The Society of Electrical and Electronics Engineers in Israel

Electricity & Energy 2019

The 20th international Annual Convention

November 5-8, 2019 | Eilat, Israel

Smart Meter Security

Basis for smart grid security, availability and reliability

Prof. Dr. Uwe Heuert
Managing Director exceeding solutions
Professor at University of Applied Science Merseburg
Germany

exceeding solutions

Content

- Introduction
- Smart Meter Rollout - Germany
- Smart Meter Rollout - International
- Common security aspects
- Testing requirements and options
- Cooperation NMi – exceeding solutions

Sorry for my bad English!

exceeding solutions

Hochschule Merseburg

- 2.500 students
- 3 faculties
- Professorship for computer networks and virtual instrumentation
- Since 2015 first test lab for German smart meter rollout (*“Intelligente Messsysteme 2020”*)

exceeding solutions

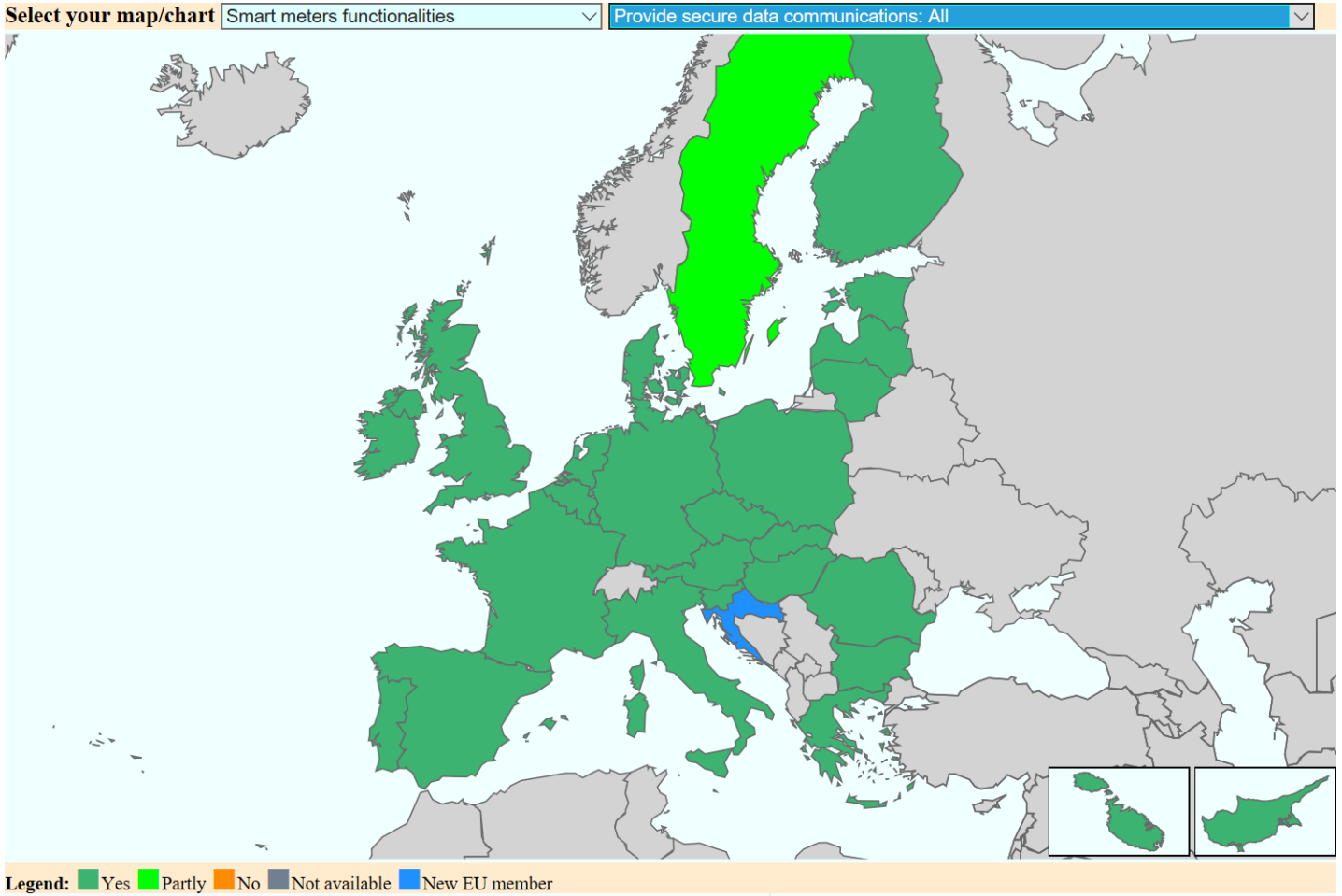
exceeding solutions

- Founded in 2013
- Employees (2019)
  - 16 of 20 are engineers/academics
  - 14 of 20 are developers for hard- and software
- Divisions
  - Smart metering (70%)
  - IoT and IT services (20%)
  - Ultrasound and industrial (10%)
- Sales
  - 1,2 Million € in 2018

E-world 2019, Essen

exceeding solutions

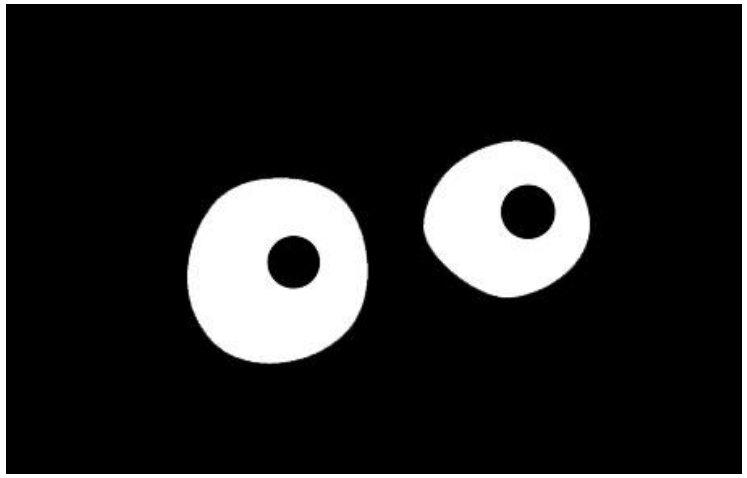
Smart Metering Rollout in EU – Secure communication



