

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

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!

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”*)



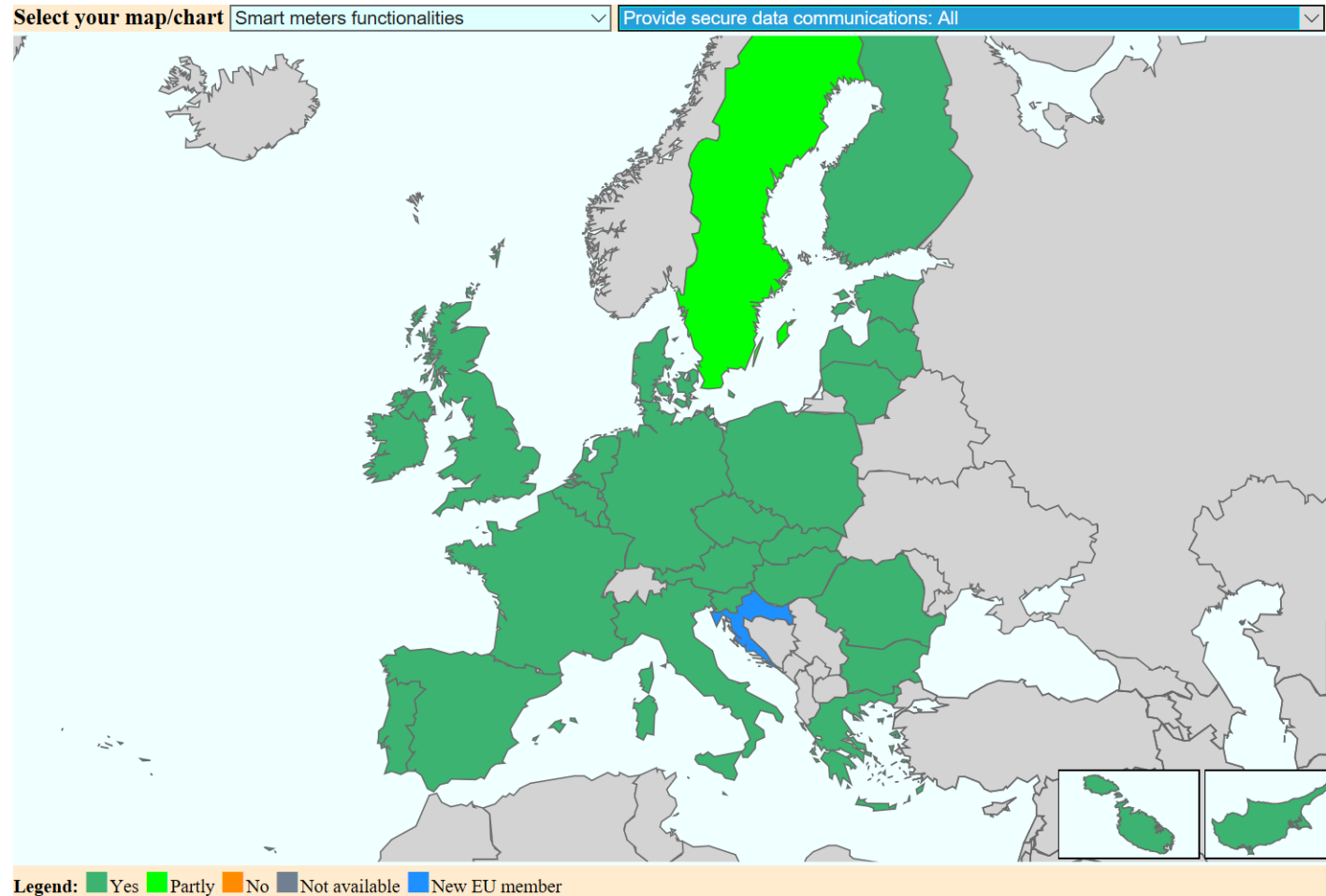
exceeding solutions

- 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

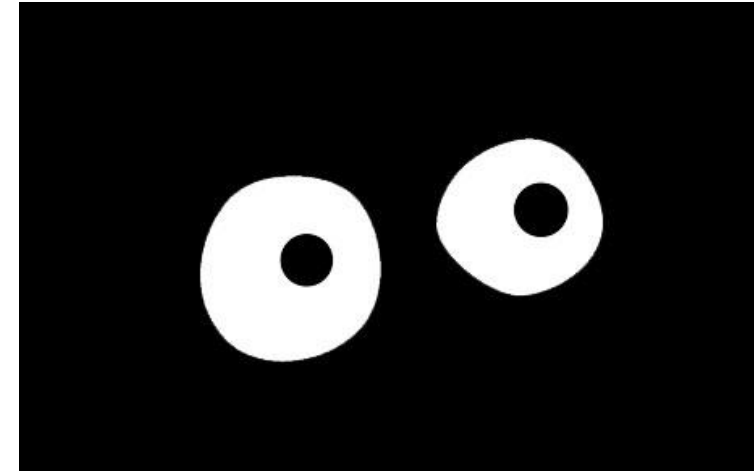
Smart Metering Rollout in EU – Secure communication



<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
- ...



