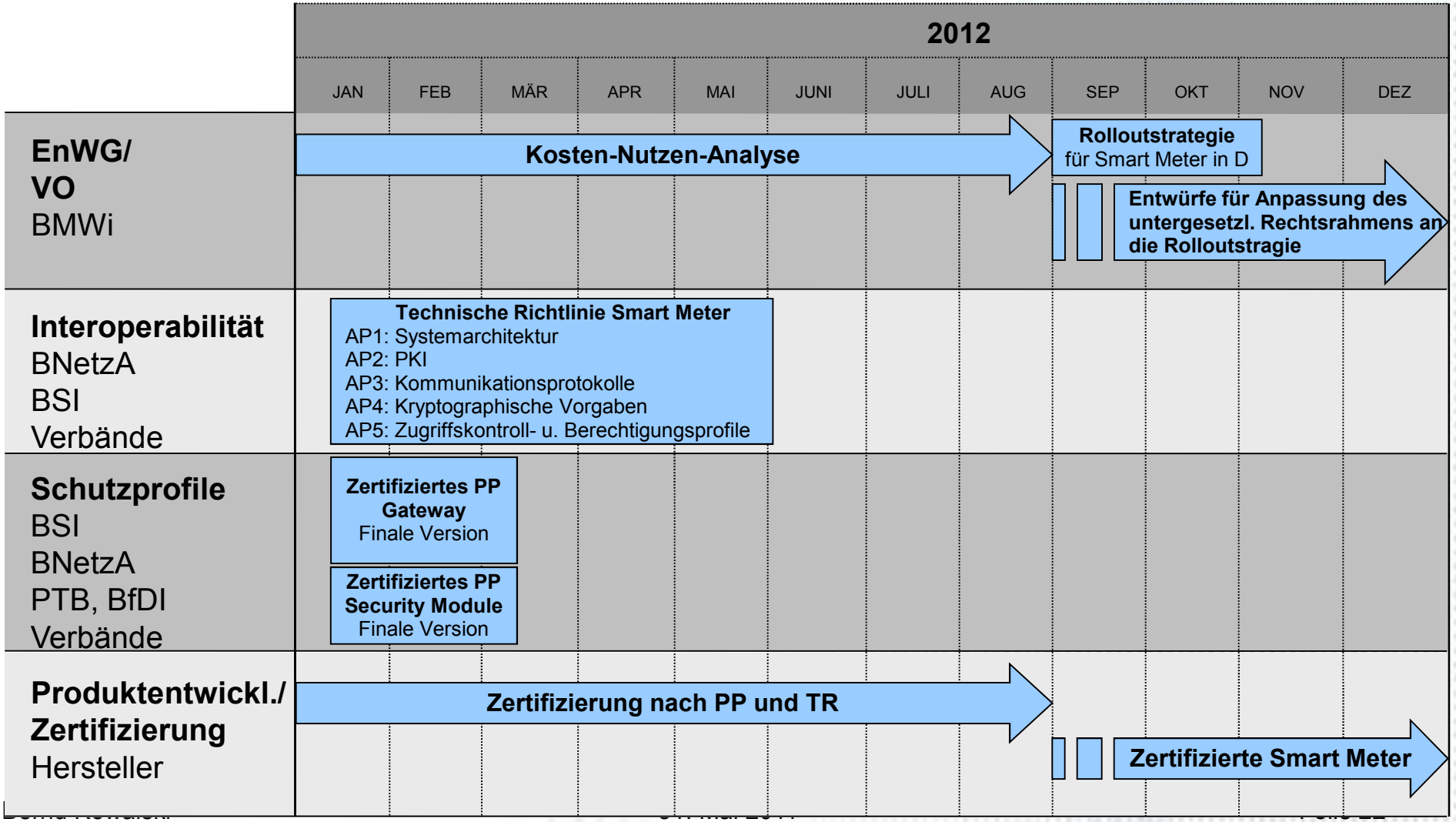
Bundesamt
für Sicherheit in der
Informationstechnik

Roadmap Smart Meter (2011)



Bundesamt
für Sicherheit in der
Informationstechnik

Roadmap Smart Meter (2012)



Zusammenfassung

- Schutzprofil und Technische Richtilinie bilden einen **einheitlichen, technischen Sicherheitsstandard für Smart Meter** im künftigen Smart Grid.
- Die Einhaltung von TR und PP werden durch entsprechende **Prüfungen bei neutralen, unabhängigen Prüflabors** mit einem abschließenden **Zertifikat des BSI** nachgewiesen.
- Die Zertifizierung nach dem CC-Standard schafft die Möglichkeit einer **internationalen Anerkennung und Vermarktung**. TR und PP werden in die europäische Normung eingebracht.
- Die technischen Standards für das Smart Meter entstehen **parallel zu der Novellierung von EnWG und MessZV.**
- Rechtsrahmen und technischer Standard schaffen **Planungs- und Investitionssicherheit** für die beteiligten Hersteller.
- Ein früher dt. Standard gewährleistet die wirksame **Einflussnahme auf entsprechende europäische Festlegungen** und **Wettbewerbsvorteile für die dt. Industrie**.

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Bernd Kowalski
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228-99-9582-5700
Fax: +49 (0)228-99-10-9582-5700

Bernd.Kowalski@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de