



Datenschutz und Datensicherheit in der Energieversorgung

- Sicherheitsstandards – Teil der Cybersicherheitsstrategie
- Erwartungen an das „Intelligente Energie-Netz“
- Rolle der Messsysteme im intelligenten Netz
- Rechtliche und sicherheitstechnische Vorgaben

Bernd Kowalski
Bundesamt für Sicherheit in der Informationstechnik
(BSI)

**Fachkonferenz Bürgernahe Sicherheitskommunikation
für Städte und Gemeinden**

13. Juni 2012



- Steigende Komplexität und Verbreitung der IT
- Verbindung von Unternehmensnetzen mit dem Internet
- Neue Anwendungen, komplexe Patchprozesse
- Täglich 43.000 neue Schadprogrammvarianten
- Schwarzmarkt für Verwundbarkeiten/Exploits

➡ auch betroffen: IT im Energiesektor



Arten und Motive bei Cyber-Angriffen



Ungezielte Angriffe

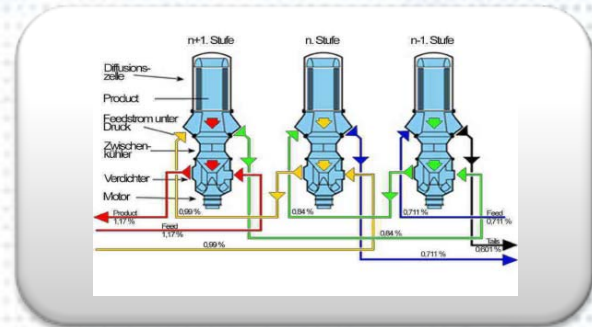
- Sabotage, Betrug, etc.
- Unspezifische Zielgruppen
- **SPAM, Viren, Würmer, Trojaner, Drive-by-Downloads**

Gezielte Angriffe

- Spionage und Sabotage
- Spezielle Zielgruppen
- **Social-Engineering + Trojaner**

Skalpelliartige Angriffe

- Sabotage spezieller IT-Systeme (und Infrastrukturen) mit großem Schadensausmaß
- Komplexe, langwierige Vorbereitung
- **Zero-Day-Verwundbarkeiten**
- **Fälschung von Zertifikaten**



- Ziele: Sicherheit, Unabhängigkeit, Erhaltung gesellschaftlicher Werte
- Strategische Zielsetzung gemäß Kabinettsbeschluss vom Feb 2011:

„Cybersicherheit auf einem der Bedeutung und der Schutzwürdigkeit der vernetzten Informationsstrukturen angemessenem Niveau zu gewährleisten ohne den Nutzen des Cyber-Raums zu gefährden“

- Dies erfordert auch **präventive Maßnahmen**, z. B.:

Gesetzliche **Verbindlichkeit von technischen Sicherheitsstandards** für sicherheitskritische Infrastrukturen

