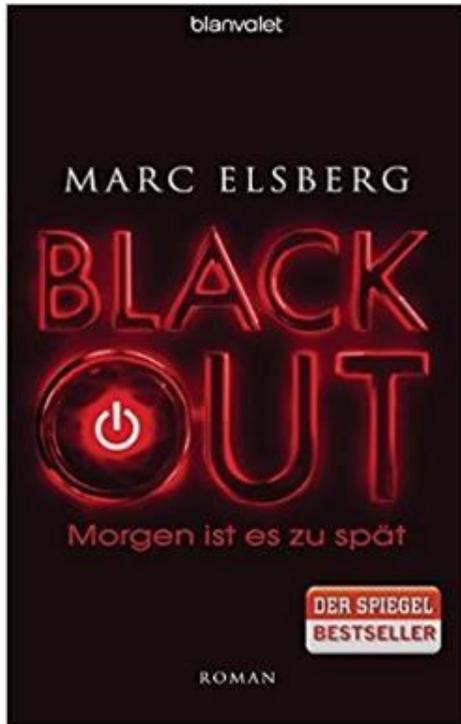


Nationale Maßnahmen zur Absicherung intelligenter Messsysteme (Smart Meter)

Vortrag: Dr. Michael Schafferer





„BLACKOUT - Morgen ist es zu spät“
von Marc Elsberg

„[...] An einem kalten Februartag brechen in Europa alle Stromnetze zusammen. Der totale Blackout. Der italienische Informatiker Piero Manzano vermutet einen Hackerangriff und versucht, die Behörden zu warnen – erfolglos. Als Europol-Kommissar Bollard ihm endlich zuhört, tauchen in Manzanos Computer dubiose Emails auf, die den Verdacht auf ihn selbst lenken. Er ist ins Visier eines Gegners geraten, der ebenso raffiniert wie gnadenlos ist. Unterdessen liegt ganz Europa im Dunkeln, und der Kampf ums Überleben beginnt ...“

Vermutung:

Manipulationen an den intelligenten Stromzählern als Ursache des Ausfalls

Interview: Marc Elsberg zum Buch

- ⬡ [...] Ich fragte mich, womit **Verbrecher oder Terroristen größtmöglichen Schaden** anrichten könnten. Sobald man sich mit der Materie auseinandersetzt, bleiben bald nur mehr zwei Bereiche: **Kommunikation und vor allem Energie**. [...]
- ⬡ [...] Bestürzt hat mich bei meinen Recherchen die Tatsache, dass europaweit technische Systeme (Smart Meter/„intelligente Stromzähler“) **eingebaut werden (müssen), die nicht die notwendigen Sicherheitsstandards aufweisen** – und sich die **Industrie dessen bewusst** ist. [...]
- ⬡ [...] Dass die verantwortlichen **Politiker entweder zu ahnungslos, uninteressiert oder zu sehr von anderen Interessen gesteuert** sind, um diese Systeme sicherer zu machen. Wobei wir uns da natürlich auch alle selbst an die Nase fassen müssen, schließlich haben wir diese Leute gewählt und tun durch Ignoranz das unsere dazu. [...]
- ⬡ [...] Erschreckend fand ich auch, wie **wenig Gedanken sich Verantwortliche selbst in führenden Positionen über die weitergehenden Auswirkungen** ihres Handelns machen, aber auch wie wenig Wissen sie zum Teil darüber überhaupt besitzen. Wahrscheinlich bedingt eines das andere. Kaum jemand sieht das ganze Bild. [...]

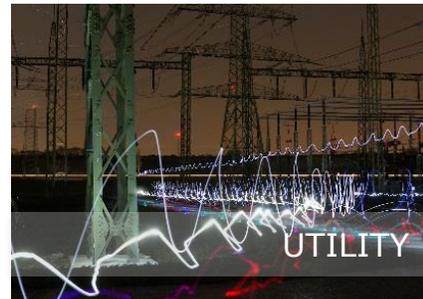
Quelle: <https://images-eu.ssl-images-amazon.com/images/G/03/books/PDF/leseproben/9783764504458.pdf>



No „Black Out“

Nationale Maßnahmen zur Absicherung intelligenter Messsysteme (Smart Meter)

- ⬡ Rail
- ⬡ Road
- ⬡ Aviation
- ⬡ Utility
- ⬡ Public Safety



Fiktion
oder
Reale Gefahr



Spanische Smart Meter können einfach gehackt werden

© Bild: Benjamin Sterbenz

UK smart vulnerable attacks –

Spanische Sicherheitsforscher haben auf der Black Hat Europe einen Hack eines intelligenten Stromzählers gezeigt, mit dem ein Blackout verursacht werden kann.

