www.pwc.de

Anforderungen an die Datenkommunikation und Datenschutz

Workshop zum Messstellenbetriebsgesetz

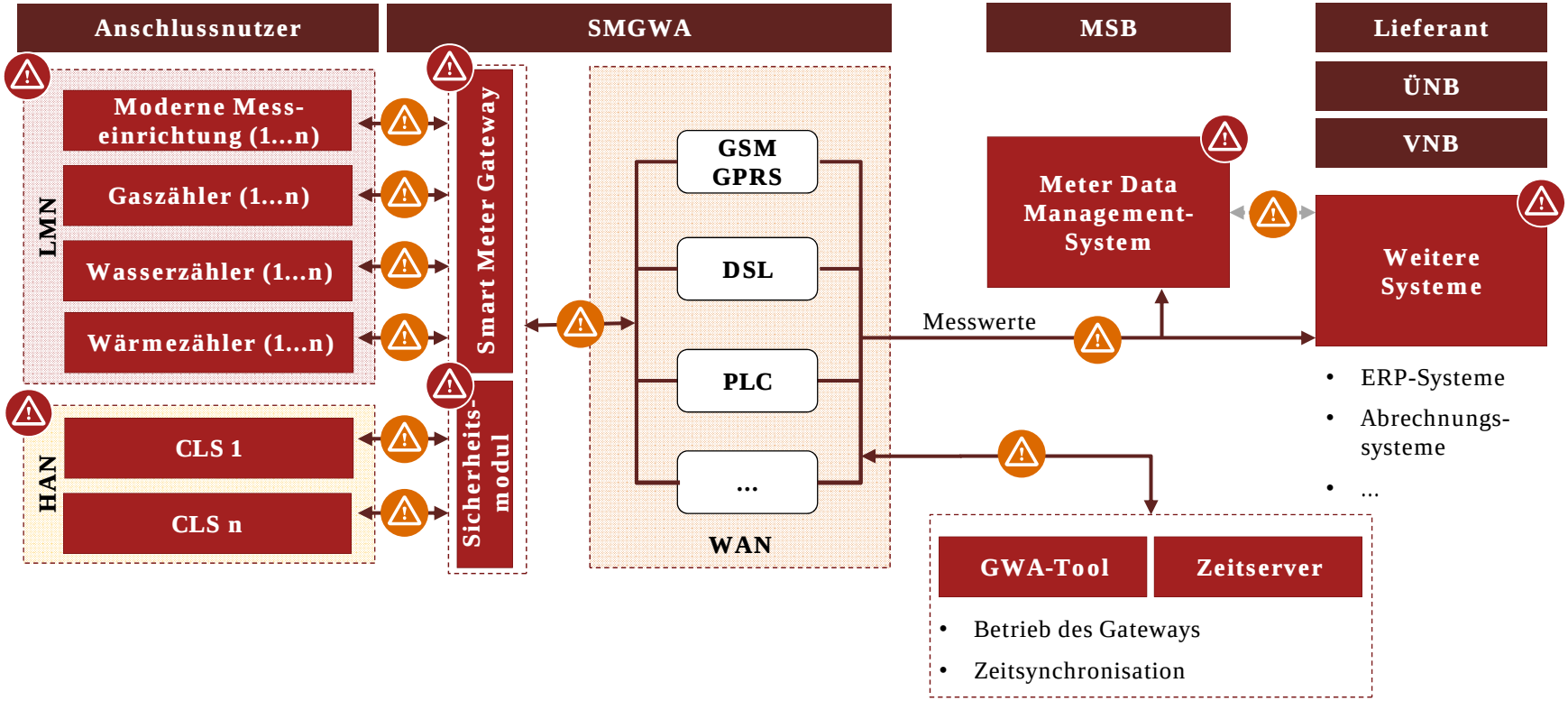
Mai 2017

pwc

Agenda

1. Systemlandschaft und relevante Schnittstellen
2. Auswahl Kommunikationstechnologien für die WAN-Schnittstelle
3. Datenkommunikation im Zielmodell
4. Kurzfristige Anforderungen des Interimsmodell für die Marktkommunikation
5. Datensicherheit im Smart Meter Bereich

Die energiewirtschaftliche Systemlandschaft weist eine Vielzahl an Schnittstellen auf



Beim Design und der Überwachung der Schnittstellen sind rechtliche, prozessuale und technische Anforderungen zu beachten

Basiszähler: die moderne Messeinrichtung wird an allen Messstellen verpflichtend

Quelle: Heinz Lackmann GmbH & Co. KG.