 **Das Intelligente Energienetz ist eine kritische Infrastruktur**





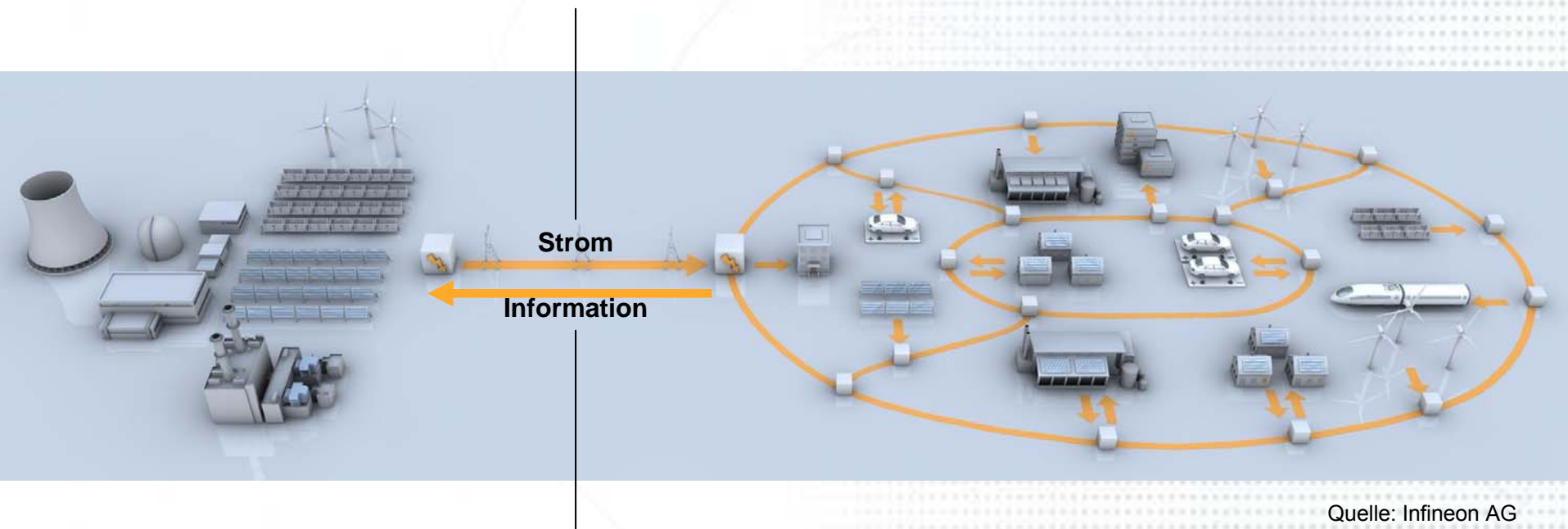
Energie- und Umweltpolitische Ziele

- Europaweite Ziele bis zum Jahr 2020:
 - **20 % Anteil an erneuerbaren Energien**
 - **20 % weniger Treibhausgasemissionen** als 1990
 - **20 % mehr Energieeffizienz** durch Verbrauchssteuerung
- Robuste und krisenfeste Sicherstellung der Energieversorgung (**Versorgungssicherheit**)
- 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**.



Smart Grid – vom passiven zum intelligenten Verteilnetz

Versorgungssicherheit



Quelle: Infineon AG

Versorgungssicherheit, Datensicherheit und Datenschutz



„Schutzziel“ Versorgungssicherheit in intelligenten Versorgungssystemen

- **„Versorgungssicherheit ist eines der zentralen energiepolitischen Ziele. [...] Die Stromkunden müssen im Durchschnitt nur mit 19 Minuten Stromausfall im Jahr rechnen. Das entspricht einer Zuverlässigkeit von 99,99996 Prozent.“**

Quelle: „Energemarkt Deutschland Zahlen und Fakten zur Gas-, Strom und Fernwärmeversorgung“, BDEW 2009

- Versorgungssicherheit → stellt sehr hohe Anforderungen an:
 - Verfügbarkeit in Normallagen
 - Qualität / garantierte Eigenschaften (Spannung, Frequenz, etc.)
 - Widerstandsfähigkeit gegen Störungen und Krisenlagen
 - Wiederherstellbarkeit nach Großstörungen („Schwarzfall“)



„Schutzziel“ Datensicherheit und Datenschutz in intelligenten Versorgungssystemen

- Marktteilnehmer (Netzbetreiber, Lieferanten) benötigen unverfälschte **Daten über Verbrauch und Einspeisung**
 - Steuerung des Energiebedarfs und –angebots (Lastmanagement/ Energieverteilung)
 - Lastvariable und tageszeitabhängige Tarife
- Kunden sehen ihre **Privatsphäre** durch spezifische Verbrauchsprofile bedroht
- **Ausfallsicherheit des Energieversorgungsnetzes** (Kritische Infrastruktur)
 - Ausschluss negativer Rückwirkung durch Fehlfunktionen oder
 - massenhaften Manipulationen von intelligenten Messsystemen

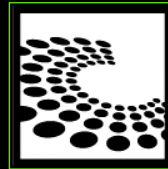


Vermeidung von Akzeptanzhürden

28th Chaos Communication Congress Behind Enemy Lines

Smart Hacking For Privacy

Advanced metering devices (aka smart meters) are nowadays being installed throughout electric networks in Germany, in other parts of Europe and in the United States. Due to a recent amendment especially in Germany they become more and more popular and are obligatory for new and refurbished buildings.