11/10/2019

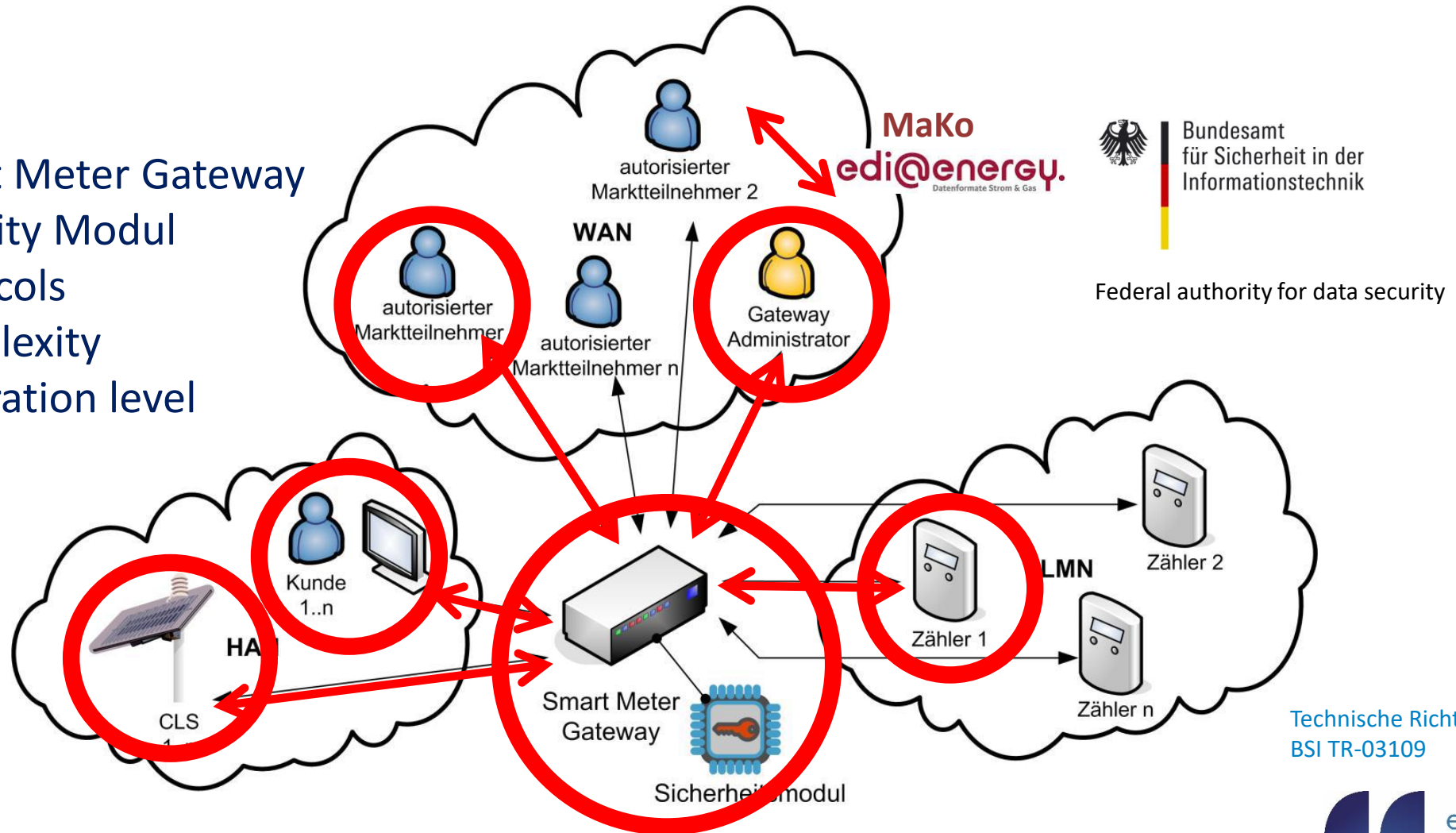


Electricity & Energy 2019 | November 5-8 | Eilat, Israel

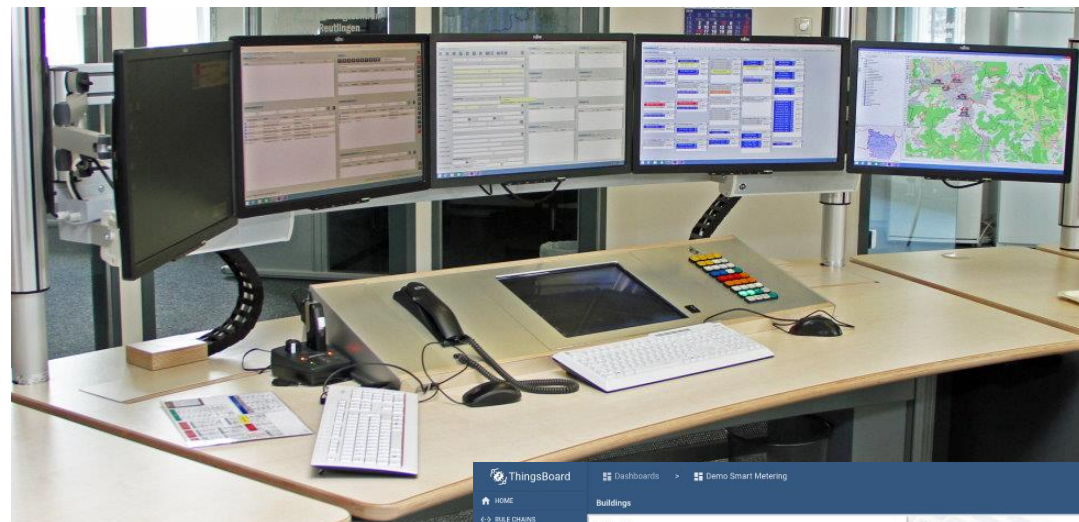


The German approach