Messen

- Messen des Stromverbrauchs und ggf. der Einspeisung
- Erfassen der tatsächlichen Nutzungszeit
- Messen von Frequenz, Spannung oder Strom (Netzbetriebsrelevante Daten)

Sicherheit

- Einhaltung Sicherheitsanforderungen in Bezug auf Datenschutz und Datensicherheit
- Persönlicher Zugangsschutz
- Manipulationserkennung

Informieren

- Vorhaltung und Anzeige am Messgerät (24 Monate = 730 Tageswerke, 104 Wochenwerte)
- Optische Datenschnittstelle für Letztverbraucher
- Schnittstelle zur Anbindung an ein Gateway

Moderne Messeinrichtungen müssen vollständig bis 2032 vollständig ausgerollt werden und ersetzen die klassischen Zähler

Smart-Meter-Gateway: als zentrale Kommunikationseinheit des intelligenten Messsystems

Quelle: Sagemcom Dr. Neuhaus GmbH

Kommunizieren

- Schnittstellen zu WAN, HAN, LMN
- Bidirektionale Kommunikation über die Schnittstellen

Daten

- Erfassung, Zeitstempelung, Tarifierung, Übermittlung, Speicherung und Löschung von Messwerten und damit zusammenhängender Daten

Sicherheit

- Gewährleistung Datenschutz, Datensicherheit und Interoperabilität
- Kommunikation nur vom Gateway aus und nur mit berechtigten Marktteilnehmern (Rollenprüfung)
- Alle Kommunikationsflüsse sind verschlüsselt und in Bezug auf Integrität, Authentizität und Vertraulichkeit abgesichert

Noch ungelöste eichrechtliche Fragestellungen zu beachten

Das SMGW ist der Datenspeicher, Datenaufbereiter und die Firewall zwischen Zählertechnik, Außenwelt und lokalem Umfeld

Generelle Anforderungen an die TK-Technologie für das Smart Meter Gateway

Anforderung	Erläuterung
Ortsverfüg-barkeit	• Wichtigste, nicht unmittelbar technische Anforderung an WAN-Kommunikationssystem
Ausfall-sicherheit	• Bei einigen Nutzergruppen teilweise hohe Anforderungen an die Kommunikation
Zukunfts-sicherheit	• Zukunftssicherheit aller Komponenten wichtig • Die Zukunftssicherheit geeigneter WAN-Technologien sollte sich im ersten Rollout über eine Eichperiode erstrecken
Leistungs-fähigkeit	• Wichtige Eigenschaften wie abzuführende Datenvolumina, minimale Anschlussdatenraten etc. müssen beachtet werden

Übersicht über bestehende WAN-Kommunikationstechnologien

Quelle: 3U TELECOM GmbH

?

Quelle: Sagemcom Dr. Neuhaus GmbH

Drahtgebundene Technologien	DSL Glasfaser Kabelmodem
Powerline Communication (PLC)	G3-PLC BPL
Drahtlose Technologien	GPRS/GSM UMTS/HSDPA LTE