News-Meldung vom 20.09.2011 12:18

Smart Meter verraten Fernsehprogramm

vorlesen / MP3-Download

Anhand der von einem intelligenten Stromzähler gelieferten Strorr es möglich, auf das auf einem typischen TV-Gerät angezeigte Fer schließen, da Fernseher je nach angezeigtem Bild unterschiedlich haben. Das haben [Forscher der FH Münster](#) im Rahmen des vom Projekts DaPrim (Data Privacy Management) in Versuchen [heraus](#) es über die Auswertung des Verbrauchsmusters prinzipiell auch rr von DVD oder anderen Quellen abgespielten Film zu identifizier

Besonders hilfreich bei dieser Analyse sind Hell-Dunkel-Abschnitt signifikante Änderungen im Stromverbrauch ergeben, sowie größ wenig Störungen durch andere Geräte. Bei den Versuchen griff m eines in einer normalen Wohnung installierten, intelligenten Strorr



News-Meldung vom 19.11.2009 14:48

« Vorige | Nächste »

Intelligente Stromnetze: Ich weiß, ob du gestern geduscht hast

vorlesen / MP3-Download

Mit der Frage, ob sich durch intelligente Stromnetze Rückschlüsse auf die Lebensgewohnheiten von Menschen ziehen lassen und wie man dem begegnet, beschäftigt sich eine Studie von US-Datenschützern. Die US-Regierung hat die Einführung eines intelligenten Stromnetzes (Smart Grid) begonnen, um die Effizienz des bereits jetzt schon am Limit arbeitenden Stromnetzes zu erhöhen. Dazu melden etwa intelligente Stromzähler in den Haushalten (Advanced Metering Infrastructure [AMI] Smart Meter) stündlich oder öfter den aktuellen Verbrauch an den Stromversorger weiter, der daraufhin entweder die Erzeugung oder die Verteilung anpassen kann.

Aus den gesammelten Daten lässt sich aber laut Studie "[SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation](#)" (PDF) erheblich mehr ableiten. Denkbar wäre anhand des für bestimmte Geräte typischen

10.04.2012 14:55



« Vorige | Nächste »

Intelligente Stromzähler in Puerto Rico häufig für dumm verkauft

vorlesen / MP3-Download

In Puerto Rico sind offenbar nicht nur Smart Meter selbst bereits selbstverständlich, sondern auch die Manipulation der "intelligenten Stromzähler", wie der US-Journalist Brian Krebs [berichtet](#). Er beruft sich dabei auf einen auf das Jahr 2010 datierten FBI-Bericht. Demnach haben Stichproben eines nicht näher genannten Stromversorgers ergeben, dass etwa jedes zehnte Smart Meter manipuliert ist. Den daraus entstehenden Schaden schätzt der Versorger auf bis zu 400 Millionen US-Dollar jährlich – entsprechend derzeit 300 Millionen Euro.



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 → „Security by Design“ gemäß EnWG/Mess ZV und TR/PP.



Einführung moderner Messsysteme: EU-Richtlinien und nationale Umsetzung

- **EU-Richtlinie 2009/72/EG (Strom) und 2009/73/EG (Gas): „3.Binnenmarktpaket“**
 - Vorgaben für intelligentes Metering für Strom und Gas
 - Einführung bei 80 % der Verbraucher / Wirtschaftlichkeitsanalyse
- ➔ **Nationale Umsetzung: Energiewirtschaftsgesetz 2011**
 - Variable Tarife und Förderung moderner Messsysteme
 - Anforderungen an ein Messsystem
 - Verbindlicher Verweis auf Schutzprofile, Technische Richtlinie

Wenn technisch möglich (am Markt verfügbar):

- bei Neubauten und größeren Renovierungen
 - bei Letztverbrauchern mit einem Jahresverbrauch größer 6.000 kwh
 - bei EEG- und KWKG Neuanlagen größer 7 Kilowatt
- } ca. 10 – 15 % der
Stromkunden
= 4 - 6 Mio.
Messsysteme

Wenn technisch möglich und wirtschaftlich vertretbar:

- Anschlussverpflichtung für bestehende EEG und KWKG-Zählpunkte, sofern bereits ein Messsystem verfügbar ist.
- ➔ Kosten-Nutzen-Analyse (1. Sep. 2012) entscheidet über weitere Verpflichtungen oder der Wettbewerb (Voraussetzung: keine Mehrkosten für den Anschlussnutzer)
- Bestandsschutz bis zum 31. Dezember 2012 / Nutzung bis zum nächsten Ablauf der Eichgültigkeit (8 Jahre)
- Die gleiche Regelung ist auch für Messeinrichtungen im Gasbereich vorgesehen.