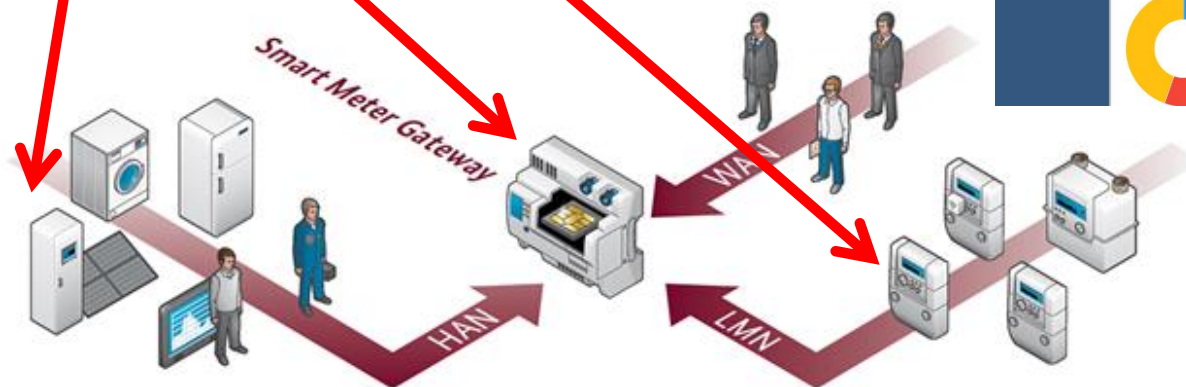
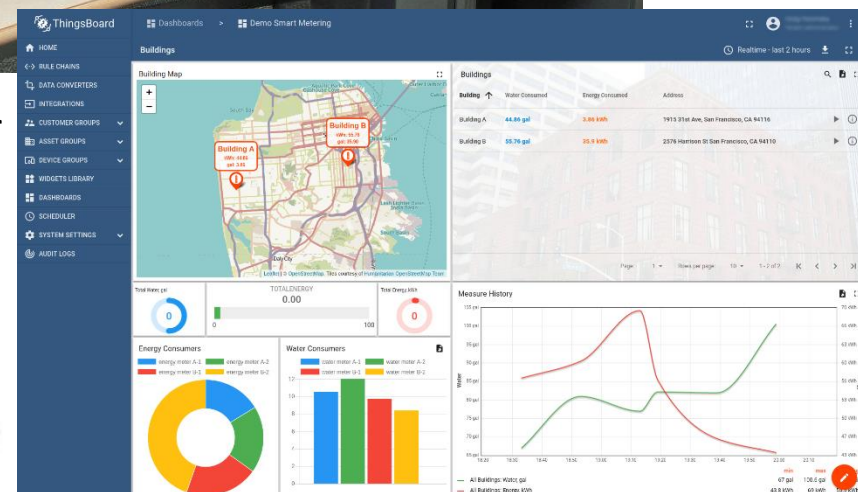
- Special:
 - Roles
 - Smart Meter Gateway
 - Security Modul
 - Protocols
 - Complexity
 - Integration level