The government's plan to install smart energy meters into UK homes, could leave households vulnerable to cyber attacks



Smart electricity meters can be dangerously insecure, warns expert

Hackers can cause fraud, explosions and house fires, and utility companies should do more to protect consumers, conference told

The big problem is that the smart servants who do not have a clue footing the bill



▲ Smart meters are frequently dangerously insecure, a security expert has warned.

Smart electricity meters, of which there are more than 100m installed around the world, are frequently "dangerously insecure", a security expert has said.

Reale Gefahr



SECURITY Your smart electricity meter could be a security risk

A new report details how hackers could use your smart meter to figure out what you're doing at home -- and when you're out.

24. August 2017, 19:52 Uhr Smart Home

Sorge um Sicherheit von smarten Stromzählern



21/12/2015

Intelligente S

Ein "intelligenter Stromzähler" wird bei den 1. Hamburger Energietagen vorgestellt. (Foto: Maja Hitij/dpa)

Intelligente Stromzähler werden bald Pflicht für viele Haushalte. Forscher warnen vor Sicherheitslücken - und dem Risikofaktor Mensch.



Intelligente Stromzähler sind künftig unumgänglich. Die sogenannten Smart Meter stehen jedoch im Verdacht, besonders anfällig für Hacker-Angriffe zu sein. Das hat nicht nur Auswirkungen auf den einzelnen Verbraucher. Im schlimmsten Fall könnten so ganze Stromnetze lahmgelegt werden.

“Smart electricity meters can be dangerously insecure.”

Netanel Rubin von Vultra

- ⌘ The problems at the heart of the insecurity stem from outdated protocols, half-hearted implementations and weak design principles.
- ⌘ While the physical security of smart meters is strong – “trust me, I tried” to hack in that way, Rubin said – the wireless protocols many of them use are problematic.
- ⌘ Worse still, said Rubin, all the meters from one utility used the same hardcoded credentials. “If an attacker gains access to one meter, it gains access to them all. It is the one key to rule them all.”
- ⌘ “This unique situation is so difficult to implement, vendors actually choose what they want to implement. And when they choose what to support, they more often than not skip security,” Rubin said.

Quelle: <https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers>

Weak security decisions made by vendors include:

- ❏ Encryption keys derived from short (often just six-character) device names.
- ❏ Pairing standards with no authentication required, allowing an attacker to simply ask the smart meter to join the network and receive keys in return.
- ❏ Hardcoded credentials, allowing administrator access with passwords as simple and guessable as the vendor's name.
- ❏ Code simplified to work on low-power devices skipping important checks, allowing nothing more than a long communication to crash the device.

Quelle: <https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers>

Sicherheitsexperte Simen Sandberg berichtete über die Sicherheits- und Schwachstellenanalysen zur Einführung der Smart Meter in Norwegen.

- ❏ Hier treffen unterschiedliche Faktoren aus Politik, Wirtschaft, Datenschutz und IT-Architektur zusammen, die zu Sicherheitsrisiken führen. Zum Beispiel ist die Möglichkeit einer Stromabschaltung aus der Ferne hier vom Gesetzgeber vorgeschrieben. Damit schafft sich Norwegen nach Ansicht von Sandberg über das Systemdesign ein potentiellies Angriffsziel auf den Smart Meter.
- ❏ Zudem verfügte die Vernetzung der Geräte nur über eine unzureichende Abschottung gegenüber externen Angreifern. Gelingt letzteren ein erfolgreicher Einbruch in den Smart Meter, sind die folgenden Backend-Systeme in der Cloud unzureichend abgeschottet. Praktischerweise bietet der norwegische Smart Meter eine ungeschützte RJ45-Buchse als Schnittstelle zur lokalen Wartung.
- ❏ „Security by Design sollte anders aussehen“, schlussfolgerte Sandberg.

Quelle: <https://www.heise.de/ix/meldung/loT-Sicherheitskonferenz-Unsichere-Smart-Meter-Mirai-und-seine-Klone-und-die-Genfer-Konvention-3872793.html>

Vorangegangen ist:

- ⊞ Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft, vorgestellt von der E-Control Austria (ECA) am 27. Februar 2014

Im Auftrag von „Oesterreichs Energie“, erstellt durch die Projektgruppe „End2End Security Smart Metering“:

- ⊞ Anforderungskatalog Ende-zu-Ende Sicherheit Smart Metering
- ⊞ Maßnahmendefinition entsprechend den Empfehlungen der ECA-Risikoanalyse
- ⊞ Maßnahmen beruhen auf dem heutigen Stand der Technik im Bereich der Sicherheit in der Informations- und Kommunikationstechnik

Das Ergebnis:

Anforderungen der Stromnetzbetreiber an die Hersteller und Lieferanten von Geräten und Systemen, die bei Smart Metering mit Ende-zu-Ende Sicherheit eingesetzt werden.