Zertifizierung von Produkten



**Common Criteria
IT-Sicherheit**



**Technische Richtlinien
Konformität**

Zertifizierung von Systemen



**ISO 27001 / IT-GS
IT-Sicherheit**

Anerkennung und Zertifizierung von Stellen und Personen



Schutzprofil (PP)

- Festlegung von Mindestsicherheitsanforderungen:
 - Datenschutz,
 - Datensicherheit,
 - eichrechtlichen Anforderungen

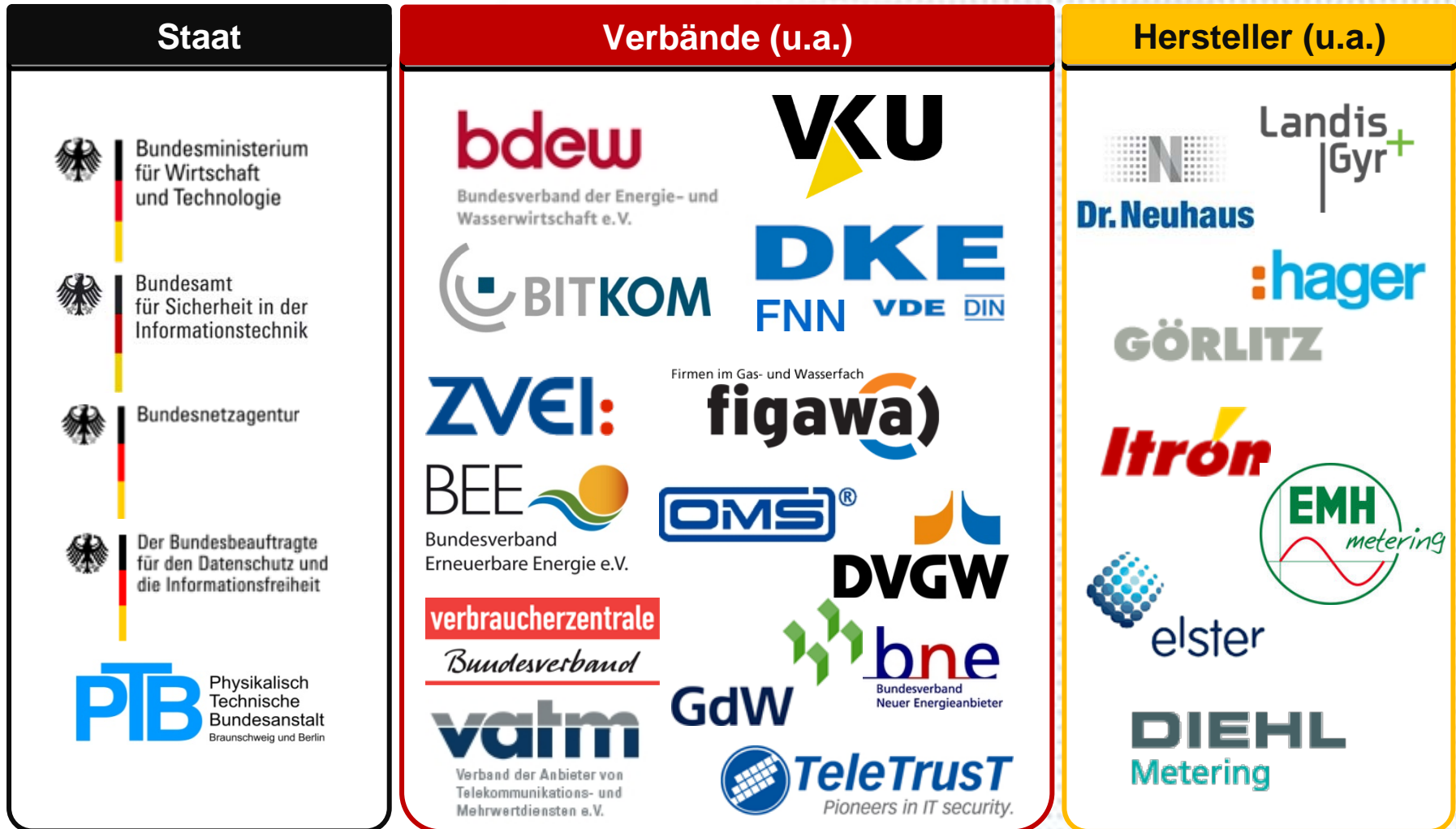
Technische Richtlinie (TR):