http://ses.jrc.ec.europa.eu/smart-metering-deployment-european-union

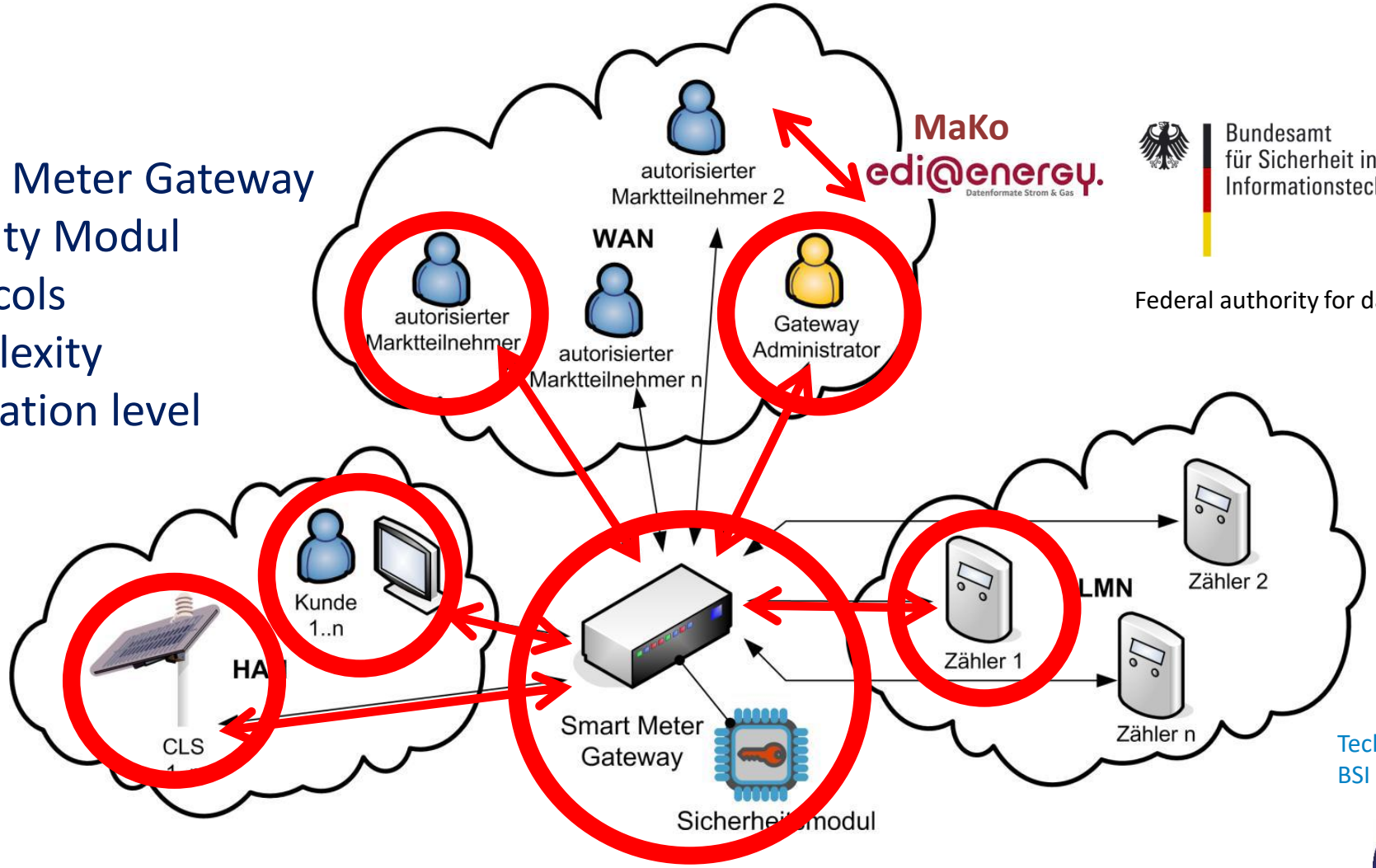
What are the challenges?

- Data protection
- Hacking prevention
- Manipulation prevention
- Grid security
- Blackout prevention
- …



The German approach

- Special:
  - Roles
  - Smart Meter Gateway
  - Security Modul
  - Protocols
  - Complexity
  - Integration level



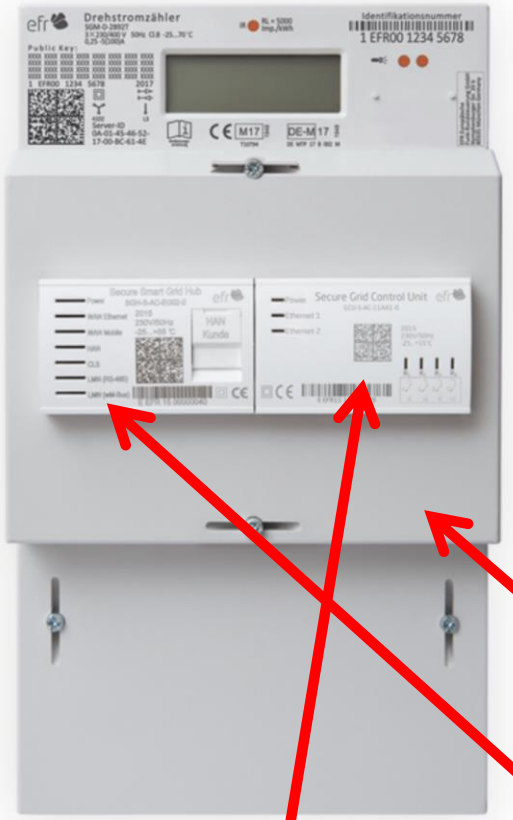
MaKo edi@energy. Datenformate Strom & Gas

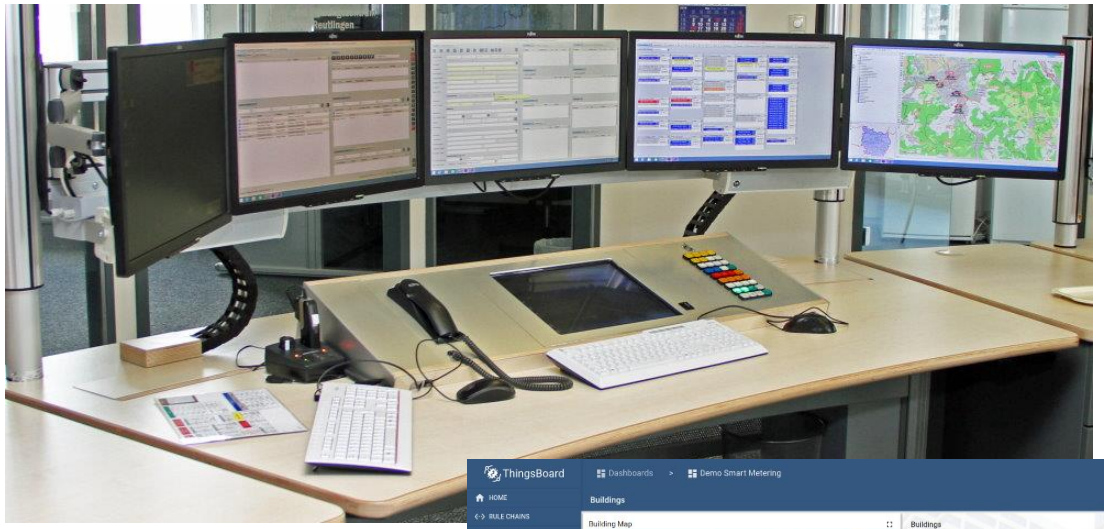
Bundesamt für Sicherheit in der Informationstechnik