Dieser Katalog beschreibt:

- Mindestanforderungen an die Hersteller bei der Ausschreibung von Stromzählern, Gateways und dem Zentralen System
- Deren Kommunikationsverbindungen, die im Smart-Metering-Bereich mit Ende-zu-Ende Sicherheit in Österreich eingesetzt werden sollen.

Ziel ist die Gewährleistung der Authentizität und damit Integrität von Informationen sowie die Geheimhaltung vertraulicher Daten:

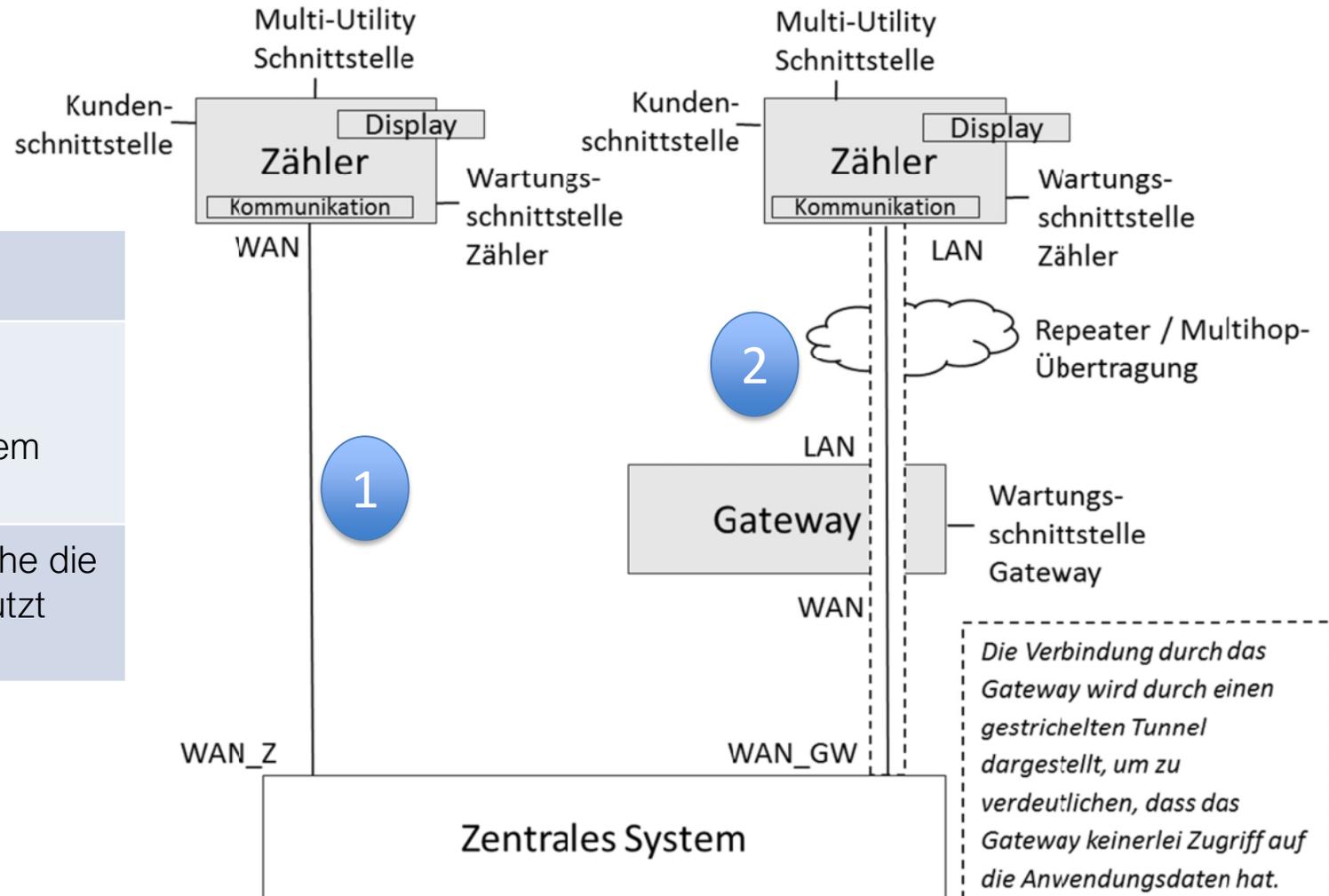
- 🔒 Allgemeine Sicherheitsanforderungen
- 🔒 Zukunftssicherheit (Aktualisierbarkeit, Performance, Konfigurierbarkeit...)
- 🔒 Schnittstellen-Reduzierung (Beschränkung Datentypen und Protokolle...)
- 🔒 Kryptografische Algorithmen (NIST SP 800-57, BSI TR-03116)
- 🔒 Datenintegrität (Authentizität und Integrität der Daten kontrollieren...)
- 🔒 Lokale Sicherung (Trennung funktionaler Blöcke nach Sicherheitsrelevanz, physische Manipulation, Zonenkonzept ZS...)
- 🔒 Zugangskontrolle (Mechanismen einer rollenbasierten Zugangskontrolle...)
- 🔒 Vertraulichkeit (Verschlüsselung auf der Anwendungsschicht...)
- 🔒 Auditierung und Protokolle (lokale & zentrale Auditierung v. Ereignissen...)
- 🔒 Produktlebenszyklus-Management (sichere Entwicklung & Produktion/ISO...)