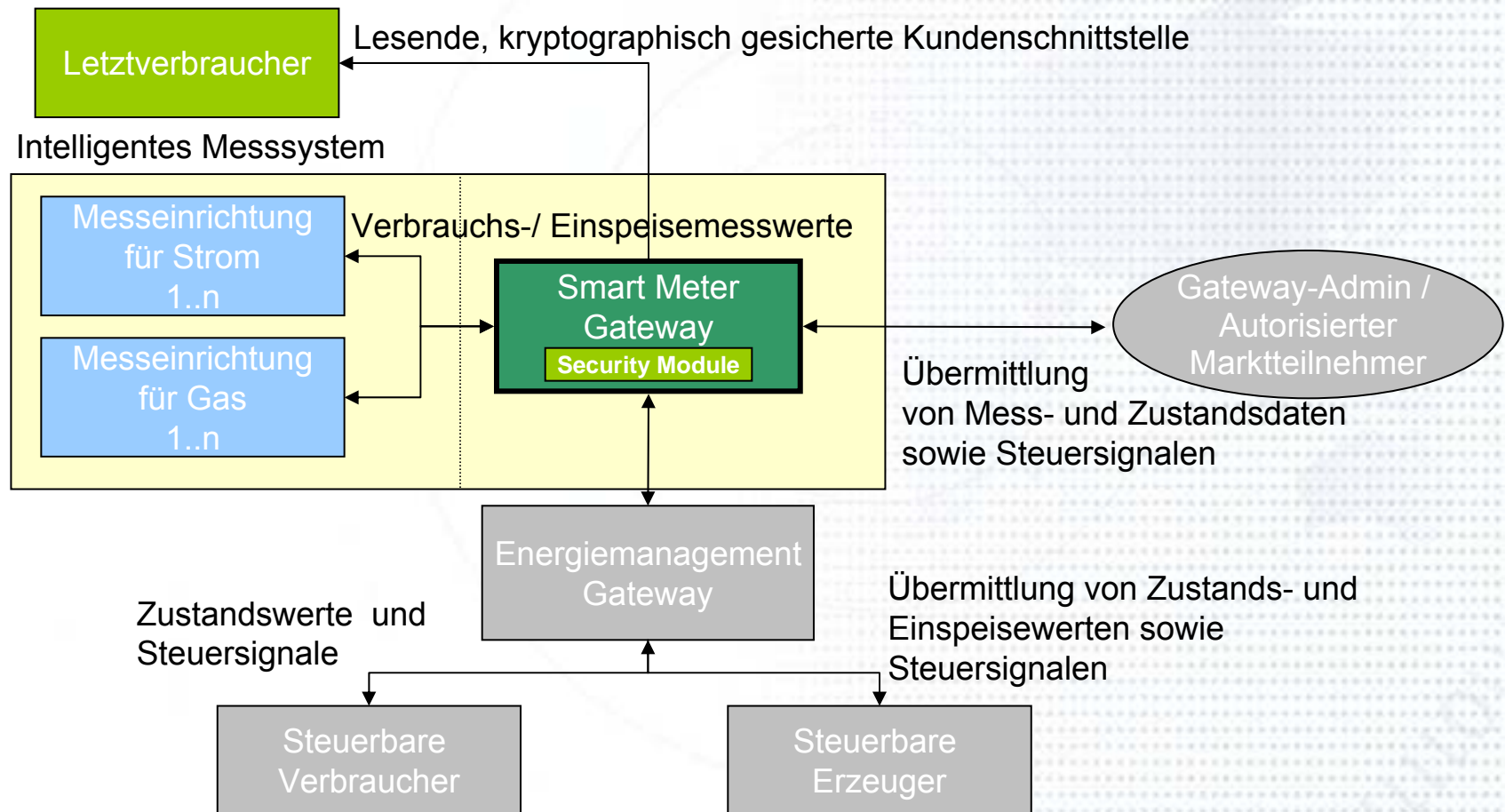
- Festlegung von Funktionalität und Interoperabilität
- ➔ Zusammenarbeit mit Hersteller-, Wirtschafts-, Verbraucherverbänden und Datenschutzbeauftragten

Künftige Smart Meter Produkte bieten daher:

- Nachweis der geforderten Sicherheitseigenschaften
- optional weitere Funktionalitäten und (Sicherheits-) Dienstleistungen
- eine Basis für den weiteren Ausbau der Infrastruktur.