Technische Richtlinie
BSI TR-03109

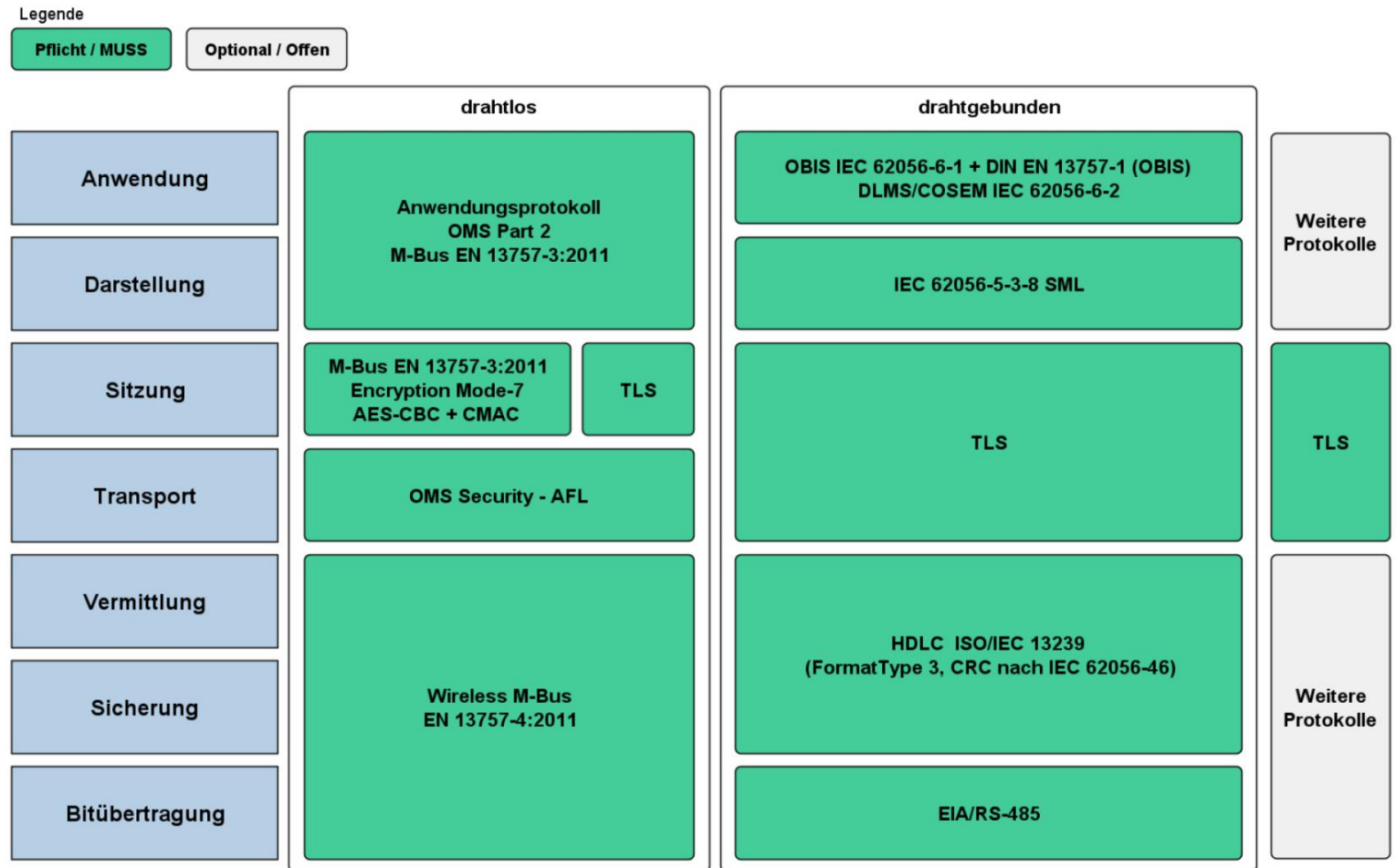


Grid operator



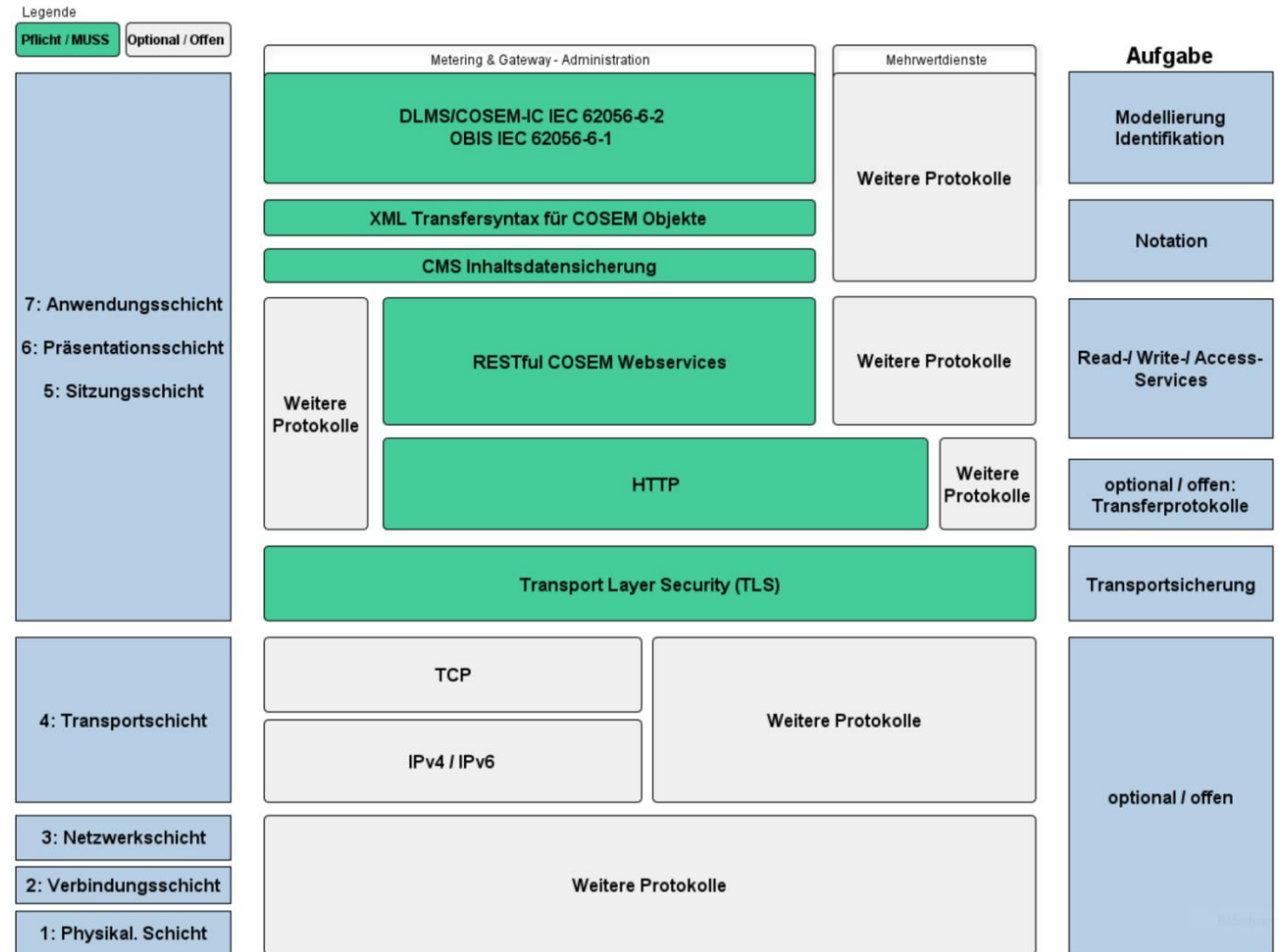
LMN protocol stack

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



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)



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 PNG) in hardware (security module, HSM)
- SM-PKI-DE
- Certification of SWIGW (BSI PP/CC, PTB), meters (PTB, FNN) and backend IT (ISO 27001)

