



Zukunftsforschungsinstitut
Öffentliche Sicherheit

Smart Grids – Smart Metering

Sicherheit

Herausforderungen und Lösungen

...oder Gestern war Heute noch Zukunft

Dr. Michael Arzberger
VP Solution Management
Elster Integrated Solutions
michael.arzberger@elster.com

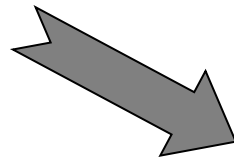
Smart Grid – Smart Metering

Intelligentes Netz

- kommunikative Vernetzung
- Steuerung

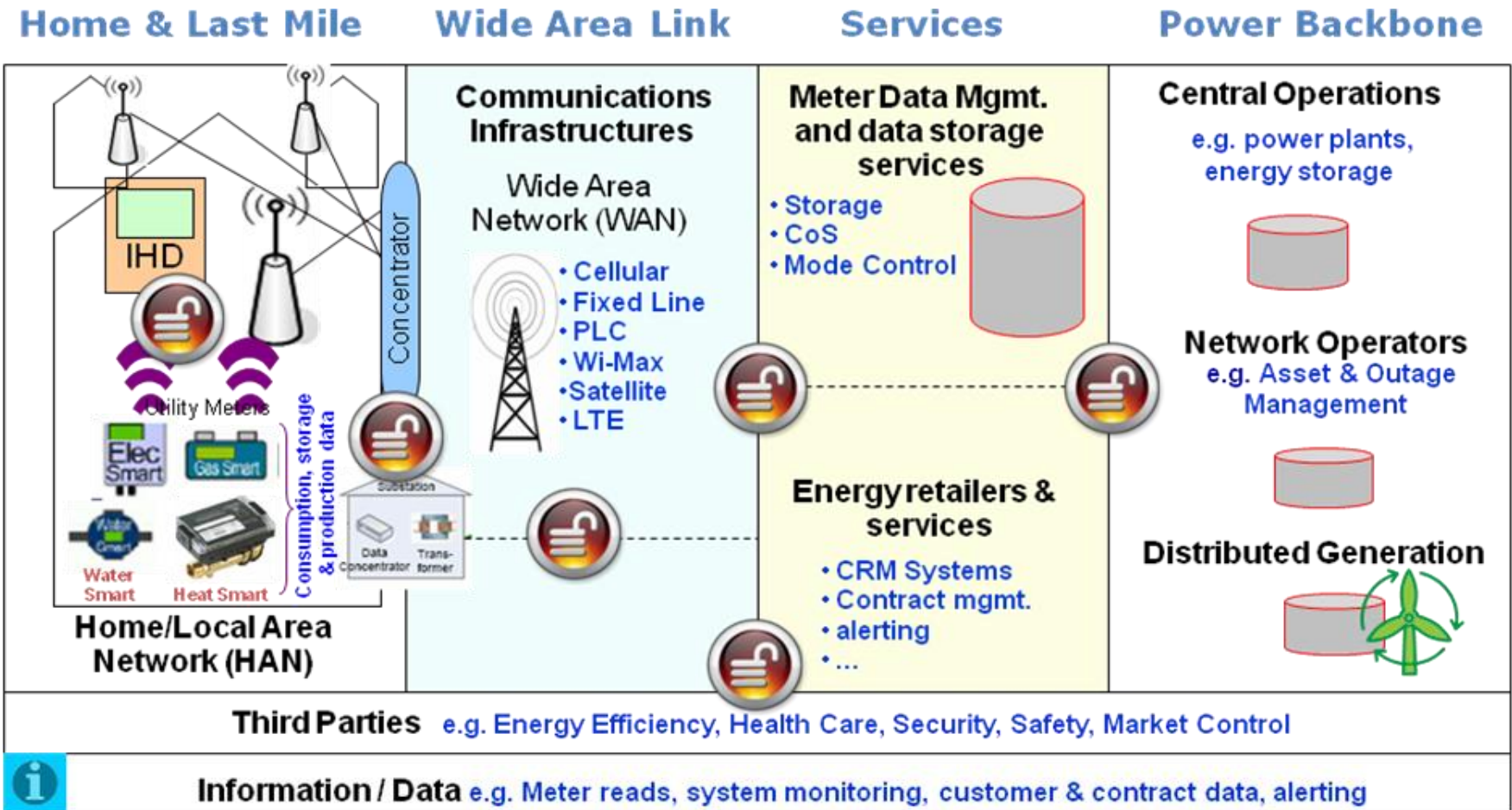
Einbeziehung aller Komponenten


- Erzeugung (..dezentral)
- Speicherung
- Verbrauch
- Betriebsmittel



Smart Metering

Intelligentes Netz



 = **Interface Risk**

Licht und Schatten

+

- Bessere Auslastung
- Vermeidung von Ausbau

-

- Komplexität
- Viele Schnittstellen
- Persönliche Daten



15 November 2010, 12:36

Symantec: We finally understand Stuxnet

Security firm Symantec says it has [discovered](#) that the [Stuxnet worm](#) targeted specific motors used, for instance, in uranium enrichment processes. With the support of a Dutch [Profibus](#) expert, Symantec says, in a blog posting, that it has now managed to fully interpret the purpose of the Stuxnet code. Apparently, Stuxnet is designed to manipulate frequency converters which determine motor speed.

Posted by [timothy](#) on Sun Mar 22, 2009 08:19 AM
from the [when-the-lights-come-on-again](#) dept.

Chinese Hackers Target Oil Companies



Internet security group McAfee Inc. has revealed that a group of hackers has carried out multiple attacks against oil companies since 2009. The hacking operation, dubbed "Night Dragon," aimed to steal information on operations and financing.

News

Minister' Integral Energy virus outbreak a threat to power grid

By R. MOSES
October 1, 2009