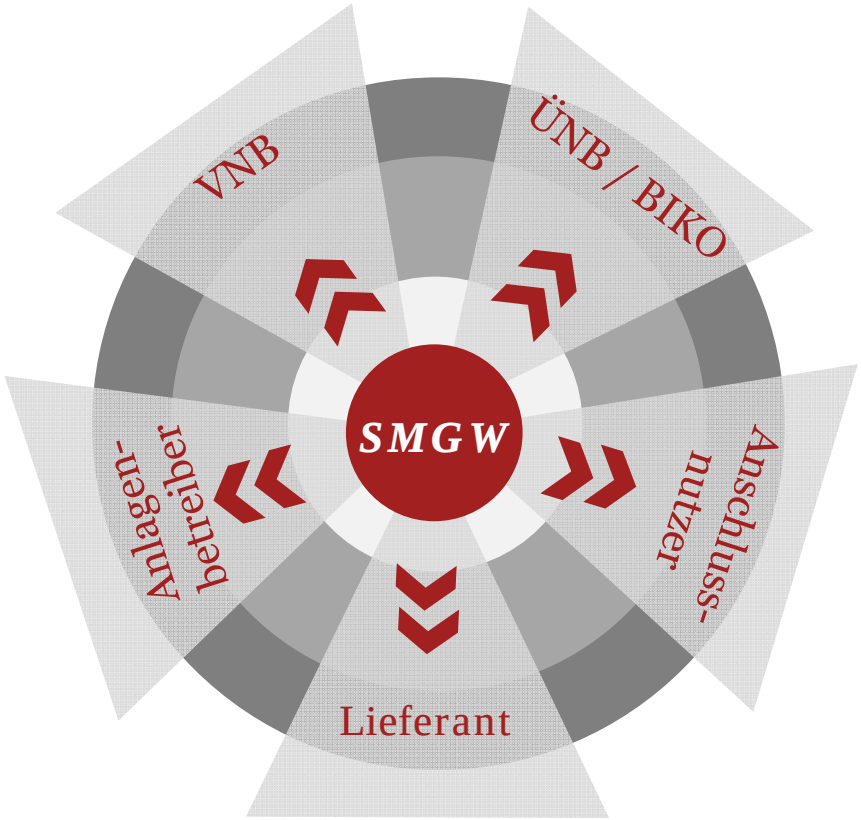
Die Kommunikationstechnologien im Vergleich

	Performance			Hintergrund

Drahtgebundene Technologien		**DSL/ Kabel**	**Glasfaser**	• Keine flächendeckende Versorgung aber sehr hohe Durchdringung
				  • DSL: Ca. 38 Millionen Haushalte
				  • Kabel: Ca. 28 Millionen Haushalte
				  • Glasfaser: ca. 1 Millionen Haushalte
				• Ggf. Probleme bei Nutzung bestehender Anschlüsse

	Downstream	24 Mbit/s	128 Mbit/s	
	Upstream	1 Mbit/s	5 Mbit/s	
	Latenzzeiten	Kurz	Kurz	
PLC	**G3-PLC**		**BPL**	• Hohe Anfangskosten • Bisher wenige Anbieter auf dem Markt • Gerätekosten streuen sehr stark zwischen Anbietern und Stückzahlen
	• Ausreichende Datenraten • hohe Reichweiten		• Hohe Datenraten • geringe Reichweite	
Drahtlose Technologien		**GSM/GPRS**	**UMTS**	**LTE**	• KNA geht von Verfügbarkeit an der Messstelle von 20-50% ohne separate Verstärkerantenne aus • Pilotprojekt Bayernwerk: 85% ohne externe Antennen • VKU AG Smart Metering: 57% mit akzeptabler Signalstärke
	Downstream	220 kbit/s	14,4 Mbit/s	100 Mbit/s	
	Upstream	110 kbit/s	5,8 Mbit/s	50 Mbit/s	
	Latenzzeiten	Hoch	Kurz	Kurz	

Zielmodell: Der Messstellenbetreiber ist die neue Datendrehscheibe für die Datenkommunikation



Zielmodell der sternförmigen Kommunikation tritt zum 01.01.2020 in Kraft; für den Übergangszeitraum gelten Anforderungen des Interimsmodells

Interimsmodell für die Marktkommunikation: Anforderungen sind bereits 2017 umzusetzen

Marktlokation und Messlokation

- Einführung der Begriffe Marktlokation und Messlokation (alle ZP)
- Einführung eindeutiger Identifikationsummern (IDs) bis zum **1. Februar 2018**
- Generierung und Vergabe der Marktlokations-ID durch zentrale Codevergabestelle – Beantragung und Zuordnung durch NB

Verschlüsselung S/MIME

- Absicherung sämtlicher EDIFACT-Nachrichten zur Marktkommunikation mittels Signatur und Verschlüsselung spätestens ab dem **01.06.2017**
- Zertifikatserstellung nur durch Zertifizierungsstelle

Aufgrund der Datenvielfalt in der bestehenden Systemlandschaft wird der Umbau des Stammdatenmodells systemübergreifend geschehen müssen