Smart Metering: Architektur

Architektur erlaubt 2 Varianten der Anbindung:

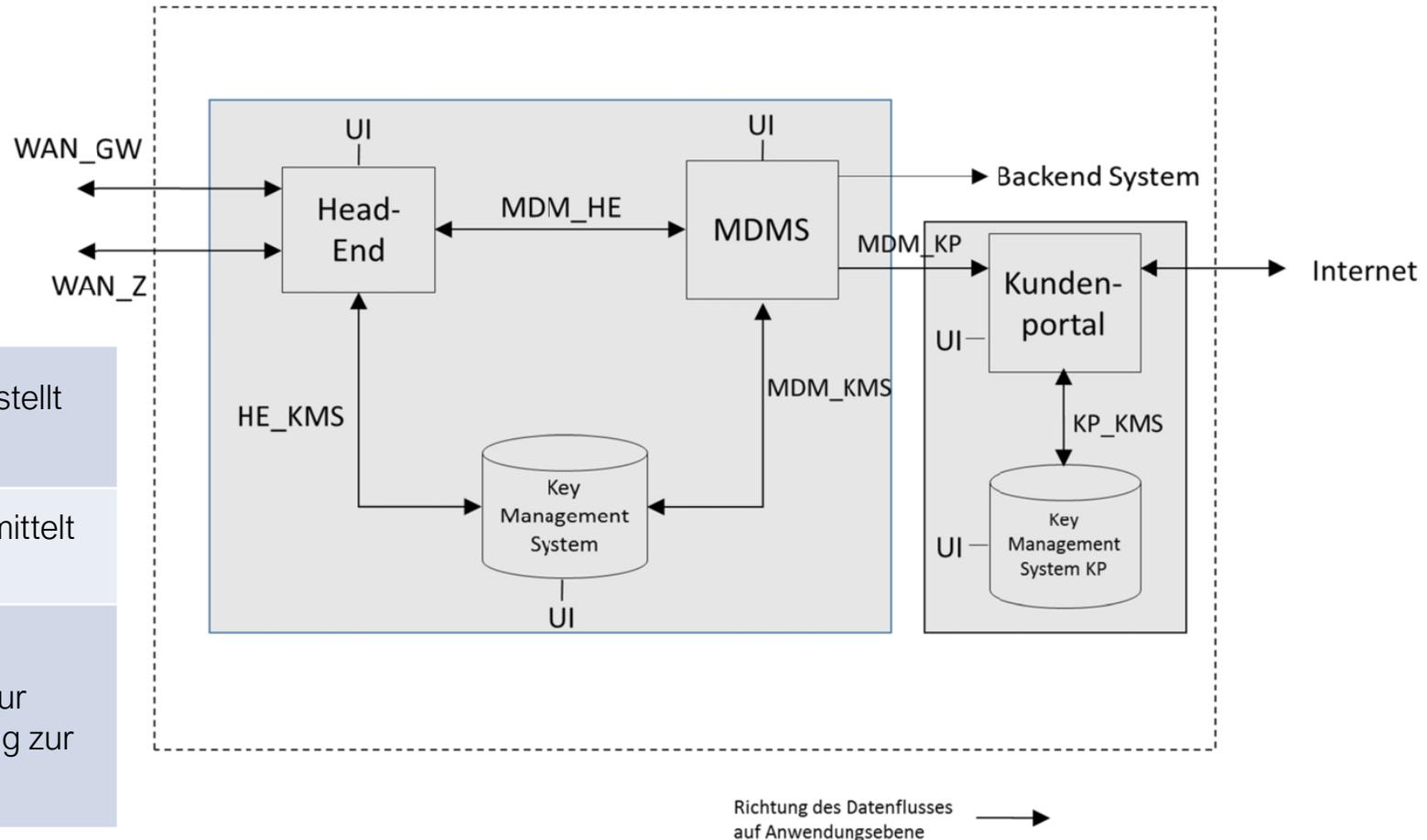
1. P2P (= Mobilfunk)
2. PLC & Gateways zum Zentralen System

| | |
|------------------|--|
| Zähler | Stellt den Smart Meter dar |
| Gateway | Transparente Kommunikationsverbindung zwischen dem Zentralen System und dem Zähler |
| Zentrales System | Verwaltungsanwendung, welche die Smart Metering Architektur nutzt und steuert |