The screenshot shows a BBC News Business article. The header includes the BBC logo, 'Mobile', and navigation links for News, Sport, Weather, iPlayer, and TV. The main navigation bar lists Home, World, UK, England, N. Ireland, Scotland, Wales, Business, Politics, Health, Education, and Sci/Env. Sub-navigation includes Market Data, Your Money, Economy, and Companies. The article is dated 7 September 2010 and was last updated at 00:01. The title is 'Scam fear over prepayment electricity credit'. The lead text states: 'Criminals have managed to clone prepayment meter keys in order to make money by offering discounted credit to thousands of customers.' A sub-image shows a close-up of a prepayment meter key slot with the text 'Insert key to add credit or activate emergency credit'. Social media sharing icons for Facebook, Twitter, LinkedIn, and Email are visible.

Datensicherheit bei intelligenten Messsystemen

Intelligente Messsysteme (Smart Meter):

- Austausch persönlicher Daten über öffentliche Netze
- Schlüsselrolle im Smart Grid - Erzeugen einen entsprechenden Anreiz
- Sicherheitslücken sind dann i.d.R öffentlich verfügbar
- Beispiele:
 - DVD-Kopierschutz
 - Videospiele-Konsolen
 - PayTV

Der Fall „Niederlande“

”TILT Analyse der „Dutch Smart Meter Directive“ 2008

Die Analyse identifizierte, dass die DSMD Artikel 8 ECHR (Right to Privacy) verletzt:

1. Übermittlung von 15 min./stündlichen Werten zum Verteilnetzbetreiber
2. Übermittlung von täglichen Werten zu Verteilnetzbetreiber und Versorger
3. Verpflichtende Benutzung des Smart Meter



Fallstricke

Persönliche Daten

- Mangelhafter Schutz
- Mißtrauen der Bevölkerung
- Manipulation / Betrug
- Mangelnde Rechtssicherheit