Im Rollenmodell für die Marktkommunikation werden neue Begrifflichkeiten eingeführt

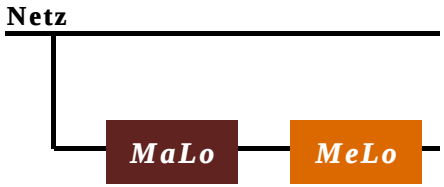
Marktlokation

- Einer Marktlokation ist jeder Punkt, an dem Energie erzeugt oder verbraucht wird und der über mindestens eine Leitung mit dem Netz verbunden ist
- Entspricht einer Einspeise- bzw. Entnahmestelle im Sinne der StromNZV
- Wenn an einem Standort Marktlokationen vorhanden sind, die Energie erzeugen und Energie verbrauchen, werden diese als separate Marktlokationen behandelt
- Die Generierung und Ausgabe der IDs der Marktlokation erfolgt durch eine zentrale Code-vergabestelle, die Zuordnung durch den Netzbetreiber

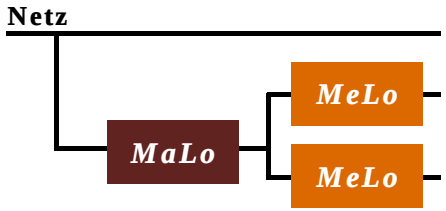
Messlokation

- Eine Messlokation ist eine Lokation, an der Energie gemessen wird und die alle technischen Einrichtungen beinhaltet, die zur Ermittlung und ggf. Übermittlung der Messwerte erforderlich sind
- Entspricht der Messstelle im Sinne des § 2 Nr. 11 MsbG
- Jede relevante physikalische Größe zu einem Zeitpunkt maximal einmal ermittelt
- Die ID ist die Zählpunktbezeichnung gemäß VDE-AR-N 4400 und wird durch den Netzbetreiber vergeben

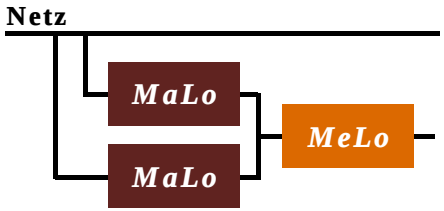
Drei Ausprägungsformen möglich:



1:1 Beziehung: Die Energie einer Marktlokation wird mit genau einer Messlokation gemessen

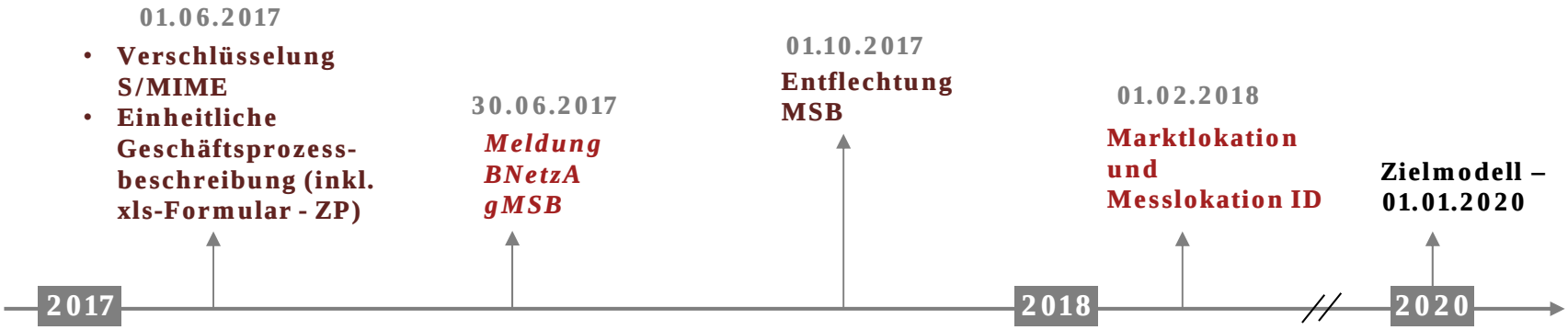


1:n Beziehung: Für die Erfassung der Energie der Marktlokation wird mehr als eine Messlokation benötigt



n:1 Beziehung: Eine Messlokation ist für die Erfassung der Energie mehrerer Marktlokationen erforderlich