Architektur: Zentrale Systeme

| | |
|----------|---|
| Head End | Kommuniziert mit Zählern und Gateways, stellt dem MDMS Daten zur Verfügung |
| MDMS | Speichert, bearbeitet, verwaltet und übermittelt Zählerdaten |
| KMS | Verwaltet und schützt kryptografische Schlüssel, stellt einen sicheren Speicher zur Verfügung und kontrolliert die Autorisierung zur Benutzung des Schlüsselmaterials |



Methoden: Verschlüsselung und Authentifizierung



Zur Verschlüsselung und Authentifizierung gegenüber den Zählern/Gateways wird auf folgende Methoden zurückgegriffen (definiert im s.g. Green Book):

Sichere Übertragung von/zu zentralen Systemen anhand authentisierter Verschlüsselung:

| Suite | Verschlüsselung (authentifiziert) | Digitale Signatur | Key Agreement | Hash | Key Transfer | Kompression |
|-------|-----------------------------------|-------------------|---------------|---------|------------------|-------------|
| 0 | AES-GCM-128 | - | - | - | AES-128 key wrap | |
| 1 | AES-GCM-128 | ECDSA (P-256) | ECDH (P-256) | SHA-256 | AES-128 key wrap | V.44 |
| 2 | AES-GCM-256 | ECDSA (P-384) | ECDH (P-384) | SHA-384 | AES-256 key wrap | V.44 |

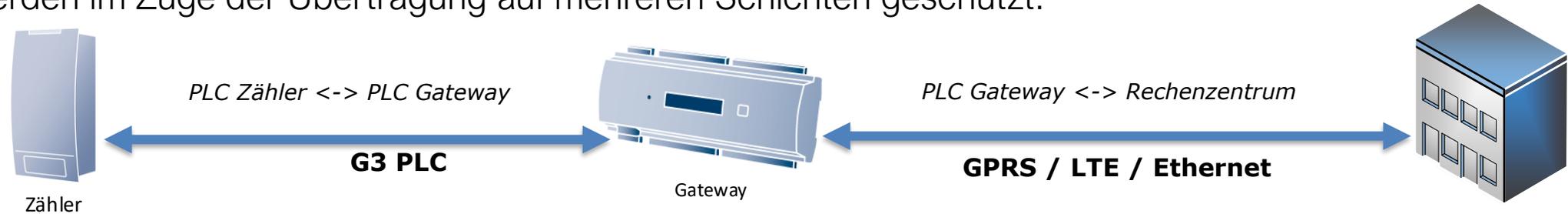
High Level Security Authentifizierung zum Session-Aufbau (= Client Association):

| Mechanismus | Bildung | Info |
|-------------|---------|---|
| HLS-5 | GMAC | |
| HLS-6 | SHA-256 | Nutzt ein zusätzliches HLS-Secret |
| HLS-7 | ECDSA | Nutzt Public Key Kryptografie anhand von Zertifikaten |

Gesicherte Datenübertragung: Beispiel

Beispiel eines Multi-Layer Security Ansatzes in PLC:

Die Daten werden im Zuge der Übertragung auf mehreren Schichten geschützt.