Federal authority for data security

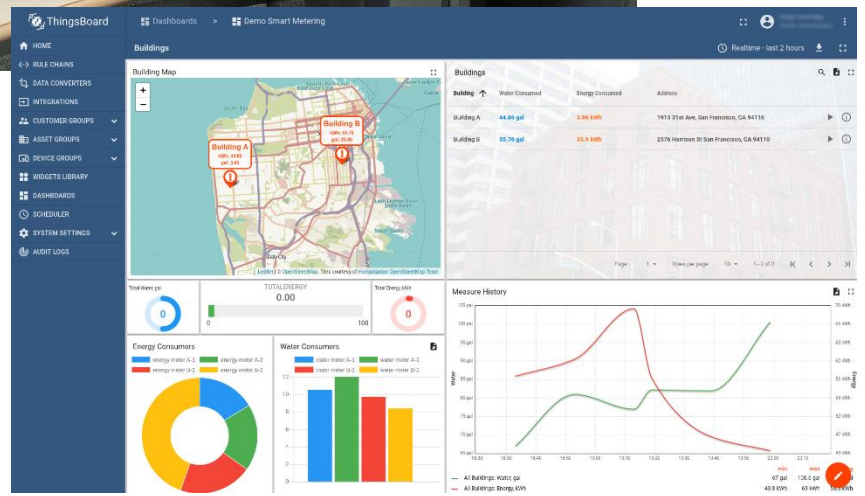
Technische Richtlinie
BSI TR-03109

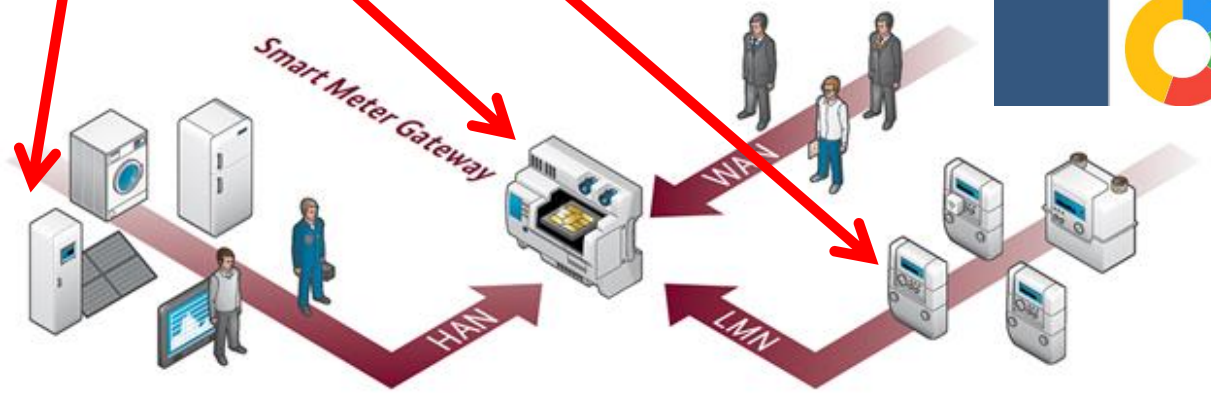
exceeding solutions





Grid operator

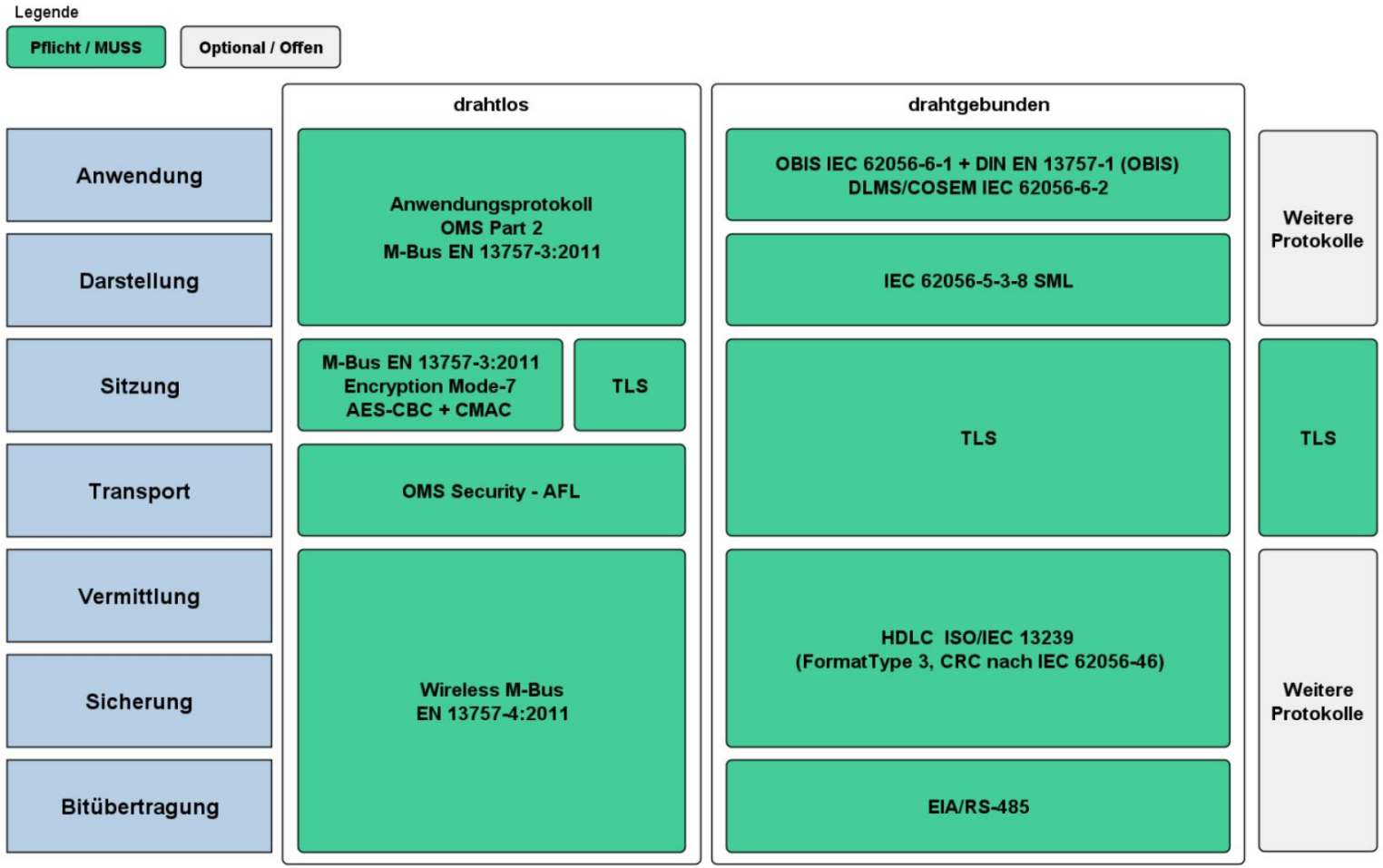




exceeding solutions

LMN protocol stack

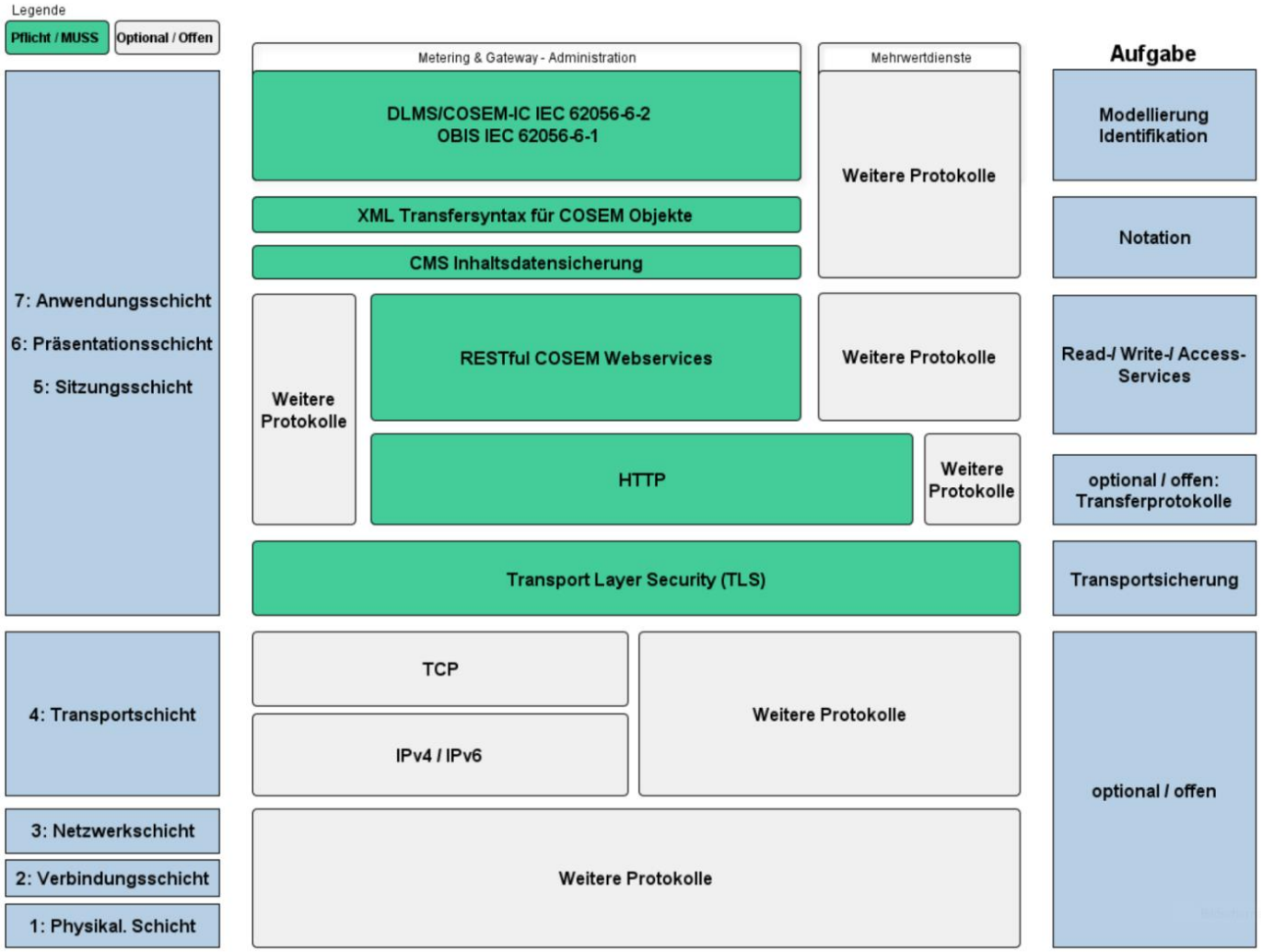
- Meter/SMGW interface:
  - Wired
  - Wireless
  - „Proprietary“ protocols (SML)
  - Combined with standards (TLS, wM-Bus, AES-CBC-CMAC)



exceeding solutions

WAN protocol stack

- SMGW-to-GWA/EMT interface:
  - On top of TCP/IP
  - GPRS, LTE, ETH, PLC, …
  - „Proprietary“ protocols (COSEM/XML)
  - Combined with standards (TLS, HTTP, RESTful WS)



exceeding solutions

What is cryptography?

- Big number computation
- Public algorithms
- Private/secret key data