Bei den Umstellungen sollten EVUs die Anforderungen des Zielmodells bereits im Blick haben

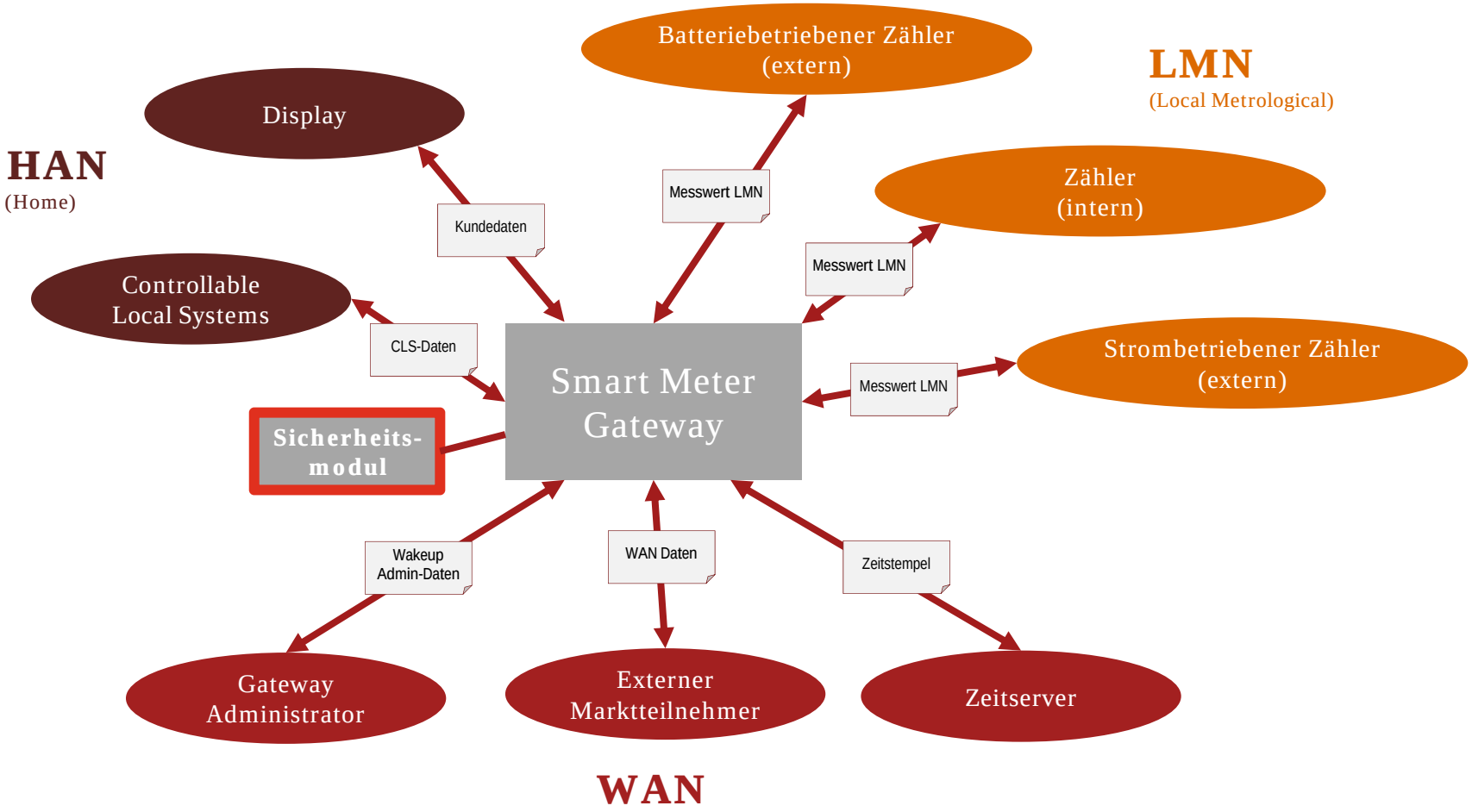


Wichtigste Risikofelder bei der Umsetzung:

Fehlerhafte Systemanpassung	Strategische Überlegungen nicht vollumfänglich abgebildet	Prozesseinführung MSB-Abrechnung	Anpassung von Prozessen und Systemen
Fehlerhafte Markt-kommunikation	Überschreiten von Fristen	Systemische Umsetzung der Entflechtungs-anforderungen	Fehlerhafte Splittung der Stammdaten-konstrukte
Überschreiten von Fristen	Ggf. Einleitung Ausschreibungs-verfahren	Fehlerhafte Abrechnung	Überschreiten von Fristen
		Überschreiten von Fristen	

Bei allen Schritten der Umstellung sind wesentliche IT-und Prozessrisiken insbesondere bei Relevanz für die Rechnungslegung zu beachten

Smart Meter im Brennpunkt Cyber Security



Es gelten hohe Anforderungen für Smart Meter an Datenschutz und Informationssicherheit, insbesondere am Smart-Meter-Gateway als Bindeglied der unterschiedlichen Netze.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf?__blob=publicationFile

Messstellenbetreiber müssen verschiedene Sicherheitsaspekte beachten

Schutz der kundenseitigen Verbrauchsdaten

- Unberechtigte Kenntnisnahme
- Unberechtigte Auswertung

Schutz der Smart Meter Steuerdaten

- Manipulation hinsichtlich Datenschutz und IT-Sicherheit
- Eingriff in den Energiefluß (z.B. regionale Abschaltung)

Schutz aller IT-Systeme vor Angriffen aus dem Smart Grid

- Jedes System ist angreifbar
- Zunehmende, komplexe und massivere Angriffe von Hackern insbesondere auf Netzwerke und Applikationen
- Gefahr durch Aufweichung der klaren Trennung zwischen Versorgungs- und IT-Netz

Es ist wichtig, systematisch die Sicherheit im Gesamtsystem zu hinterfragen

- Sicherheit der physischen Komponenten
- Sicherheit der Software (BSI TR-03109)
- Sicherheit der verbundenen IT

Architektur	Quellcode	Programmverhalten
• Identifikation Assets • Bedrohungsanalyse • Bedrohungsmodell • Datenflussanalyse • Schnittstellenanalyse • Analyse des Sicherheitsdesigns • Identifikation der Sicherheitslücken	• Code Reviews • Tool-basiert • White-Box Ansatz • Syntax, Semantik • Anwendung formaler Rahmen für sichere Software-Entwicklung	• Black-Box-Ansatz • Robustness Testing/ Fuzzing • Zufällig generierte Massendatentests

BSI TR-03109: Technische Vorgaben für intelligente Messsysteme und deren sicheren Betrieb

Interoperabilität im Smart Grid

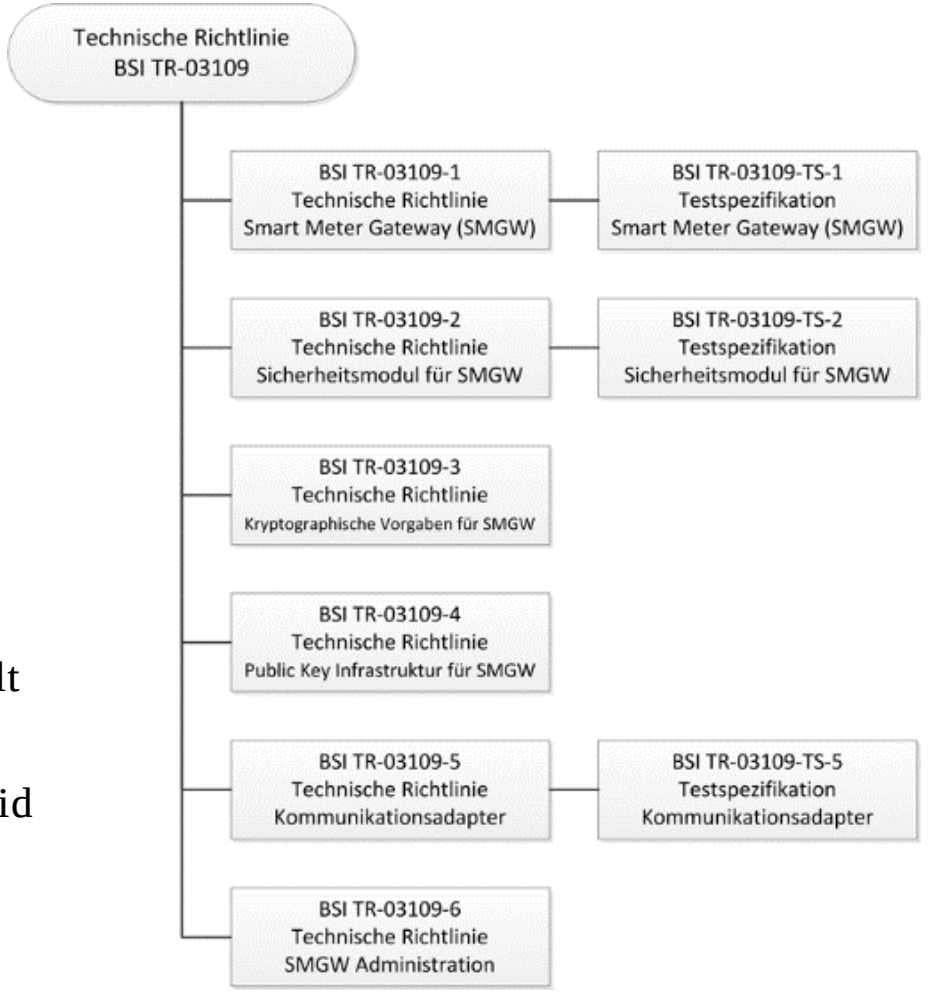
Sicherheitsanforderungen in der Kommunikation