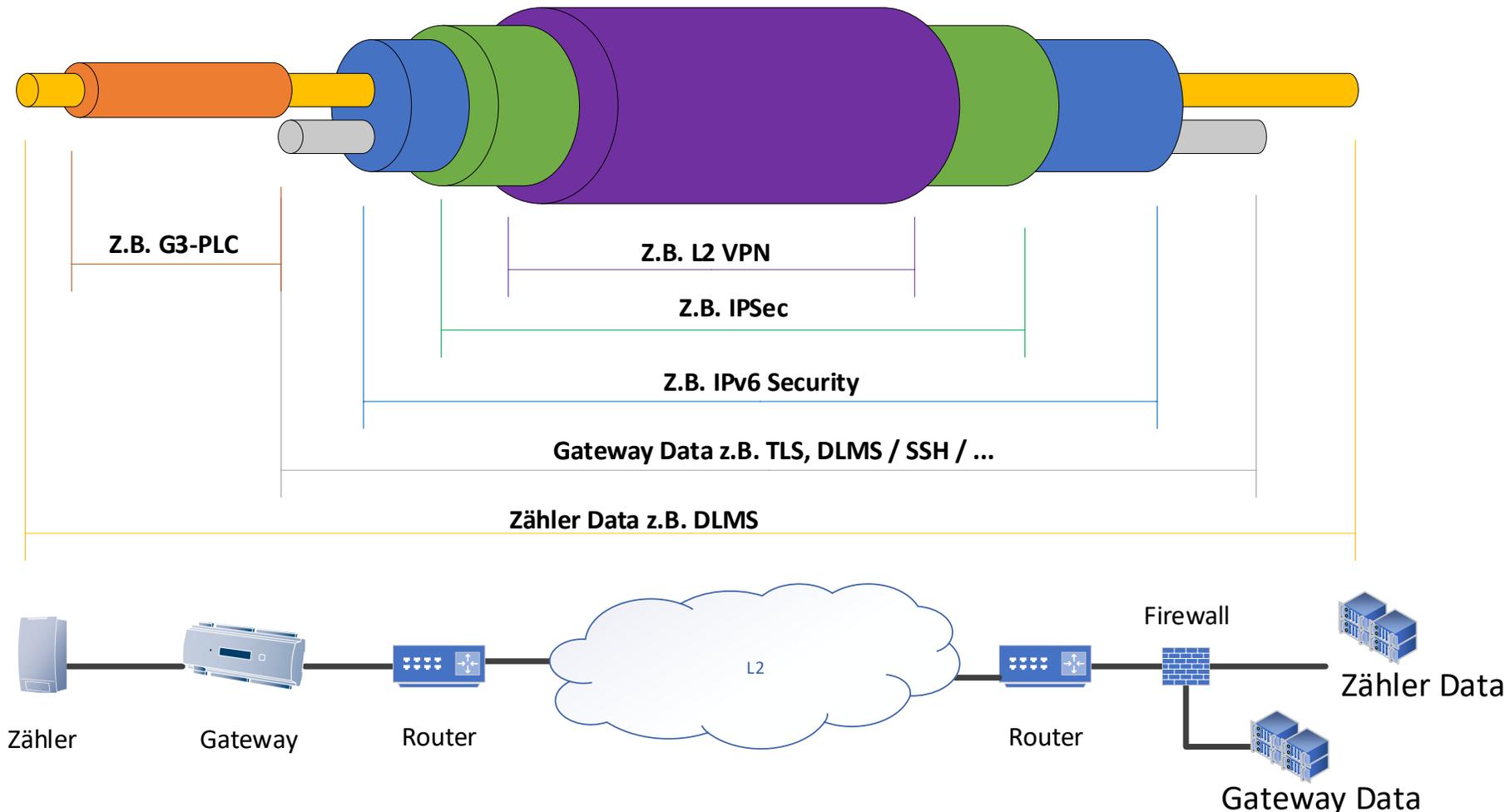
| OSI Model |
|------------------|
| L7: Application |
| L6: Presentation |
| L5: Session |
| L4: Transport |
| L3: Network |
| L2: Data Link |
| L1: Physical |

| Communication | Security |
|---------------|---|
| DLMS | DLMS security suite 1 authentication & encryption |
| UDP | |
| IPv6 | |
| G3-PLC | EAP-PSK AES 128 |

| Communication | Security |
|---------------------------|---|
| DLMS | DLMS security suite 1 authentication & encryption |
| UDP / TCP | TLS1.2 |
| IPv4/v6 | IPsec VPN |
| GPRS / 3G / 4G / Ethernet | A5/3 (bei GPRS / 3G) |