- Symmetric, asymmetric and message digest algorithms and their combinations
- Data structures, data encoding, protocols
- International standards
- National/proprietary standards

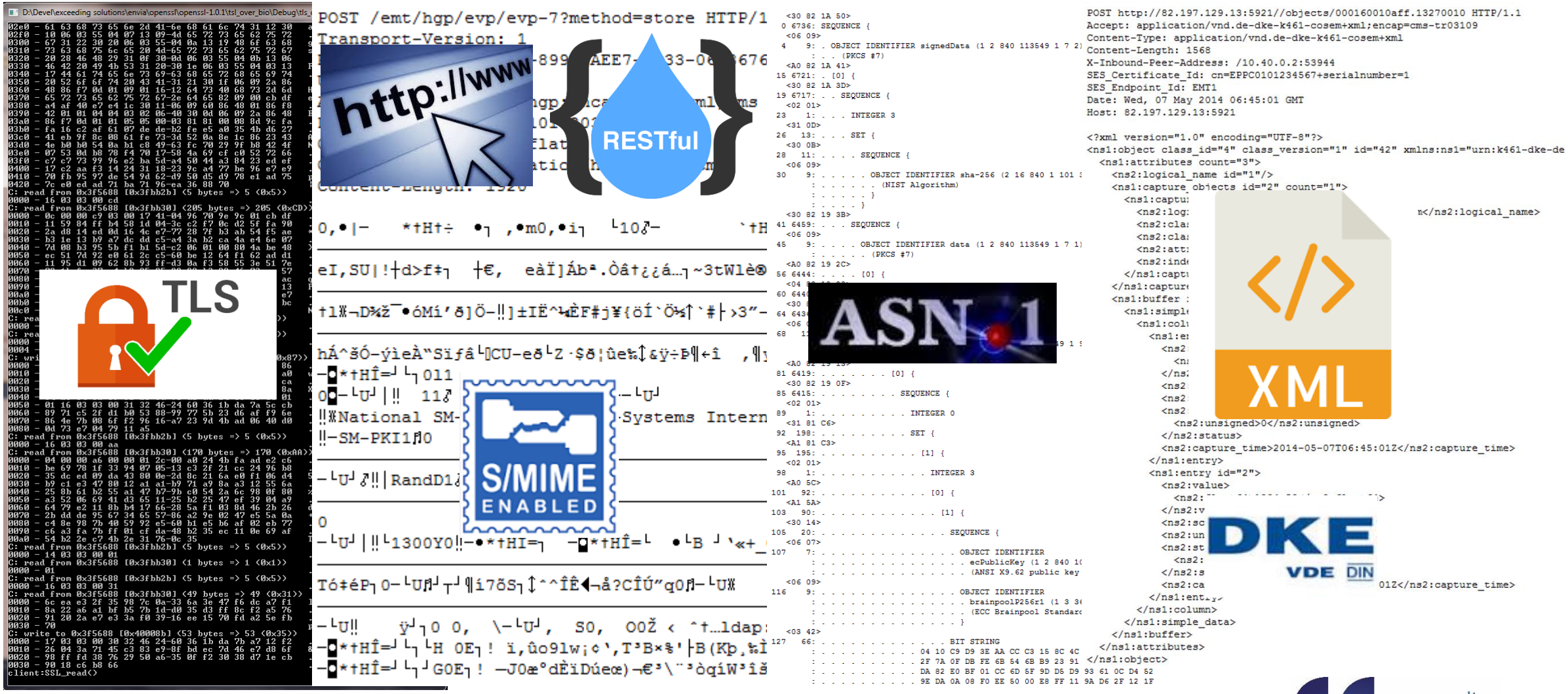
BSI selected cryptography

- Premium quality
- Similar to other eGovernment security project (e.g. identity card)
- Elliptic curve cryptography (ECC … no RSA or others)
- Special curves (brainpool)
- AES-CBC-CMAC (authenticated encryption)
- TLS 1.2 (with strong restrictions and always client authentication)
- Additional end-to-end data security with CmsSignedData and CmsAuthEnvelopedData (similar to signed and encrypted email)
- All ECC operations (plus RNG) in hardware (security module, HSM)
- SM-PKI-DE
- Certification of SMGW (BSI PP/CC, PTB), meters (PTB, FNN) and backend IT (ISO 27001)