Nichtpersönliche Daten

- Manipulation
- Mangelnde Rechtssicherheit

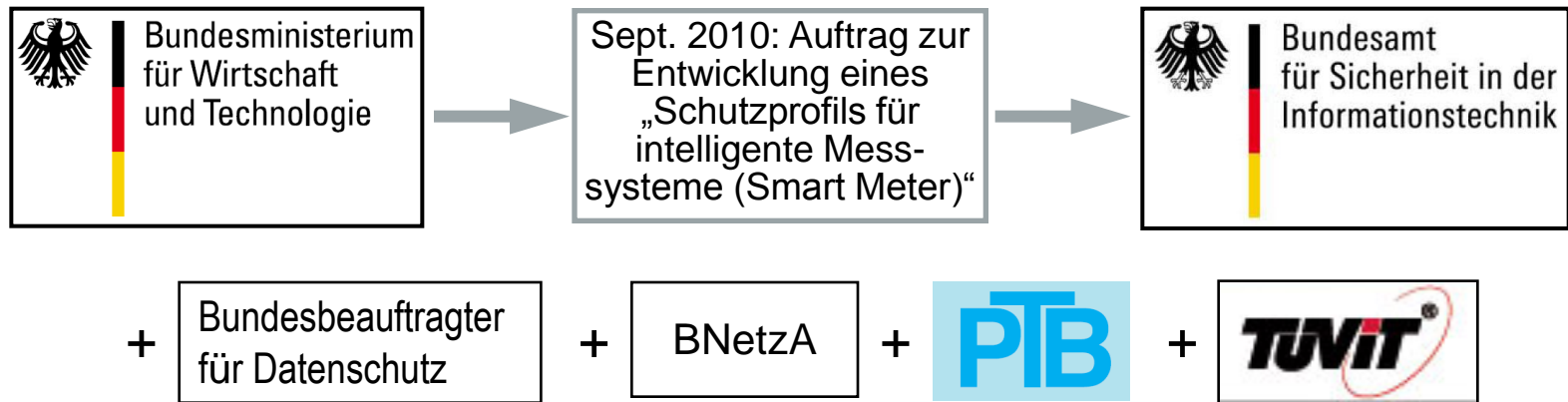
Kritische Infrastruktur

- Ziel terroristischer / verbrecherischer Angriffe

Folge

- Hohe Anforderungen an Datenschutz und Datensicherheit
- Mögliche Lösungen:
 - Explizite Einwilligung des Kunden
 - Aggregation von Daten
 - Anonymisierung von Daten
 - Vermeidung von Daten
(Datensparsamkeit – BDSG § 3a)
 - Gesetzliche Regelungen
- Aktive Adressierung der Thematik von Anfang an notwendig

In Deutschland



- Kein eigenes Datenschutzgesetz für die Energiewirtschaft in Planung
=> Anwendung eines Schutzprofils (ein in der IT-Sicherheit etabliertes Verfahren) auch für Smart Meter
- Ziele:
 - Fertigstellung des Schutzprofils bis Mitte 2011
 - Verbindlich für Smart Meter in Deutschland

Deutschland II

- Projekt SELMA: Sicherer Elektronische Messdaten Austausch
- Im Rahmen der VERNET Programmes vom BMWA gefördert
- Energieversorger, Zählerhersteller, Forschung, PTB
- Fokussierte, auf das Wesentliche reduzierte Lösungen
- **2005 !!!**

In Europa

20 / 20 / 20 EU Target: 20% CO2 reduction, 20% renewable energy, 20% energy consumption reduction

Expert Group 1:
Regulatory
functionalities for Smart
Grids and Meters

Expert Group 2:
Regulatory
recommendations for data
safety, data handling and
data protection

Expert Group 3:
Roles and
responsibilities of actors
involved in Smart Grids
deployment

EG2 – Datensicherheits Empfehlungen

- Smart Grid products and solutions should be designed incorporating data privacy and security principles at their core
- Security levels need to be defined from minimum to advanced and the costs for the different security levels to be estimated
- A specification should not preclude the initial adoption of symmetric key followed by a further smooth migration to asymmetric key cryptography (if required)
- Conduct study on how to handle multi-national key management (PKI)
- One generic model is adopted by all European countries, for key management, and security and privacy principles

EG2 – Datensicherheits Empfehlungen

- The Expert Group's recommendation is to distinguish between personal and non-personal data to minimize the exposure of personal data
- Personal data is considered as specific data and can be traced back to the individual consumer whereas non personal data could be aggregated and / or anonymous
- To ensure data safety and security a clear division of roles and responsibilities of all parties involved has to be defined

Sicherheit ist heute schon machbar

- in Stromzählern
- in batteriebetriebenen Verbrauchszählern
- Mögliche Verschlüsselungstechnologien :
 - Zertifikat-basiertes Sicherheitskonzept
 - ECC 256 Bit asymmetrische Verschlüsselung
 - AES 128 Bit symmetrische Verschlüsselung
 - SHA-256 Hash-Algorithmus
 - ECDH Schlüssel-Austausch
 - ECDSA Digitale Signaturen
 - ...



Zusammenfassung

- Datenschutz (Privatsphäre) und Datensicherheit müssen integraler Bestandteil smarterer Infrastrukturen sein
- Datensicherheit als holistischer Ansatz
- Ende-zu-Ende Schutz
- Technologien sind ausgereift, verfügbar und ökonomisch umsetzbar – auch in Batteriegeräten

....Heute ist Gestern Vergangenheit!