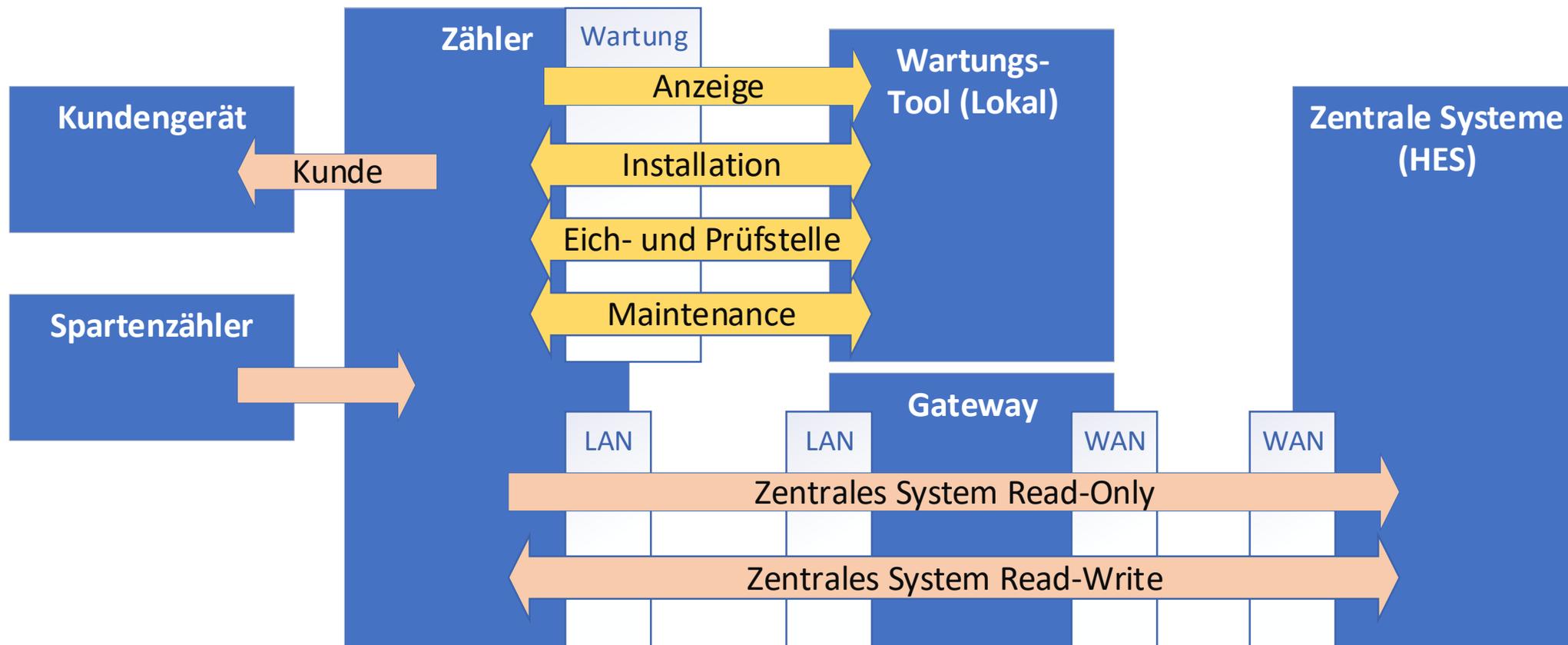
Gesicherte Datenübertragung: Real-Beispiel PLC

- Die Daten sind Ende-Zu-Ende verschlüsselt zwischen dem Sender und dem jeweils designierten Empfänger.
- Die Zählerdaten liegen lediglich beim Zähler und in den zentralen Systemen unverschlüsselt vor.



Rollenkonzept: Beispiel gemäß E2E Sicherheit

- ⊞ Zähler und Gateways haben ein stringentes Rollenkonzept
- ⊞ Rollen werden hierbei „Clients“ genannt. Jeder Client hat definierte Berechtigungen.
- ⊞ Authentisierung erfolgt durch Client-spezifisches kryptografisches Material und einer High Level Security Challenge-Response Methodik (HLS)



Key Management wird anhand eines dedizierten Systems (Key Management System, KMS) gewährleistet.

KMS Aufgaben umfassen unter anderem:

- ⬡ Gesicherter Import der symmetrischen Schlüssel aus dem Shipment File des Zählerherstellers
- ⬡ Verwaltung des Client-spezifischen symmetrischen Schlüsselmaterials und Zertifikate (wenn vorhanden)
- ⬡ Lifecycle-Management (erneuern, zurückziehen u.D.) der symmetrischen Schlüssel und Zertifikate (wenn vorhanden)
- ⬡ Bereitstellen von Verschlüsselungs- und Entschlüsselungsservices ggü. dem HES und/oder MDMS
- ⬡ Bereitstellen von Authentifizierungs- und Authentifizierungsprüfungsservices ggü. dem HES und/oder MDMS
- ⬡ Signaturprüfung, z.B. von Firmware-Dateien der Hersteller

Smart Meter PKI: ab Security Suite 1 & 2

Bei Nutzung der Security Suite 1 & 2 sind Zertifikate im Einsatz.

Es wird eine spezifische Smart Meter PKI genutzt. Folgende Zertifikate werden dabei ausgegeben:

- ⬢ DLMS/COSEM – für Authentisierung, Signatur, Key-Agreement
- ⬢ TLS – für Transportverschlüsselung und Authentisierung
- ⬢ Datenübermittlung File-basiert – Inhaltsverschlüsselung, z.B. für Shipment Files

Die PKI-Ausprägung:

- ⬢ Autonome Public-Key-Infrastruktur (PKI) zur Zertifikatsverwaltung und Erstellung
- ⬢ Beantragung, Abfrage und Sperrung von Zertifikaten automatisiert und manuell möglich