- Vertraulichkeit
- Datenintegrität
- Authentizität

Transport Layer Security für alle bidirektionalen Kommunikationsverbindungen

Zählerdaten grundsätzlich verschlüsselt

Ziel: SMGW als hochsichere Kommunikationszentrale im Smart Grid



https://www.bsi.bund.de/SharedDocs/Bilder/DE/BSI/Publikationen/Techn_Richtlinien/tr031 09_struktur.png;jsessionid=35D419D58D8C7413F3AAF3280B2AA7D1.1_cid360?__blob=poster&v=2

Der SMGW Administrator als Gralshüter

Funktionale Anforderungen

Informationssicherheit (Prozess, Maßnahmen, Risikomanagement, PKI-Betrieb, Updates), Monitoring, Change-Management, Asset-Management, Profilverwaltung, Kommunikation, Störungs-management, Zertifikatsmanagement

Betrieb und Sicherheitsanforderungen

- Verantwortet zuverlässigen technischen Betrieb (§ 25 Abs. 1 MsbG)
- Verankerung von entsprechenden Mindestanforderungen im MsbG (u.a. Verweis auf BSI TR-03109-6)
- Obligatorisches ISMS
- Nachweis durch ISO 27001-Zeritifzierung

Das Aufgabenprofil des SMGW Admin ist hochkomplex, risikobehaftet und nur im Bereich der technischen Anforderungen im Ansatz geregelt.

Mindestanforderungen und sichere Anbindung an Smart Meter

§ 22: Mindestanforderungen

- Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität nach dem Stand der Technik
- Schutzprofile und Technische Richtlinien veröffentlicht das BSI

Fragestellungen

- Definition „nach dem Stand der Technik“ geht aus dieser Regelung nicht eindeutig hervor, es wird lediglich „vermutet“ und bietet Interpretationsspielraum, da dies beim BSI noch nicht vollständig geregelt ist
- Erreichen der Ziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität (TLS-Handshake, Public-Key-Infrastruktur), Verbindlichkeit und Zurechenbarkeit

§ 23: Sichere Anbindbarkeit

- Vorgaben an die Ausgestaltung zur Einbindung in das Kommunikationsnetz
- Benennung der Komponenten und Anlagen für eine sichere Einbindung und Erfüllung der technischen Mindestanforderungen
- Die Definition von Komponenten und Anlagen sind abschließend vom Gesetzgeber aufgezählt, z.B. Erzeugungsanlagen nach dem EEG und KWKG

Smart Meter Zertifizierung

§ 24: Zertifizierung

- Erstellung von Sicherheitszertifikaten nach „Common Criteria“ durch das BSI
- Ziel ist es, Rechtssicherheit für Hersteller und Anwender zu gewährleisten