very difficult

exceeding solutions

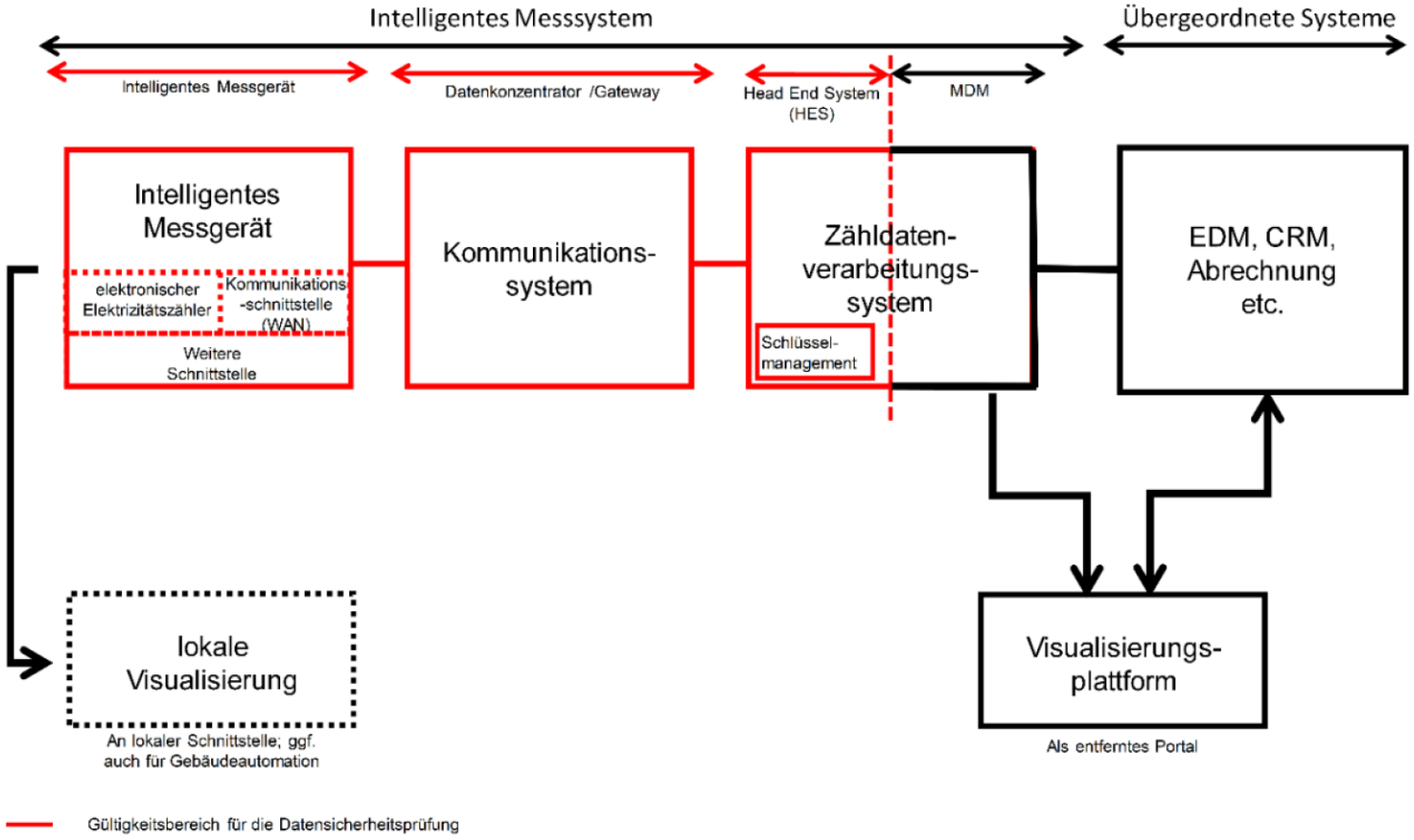
How the communication looks like?



exceeding solutions

Smart Meter Rollout Swiss

- Different wording
- Different technologies
- Different certification
- Similar architecture



exceeding solutions

International

- DLMS
  - „DLMS -The true international metering standard“

exceeding solutions

Comparision - cryptography

Category	German approach	International
Symmetric cryptography	Wired LMN pairing phase 1 (SYM) [FNN] wM-BUS (security mode 7) [OMS] AES-CBC-CMAC-128	DLMS/COSEM security suite 0 [DLMS] wM-BUS (security mode 5, 7) [OMS] AES-GCM-128
Transport layer security	TLS 1.2 (SM-PKI-DE) [RFC + BSI] >= TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.0 – 1.2 [RFC] VPN
Application layer security (asymmetric/hybrid cryptography)	SML signature [FNN] CmsSignedData (SM-PKI-DE) [RFC + BSI] CmsEnvelopedData (SM-PKI-DE) [RFC + BSI] ECC BRAINPOOL (& NIST)	DLMS/COSEM security suite 1 [DLMS] DLMS/COSEM security suite 2 [DLMS] ECC NIST ECDH_ECDSA_WITH_AES_GCM_128_SHA256

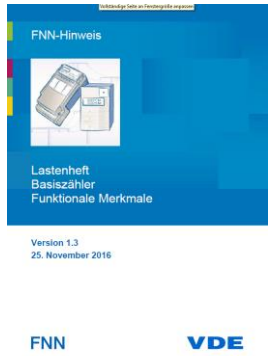
not so different

exceeding solutions

Standardization/Certification

- International
  - MID
  - DLMS
  - OMS
  - ESMIG
- Germany
  - MID
  - FNN
  - OMS
  - DKE
  - PTB
  - BSI

mostly different



exceeding solutions

Challenges

- Complex technologies
- Special and proprietary protocols
- „invisible“ data
- Huge number of transactions and amount of data
- Limited humans
- Infinitely sources of error
- Many threats