How the communication looks like?

```
0200 - 61 63 68 73 65 6e 2d 41 6e 68 61 6c 74 31 12 30
0201 - 10 06 03 55 04 07 13 09 4d 65 72 73 65 62 75 72
0300 - 67 31 22 30 20 06 03 55 04 0a 13 19 48 6f 63 68
0310 - 73 63 68 75 6c 65 20 4d 65 72 73 65 62 75 72 67
0320 - 20 20 46 40 29 31 08 30 0d 06 03 55 04 0b 13 06
0330 - 46 42 20 49 4b 53 31 20 30 1e 06 03 55 04 03 13
0340 - 17 44 61 74 65 6e 73 69 63 68 65 72 68 65 69 74
0350 - 20 52 6f 6f 74 20 43 41 31 21 30 1f 06 09 2a 86
0360 - 40 06 f7 0d 01 09 01 16 12 64 73 40 68 73 2d 6d
0370 - 65 72 73 65 62 75 72 67 2e 64 65 82 09 00 cb df
0380 - a4 af 04 e7 e4 1c 30 11 06 09 60 86 40 01 86 f8
0390 - 42 01 01 04 04 03 06 40 30 0d 06 09 2a 86 48
03a0 - 06 f7 0d 01 01 05 05 00 03 81 01 00 0d 9e fa
03b0 - fa 16 c2 af 61 07 de d2 fe e5 a0 35 4b d6 27
03c0 - 41 eb 9f 8c 08 61 fe 73 3d 52 0a 8e 1c 86 23 43
03d0 - 4e b0 b0 54 0a b1 c8 49 63 fc 70 29 9f b8 42 4f
03e0 - 07 53 0d b0 78 f4 70 17 50 4a 59 cf c0 52 72 66
03f0 - e7 c7 73 99 96 e2 ba 5d a4 5d a4 a3 84 23 ed ef
0400 - 17 c2 aa f3 14 24 31 18 23 9c a4 77 be 96 e7 e9
0410 - 70 fb 95 97 de 54 9d 62 49 50 d5 d9 78 e1 ad 75
0420 - 7e e0 ed ad 71 ba 71 96 ea 36 08 70
C: read from 0x3f5688 [0x3fbb2h] (5 bytes => 5 (0x5))
0000 - 16 03 03 00 cd
C: read from 0x3f5688 [0x3fbb30] (205 bytes => 205 (0xcd))
0000 - 0c 00 00 c9 04 00 17 41 04 9c 01 cb df
0010 - 11 59 84 ff b4 58 1d 04 3c c2 f7 0c d2 5f fa 90
0020 - 2a d8 14 ed 0d 16 4c e7 77 28 7f b3 ab 54 f5 ae
0030 - b3 1e 13 b9 a7 dc c5 a4 3a b2 ca 4a ea 6e 07
0040 - 7d 00 b3 25 5a f1 b1 5d e2 06 01 b0 00 4a be 05