- Start des Projekts im September 2010: Forderung des BfDI / Auftrag durch das BMWi



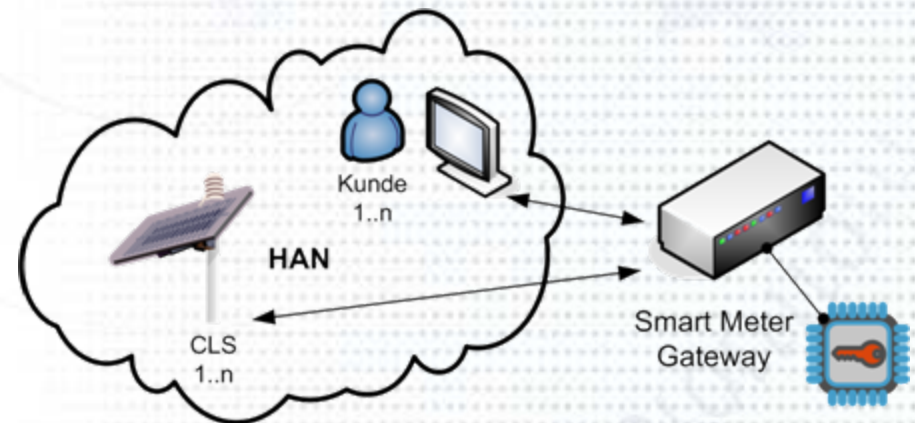


Smart Meter Gateway

- unterstützt die Kommunikation mit verschiedenen externen Marktteilnehmern
- ist multimandantenfähig und unterstützt flexible, variable Tarife
- bietet mit der CLS-Schnittstelle einen sicheren Kommunikationskanal zwischen WAN und lokalen Systemen (Controlable Local Systems, CLS)
- kann sicheren Kommunikationskanal bis zu 48 Stunden aufrecht erhalten, um zeitnah Daten auszutauschen
- muss gemäß Schutzprofil selbst keine Steuerungsfunktionalität für CLS Geräte implementieren

Beispiele für CLS

- Erzeugungsanlagen nach EEG/KWKG
- Energiemanagement Gateway
- andere (Weiße Ware)