Testing, testing, testing, …

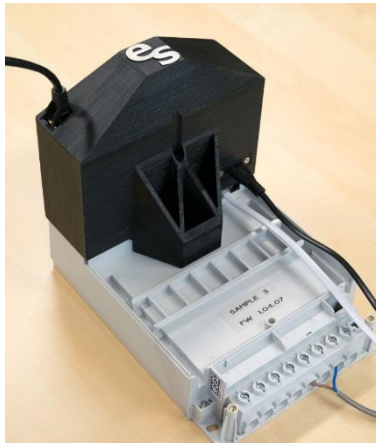
exceeding solutions

es:Testsystem

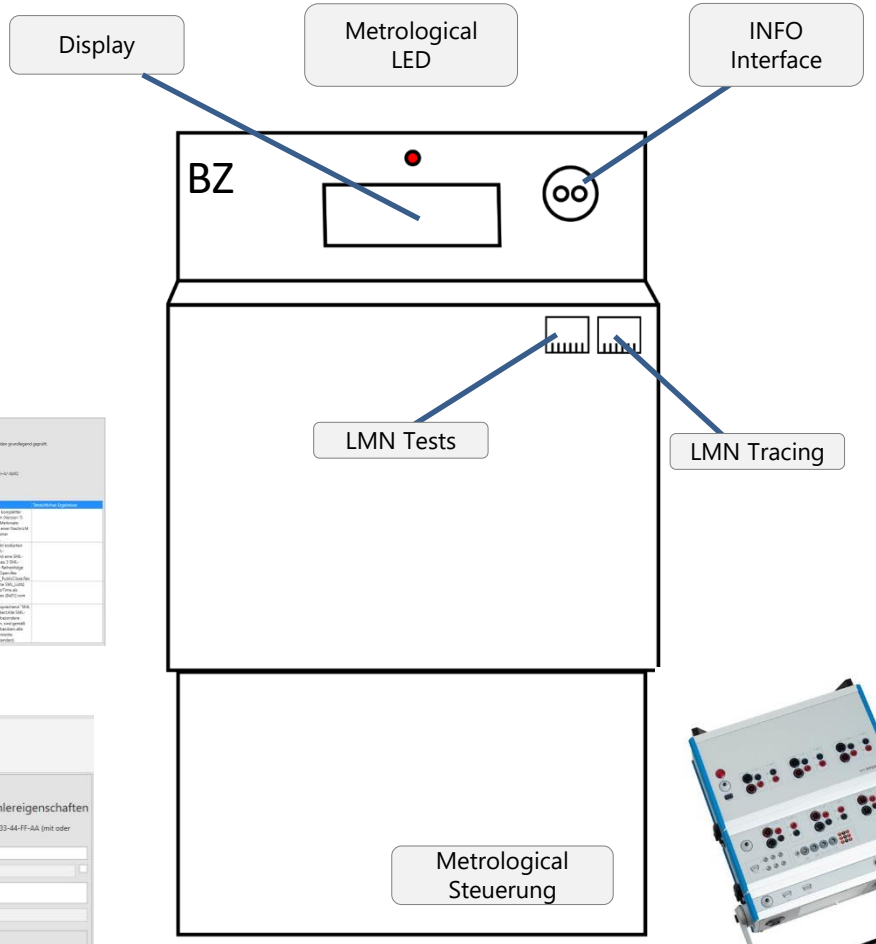
advertising block

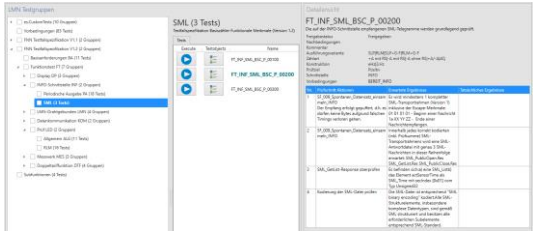
exceeding solutions

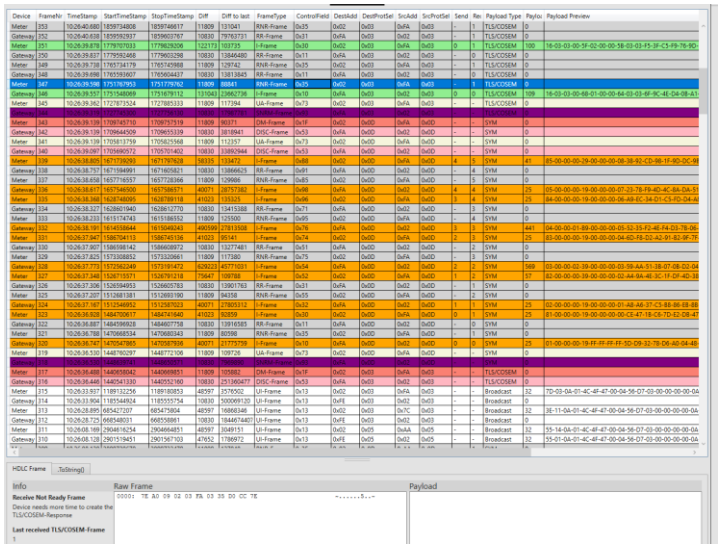
ToE - FNN base meter



exceeding solutions
SMOCS
Smart Metering Optical Capture System



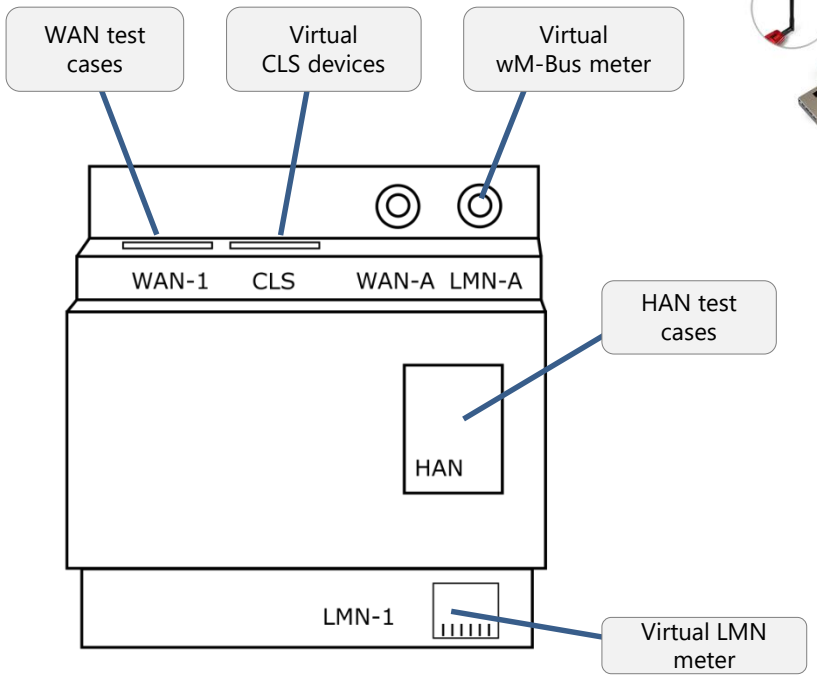


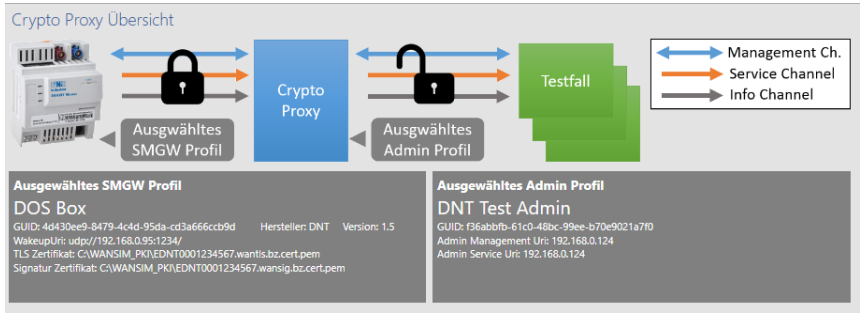


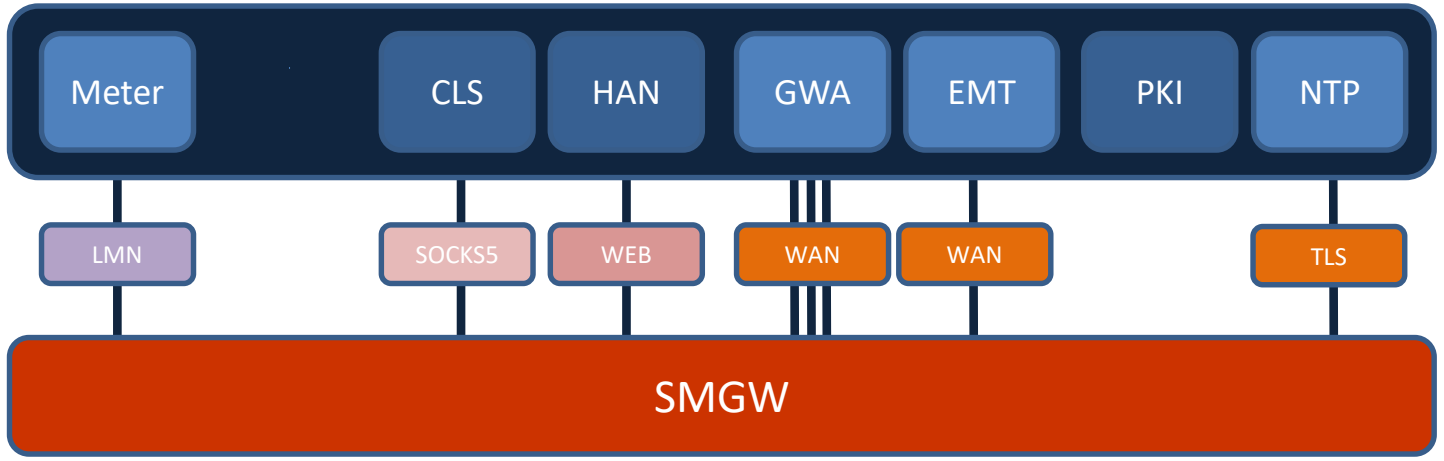
exceeding solutions

ToE - BSI SMGW


WAN-A
LMN-A
theben
PWR
TLS
LMC
wMT
DE-M
CX
CONEXA 3.0
WAN-1
CLS
LMN-1

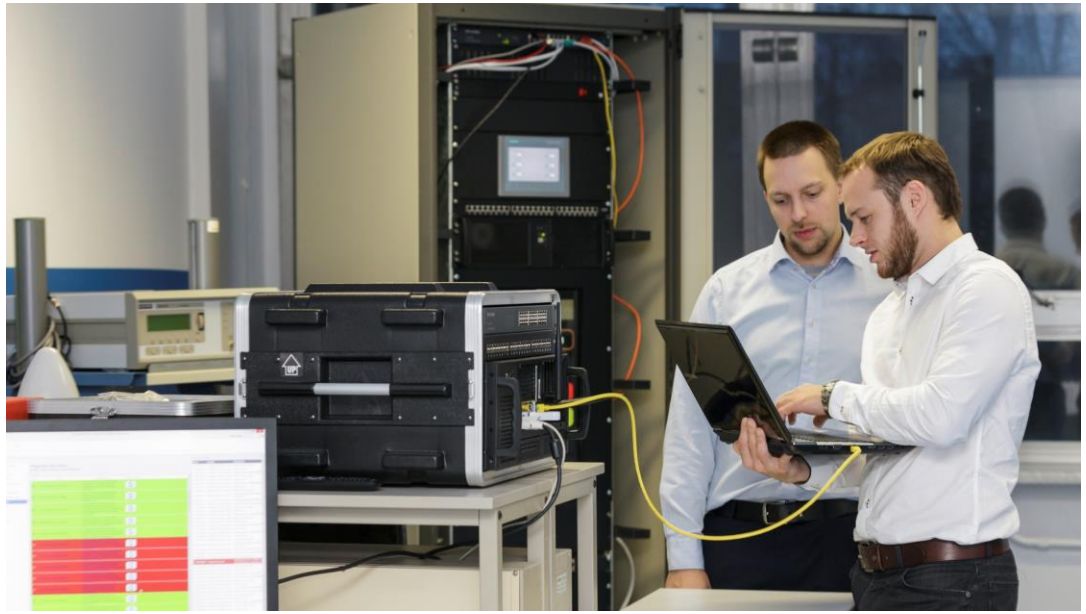

WAN test cases
Virtual CLS devices
Virtual wM-Bus meter
WAN-1
CLS
WAN-A
LMN-A
HAN test cases
HAN
LMN-1
Virtual LMN meter

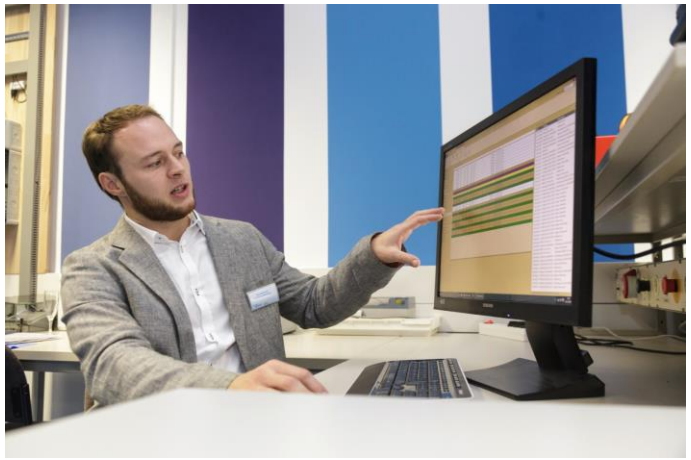

Crypto Proxy Übersicht
Ausgewähltes SMGW Profil
Crypto Proxy
Ausgewähltes Admin Profil
Testfall
Management Ch.
Service Channel
Info Channel
Ausgewähltes SMGW Profil
DOS Box
GUID: 4d430ee9-8479-4c4d-95da-cd3a666ccb9d
Hersteller: DNT
Version: 1.5
WakeupUri: udp://192.168.0.95:1234/
TLS Zertifikat: C:\WANSIM_PKI\EDNT0001234567.wantls.bz.cert.pem
Signatur Zertifikat: C:\WANSIM_PKI\EDNT0001234567.wansig.bz.cert.pem
Ausgewähltes Admin Profil
DNT Test Admin
GUID: f36abbfb-61c0-48bc-99ee-b70e9021a7f0
Admin Management Uri: 192.168.0.124
Admin Service Uri: 192.168.0.124


Meter
CLS
HAN
GWA
EMT
PKI
NTP
LMN
SOCKS5
WEB
WAN
WAN
TLS
SMGW

Testing services

- Meter
- SMGW
- Backend IT
- Conformance
- Vulnerability
- Interoperability
- Performance
- …





Activities with NMi Certin B.V.