Fragestellungen

- Gestaltung des Zertifizierungsprozesses durch das BSI, insbesondere durch die zeitliche Befristung und Beschränkung
- Absicherung für eine sichere Anbindung, da nur das Gateway selbst zertifiziert wird
- Risikobehandlung, falls Geräte verwendet werden, die nicht zertifiziert sind (eigenes Risiko des Administrators)
- Gültigkeit Sicherheitszertifikate anderer Zertifizierungsstellen
- Parallele Aufsichtsmaßnahmen der Bundesnetzagentur (§76)
- Umfang und Vollständigkeit der „Common Criteria“-Regelungen

§ 25: Administrator-Regelung

- Verbot hinsichtlich Verwendung nicht zertifizierter Smart-Meter-Gateways
- Übermittlung der Daten unter Beachtung u.a. datenschutzrechtlichen Vorgaben
- Verpflichtung zur Einrichtung eines ISMS (Akkreditierung BSI oder ISO 27006), Erstellung IT-Sicherheitskonzeption

Fragestellungen

- Regelung der Mindestanforderungen an den Administrator in personeller und wirtschaftlicher Hinsicht (hier nur technischer Betrieb)
- Keine Schwellwerte für „Zuverlässigkeit“, Verfügbarkeit lediglich über möglichst geringe „Down-Time“ und „Mean Time between Failures“
- Effizientes Management der zu transferierenden Daten
- Umsetzung zu Verfügbarkeit, Vertraulichkeit und Integrität (z.B. asymmetrische Verschlüsselungen, Signaturen, Protokolle, etc.)
- Notwendige ISMS-Ergänzung, wie z.B. Risiko-management oder Mitarbeitersensibilisierung

Smart Meter einheitliches Sicherheitsniveau und Weiterentwicklung durch einen Ausschuss

§ 26: Sicherheitsniveau

Zur Sicherstellung und Aufrechterhaltung eines einheitlichen Sicherheitsniveaus wurden das BSI

- mit Aufgaben zur Analyse, Priorisierung und Bewertung der Smart Meter Gateway Schwachstellen betraut
- zum Erlass für Vorgaben für den SMGW-Administrators ermächtigt

Fragestellungen

- Definition „hoher Standard an Datenschutz und Datensicherheit“
- Einrichten eines Meldeprozesses

§ 27: Schutzprofile, Richtlinien

- Regelung Weiterentwicklung Schutzprofile und Technische Richtlinien durch das BSI
- Ein Ausschuss für Gateway-Standardisierung ist vorhanden (u.a. Bundesministerium für Wirtschaft und Energie, BSI, Physikalisch-Technische Bundesanstalt, Bundesnetzagentur)
- Einbezug des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Kontrolle und Wahrung der gesetzlichen Kompetenzen (auch personenbezogene Daten)

Smart Meter Zertifikatsmanagement

§ 28: Wurzelzertifikate

- Sicherstellung, dass durch die durch Smart Meter erfassten und übermittelten Daten hinreichend sicher vor dem Zugriff unberechtigter Dritter geschützt werden
- Das BSI ist die Zertifizierungsinstanz und hat die Inhaberschaft über die Wurzelzertifikate

Fragestellungen

- Gestaltung „Wurzelzertifikate“
- Umsetzung von Verschlüsselung und Signatur der Daten für verschlüsselte und integritätsgesicherte Kanäle (Authentizitätsnachweise)
- Vorschrift zur Teilnahme an der Metering-Public-Key-Infrastruktur

Vielen Dank für Ihre Aufmerksamkeit.

PricewaterhouseCoopers GmbH
Wirtschaftsprüfungsgesellschaft
Bernhard-Wicki-Straße 8
80636 München

Telefon: +49 89 5790-5425
joerg.netzband@de.pwc.com
www.pwc.de

Jörg Netzband
Partner
Risk Assurance / PS, Energy

PricewaterhouseCoopers GmbH
Wirtschaftsprüfungsgesellschaft
Moskauer Str. 19
40227 Düsseldorf

Telefon: +49 211 981-2192
derk.fischer@de.pwc.com
www.pwc.de

Derk Fischer
Partner
Risk Assurance /
Informationssicherheit