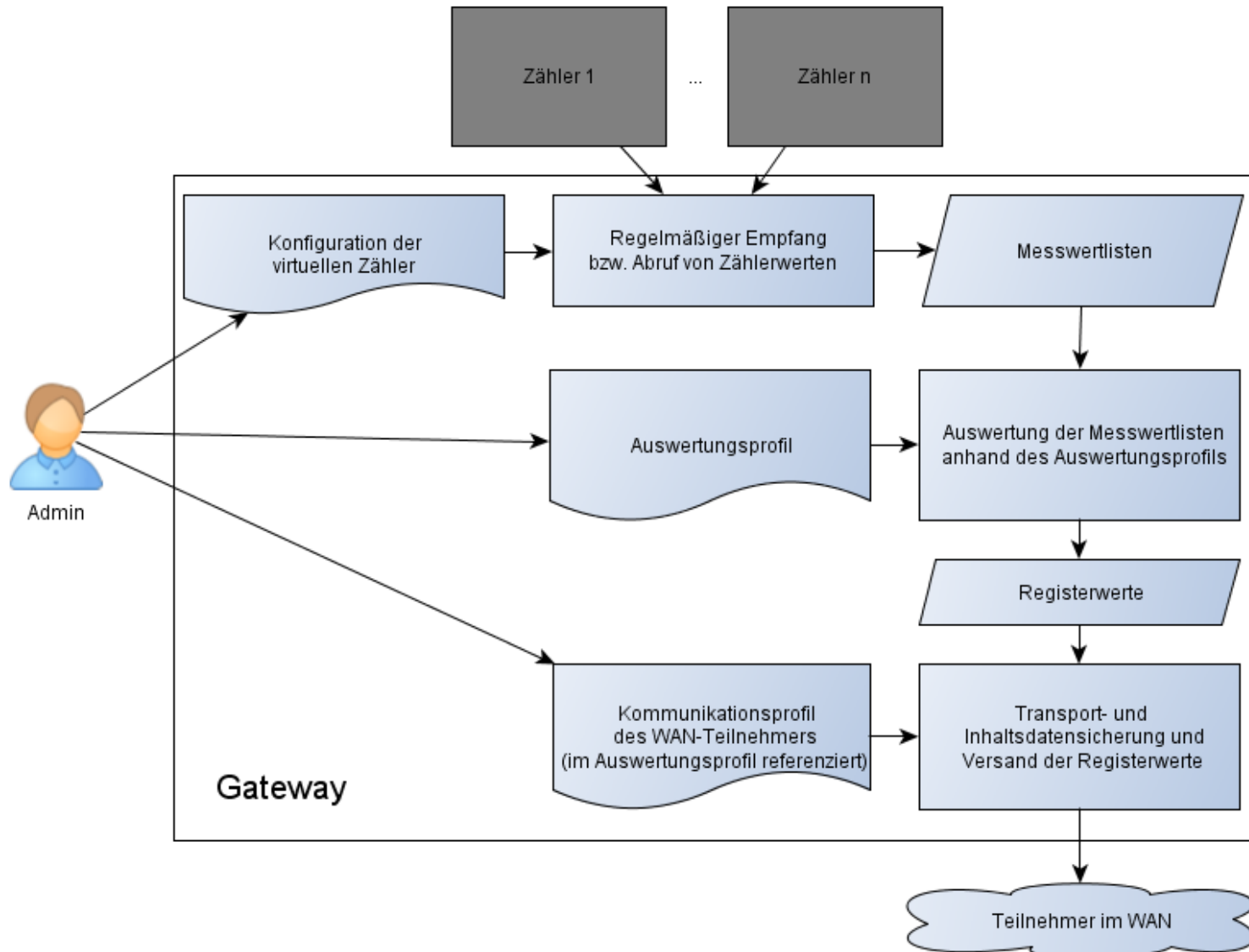


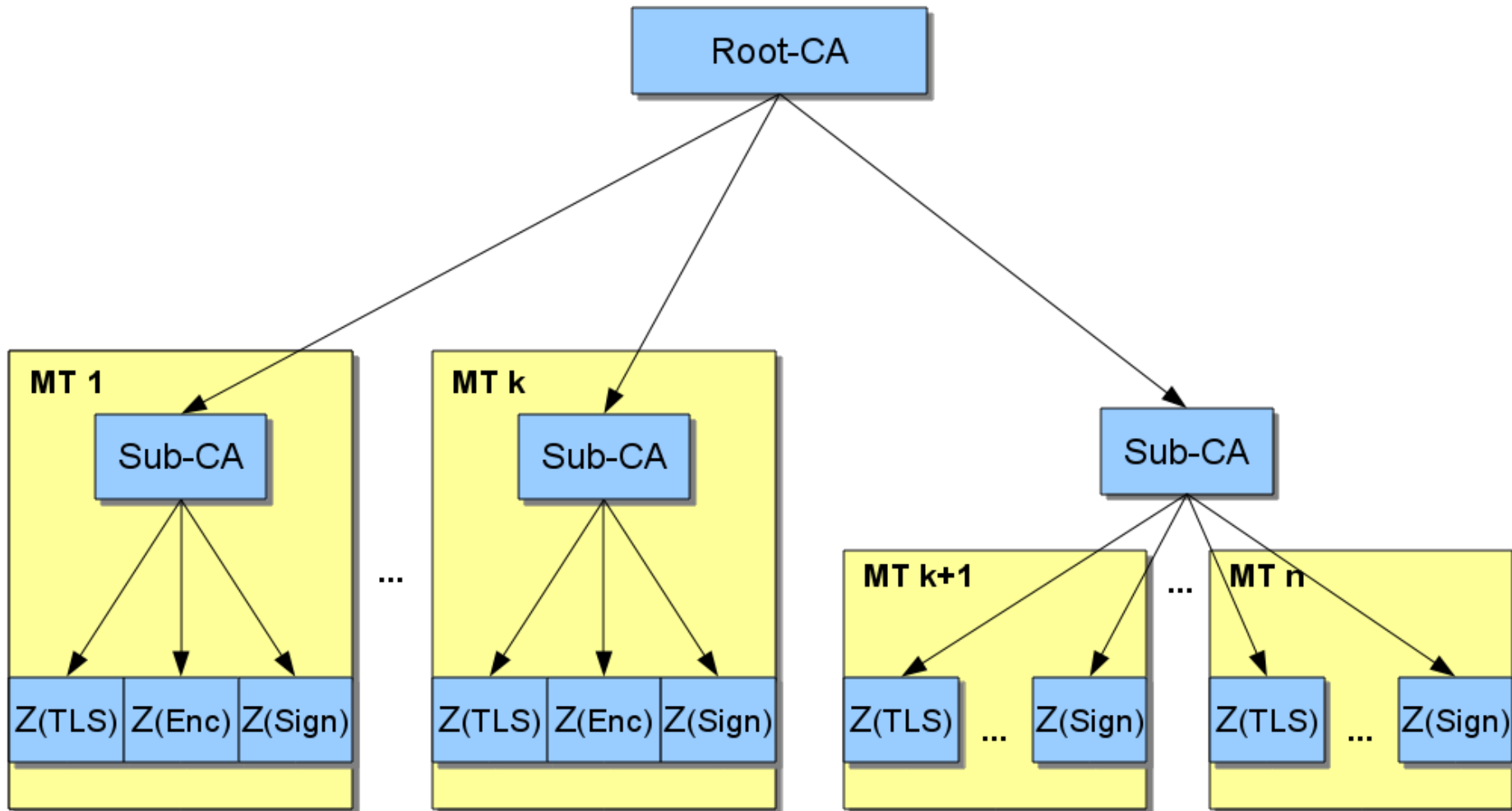


Dezentrale und zentrale Tarifierung

- **Tarifierungskonzept** berücksichtigt sowohl
 - die Möglichkeit der **dezentralen Tarifierung** im Gateway
 - als auch die **zentrale Tarifierung** in nachgelagerten Systemen.
- Tarifierungskonzept ist flexibel in Bezug auf die Granularität der zu erhebenden Daten.
- Es können **zeit-, last- und verbrauchsbasierte** Tarife modelliert werden.
- Flexible, transparente und nachvollziehbare Tarifwechsel möglich, je nach Tarifwechselprozess realisierbar.
- Erhebung von granularen Netzparametern, **Bilanzierungsrelevanten Statusdaten** möglich.

Übersicht des Tarifierungskonzepts







Verschiedene Markakteure in der PKI-Hierarchie

Root-CA: Zentraler Vertrauensanker (Hoheitlich)

- Vertrauensanker für die PKI
- Stellt Zertifikate Sub-CAs aus
 - ➔ Berechtigung von Sub-CAs zur Ausstellung von Endnutzer-Zertifikaten

Sub-CA: Endnutzerzertifizierung

- Privater Dienstleister
- Müssen die Anforderungen der Root erfüllen zur PKI-Teilnahme
- Stellen Zertifikate für Endnutzer aus

Endnutzer (nutzen die PKI-Zertifikate)

- Smart Meter GW / GW-Admin
- Externe Marktteilnehmer (z.B. Messstellenbetreiber und Stromanbieter)



- **Intelligente** Energienetze sind **Kritische Infrastrukturen** und benötigen daher SMGs mit „Security by Design“ gemäß EnWG und MessZV.
- Schutzprofil und Technische Richtlinie gewährleisten **hohe Datenschutz- und Datensicherheitsmaßnahmen** für intelligente Messsysteme.
- **Vertrauen und Akzeptanz** durch Umsetzung von Daten- und Verbraucherschutzmerkmalen sind wesentliche Erfolgsfaktoren.
- Zertifizierung nach dem CC-Standard schafft für die Hersteller die Möglichkeit einer **internationalen Anerkennung und Vermarktung**.
- Rechtsrahmen und technischer Standard ermöglichen **Planungs- und Investitionssicherheit**.
- Energienetzbetreiber müssen sich mit **neuen Marktrollen** auseinandersetzen.



Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bernd Kowalski
Abteilung S
Godesberger Allee 185-189
53175 Bonn

smartmeter@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

www.bsi.bund.de/SmartMeter