0050 - ec 51 7d 92 e9 61 2c c5 60 be 12 64 f1 62 ad d1
0060 - 11 95 d1 09 62 8b 93 ff d3 0a f3 58 55 3e 51 7e
0070 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
C: read from 0x3f5688 [0x3fbb2h] (5 bytes => 5 (0x5))
0000 - 16 03 03 00 aa
C: read from 0x3f5688 [0x3fbb30] (170 bytes => 170 (0xaa))
0000 - 04 00 00 a6 00 00 01 2c 00 a0 24 4b fa ad e2 c6
0010 - 06 69 70 1f 33 94 07 05 13 c3 21 c1 24 96 b8
0020 - 35 dc ed 09 da 43 08 0e 2d 8c 21 6a e9 f1 0e 14
0030 - b9 c1 e3 47 80 12 a1 a1 b9 71 a9 8a a3 12 55 6a
0040 - 25 0b 61 b2 55 a1 47 b7 9b c0 54 2a 6c 98 0f 80
0050 - a3 52 06 69 41 d3 65 11 25 b2 25 47 e7 39 04 a9
0060 - 64 79 e2 11 8b b4 17 66 28 5a f1 03 8d 46 2b 26
0070 - 2b dd de 95 67 34 65 57 86 a2 9e 02 47 e5 5a 0a
0080 - c4 8e 98 7b 40 59 92 e5 60 h1 e5 b6 af 02 eb 77
0090 - 05 a3 fa 7b ff 01 cf da 40 b2 35 ec 11 0e 69 af
00a0 - 54 b2 2e c7 4b 2e 31 76 0c 35
C: read from 0x3f5688 [0x3fbb2h] (5 bytes => 5 (0x5))
0000 - 14 03 03 00 01
C: read from 0x3f5688 [0x3fbb30] (1 bytes => 1 (0x1))
0000 - 01
C: read from 0x3f5688 [0x3fbb2h] (5 bytes => 5 (0x5))
0000 - 16 03 03 00 31
C: read from 0x3f5688 [0x3fbb30] (49 bytes => 49 (0x31))
0000 - 6c ea e3 2f 35 98 7c 0a 33 3e 47 fc d6 a7 f1
0010 - 8a 22 a6 a1 bf b5 7b 1d 00 35 d3 ff 8c f2 a5 76
0020 - 31 20 2a e7 e3 3a f0 39 16 ee 15 70 f4 a2 5e fb
0030 - 70
C: write to 0x3f5688 [0x4000b1] (53 bytes => 53 (0x35))
0000 - 17 03 03 00 30 32 46 24 60 36 1b da 7a 5e cb
0010 - 26 04 3a 71 45 c3 83 e9 8f bd ec 7d 46 e7 d8 6f
0020 - 93 ff f4 30 78 29 50 a6 35 0f f2 30 38 d7 1e cb
0030 - 70
client:SSL_read()
```