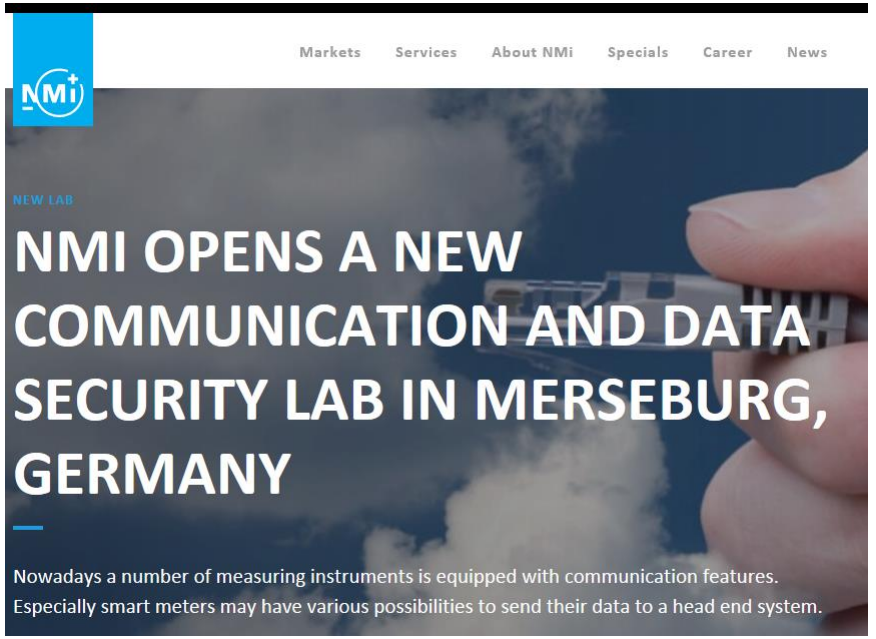
- First projects (started in 2017)
- Mutual education and certification (01/2019)
- Smart Meter Test Lab Merseburg, Germany (06/2019)
- Strong Cooperation in several fields (ESMIG, penetration testing, …)

https://www.nmi.nl/data-security-of-smart-meters/

https://www.nmi.nl/markets/cyber-security-and-safety/

exceeding solutions

NMi Smart Meter Test Lab Merseburg, Germany



https://www.nmi.nl/nmi-opens-a-new-communication-and-data-security-lab-in-merseburg-germany/

exceeding solutions

ESMIG security requirements

Smart Meter Co-ordination Group
Privacy and Security Approach – Part IV

Minimum security requirements for AMI components

European level requirements for Smart Metering

Version: 1.1
Date: 17th July 2016
Authors: SM-CG Task Force on Privacy and Security / ESMIG

- A: All AMI components SHALL provide a log of security events
- B: All data exchanges SHALL take place in a (end-to-end) secure manner
- C: Availability of the system (AMI components and communication network) SHALL be sufficient
- D: Crypto mechanism and key management SHALL be documented and be compliant with recognized/proven and approved open standards
- E: Every AMI component SHALL check the authorization
- F: Data at rest SHALL be protected in all system components
- G: AMI components SHALL be upgradable for new (security) functionalities
- H: Functionalities in AMI components SHOULD be limited to the intended operational Use Cases
- I: AMI components and the communications network SHALL be adequately protected against external disturbances and/or attacks

AMI … advanced metering infrastructure

exceeding solutions

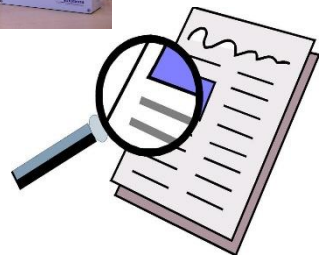
ESMIG … certificate

ESMIG

Test specification

Test implementation

Test report



Certificate

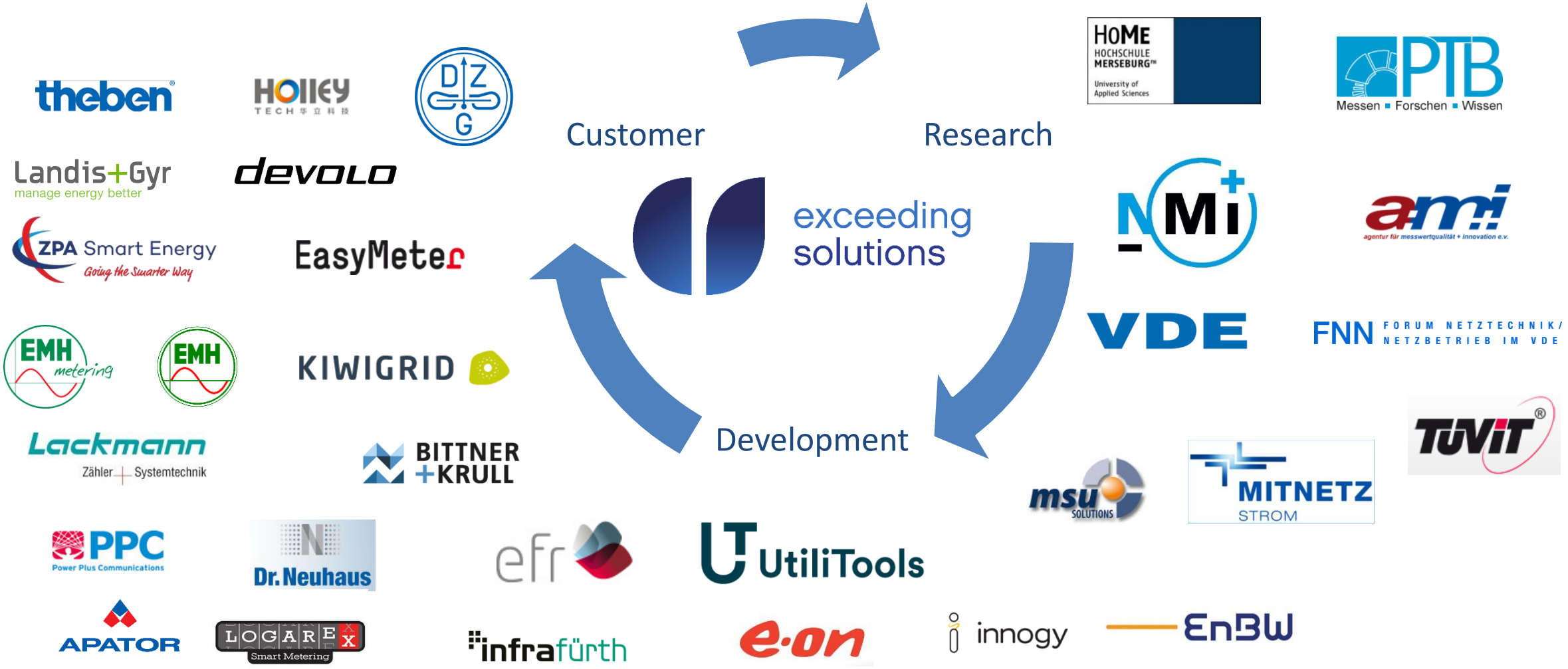
First pilot projects are running!

Any questions …

- Why the smart meter rollout projects are late (so late)?
- Complexity means security?
- What about process security?
- … communication stability?
- … business cases?
- … customer acceptance?
- Where we find the technical experts?

exceeding solutions

Cooperation – Smart Metering



exceeding solutions