Protokollierung von Ereignissen

Zähler und Gateway sollen mindestens die Protokollierung folgender Ereignis-Typen unterstützen:

| Ereignis | Zähler | Gateway |
|--|--------|---------|
| Registrieren einer erfolgreichen oder fehlgeschlagenen Authentifizierung für eine bestimmte Rolle | x | x |
| Durchführung eines Firmware-Updates (erfolgreich/fehlgeschlagen/aktivieren) | x | x |
| Setzen der Systemzeit | x | x |
| Ereignisse, welche durch die Manipulationssensoren registriert werden. Hierzu zählen zum Beispiel das Öffnen von Gehäusedeckeln. | x | x |
| Starten eines Gerätes (Bootvorgang) | x | x |
| Durchführen eines Resets oder Reboots des Gerätes | x | x |
| Rücksetzen von Fehler- oder Alarmregistern oder den zugehörigen Protokollen | x | x |
| Registrieren von Gerätefehlern | x | x |
| Rekonfiguration von kryptografischen Parametern | x | x |
| Schalten des Breakers: aus / einschaltbereit | x | |
| Ereignisse in Bezug auf Spartenzähler | x | |
| Änderung der Parameter der Leistungsgrenze | x | |
| Leistungsbegrenzung | x | |

Thema Sicherheit: Verfolgte Sicherheitsstrategie

Klares Commitment zum Thema „Sicherheit“

Authentisierung an allen Schnittstellen

- ⊞ Kommunikationspartner müssen sich immer authentisieren und ihre Identität sicherstellen, bevor Daten übermittelt werden dürfen.

(Ende-zu-Ende) Verschlüsselung und Integritätsschutz/Signierung der Daten während der Übertragung

- ⊞ Daten müssen während der Übertragung durch kryptographische Methoden vor Veränderung oder unzulässiger Kenntnisnahme geschützt werden.

Nutzung etablierter Standards

- ⊞ Die Realisierung soll auf etablierten Standards beruhen und damit ein entsprechendes Maß an Sicherheit und Kontinuität gewährleisten.

Abgrenzung der Systeme anhand eines Zonenkonzepts

- ⊞ Zonen erlauben Maßnahmen ggü. Informationsobjekten und ihrer Übertragung; Zonen werden je nach Bedarf hart getrennt (physisch, durch Firewalls, Router, u.D.) oder weich getrennt (logisch, durch VPNs, port-based VLAN, u.D.).

Thema Sicherheit: Verfolgte Sicherheitsstrategie

Klares Commitment zum Thema „Sicherheit“

Dedizierte Eingrenzung des Informationsflusses

- ⦿ Eingrenzung von erlaubten und zu verhindernden Informationsflüssen sowie Abbildung der Spielregeln der System-Interoperation

Gezielter Einsatz von lokalen (Host-)basierenden und übergreifenden (Sicherheits-)Maßnahmen

- ⦿ Sicherheitsmaßnahmen werden dort angesetzt, wo diese sinnvoll sind und effektiv wirken können.

Audit / Logging

- ⦿ Nachvollziehbarkeit und Nachverfolgbarkeit von relevanten Ereignissen zu jeder Zeit gewährleistet

Definierte Festlegung von Akteuren / Rollen und deren Berechtigungen

- ⦿ Klare Rollen- und Berechtigungsdefinition im System und Zuteilung entsprechender Mitarbeiter; dadurch ergeben sich strukturierte Aufgaben und Verantwortlichkeiten innerhalb des Systems und ein gewisses Controlling sicherheitsrelevanter Aspekte ist sichergestellt

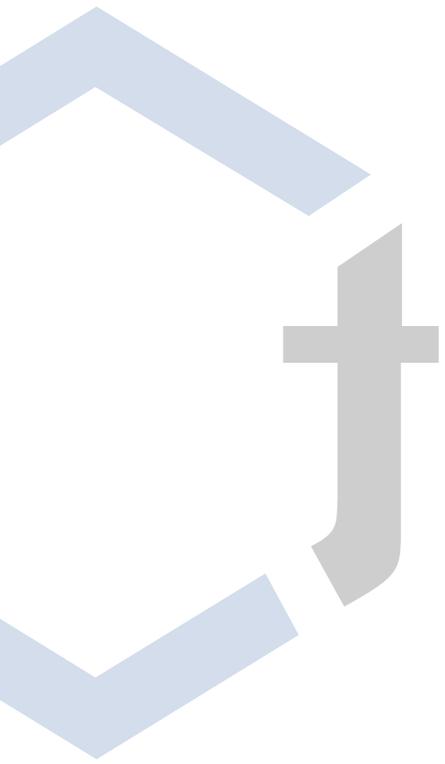
Zum Nachschlagen: weiterführende Links

OE Ende-zu-Ende Sicherheit

- 🔗 Anforderungskatalog Ende-zu-Ende Sicherheit Smart Metering
- 🔗 <https://oesterreichsenergie.at/sicherheitsanforderungen-fuer-smart-meter.html>

Green Book

- 🔗 DLMS User Association, DLMS/COSEM Architecture and Protocols, Edition 8.1
- 🔗 <https://www.dlms.com/>



Herzlichen Dank!

Dr. Michael Schafferer
michael.schafferer@te-am.net