POST /emt/hgp/evp/evp-7?method=store HTTP/1.1
Transport-Version: 1

 http://www... RESTful

Content-Length: 1520

0, • | - * + H ÷ • , • m 0 , • i , L 1 0 3 - ' + H

e I, S U ! | + d > f # , + € , e a ï | Á b * . Ò â + ç ç á ~ 3 t W l e Ò

+ 1 % - D % z - • 6 M i ' 8] Ö - !] ± I E ^ - 4 E F # j ¥ { ö í ' Ö * ↑ # | > 3 " -

h Á ^ š Ó - ý i e À " S i f â L [C U - e š L Z - \$ š ; ù e % ; ÷ y ÷ F q | + i , q |

- • * + H ÷ = L , 0 1 1

0 0 - L U | | ! 1 1 3

!! National SM - Systems Intern

!! - SM - PKI 1 1 3 0

- L U | 3 || Rand D 1 3

0

- L U | | ! 1 3 0 0 Y 0 ! - • * + H ÷ = L - • * + H ÷ = L • L B ' ' « +

T 6 ± é P 1 0 - L U | 1 1 1 7 8 5 1 1 ^ ^ Î Ê « - â ? C i Ú " q 0 1 - L U %

- L U ! ! y 1 0 0 , \ - L U , S 0 , 0 0 ž < ^ + l d a p :

- • * + H ÷ = L , L H O E 1 ! i , ú o 9 l w ; • ' , T ' B * % ' | B (K p , š i

- • * + H ÷ = L , L G O E 1 ! - J 0 æ ° È i D ú e æ - € ' ' " ò q i W ' i š

```
<30 82 1a 50>
0 6736: SEQUENCE {
  <06 09>
  4 9: . . . OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
    . . . (PKCS #7)
  <A0 82 1a 41>
  15 6721: . . . [0] {
    <30 82 1a 3D>
  19 6717: . . . SEQUENCE {
    <02 01>
    23 1: . . . INTEGER 3
    <31 0D>
    26 13: . . . SET {
    <08 0B>
    28 11: . . . SEQUENCE {
    <06 09>
    30 9: . . . . . OBJECT IDENTIFIER sha-256 (2 16 840 1 101 :
      . . . . . (NIST Algorithm)
      . . . . .
      . . . . .
    }
  }
  <30 82 19 3B>
  41 6459: . . . SEQUENCE {
    <06 09>
    45 9: . . . . . OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)
      . . . . . (PKCS #7)
    <A0 82 19 2C>
    56 6444: . . . . . [0] {
      <04 03>
      60 6440: . . . . .
      <30 82 19 1F>
      64 6436: . . . . . SEQUENCE {
        <06 09>
        68 1: . . . . .
      }
    }
    <A0 82 19 1B>
    81 6419: . . . . . [0] {
      <30 82 19 0F>
      85 6415: . . . . . SEQUENCE {
        <02 01>
        89 1: . . . . . INTEGER 0
        <31 81 C6>
        92 198: . . . . . SET {
          <A1 81 C3>
          95 195: . . . . . [1] {
            <02 01>
            98 1: . . . . . INTEGER 3
            <A0 5C>
            101 92: . . . . . [0] {
              <A1 5A>
              103 90: . . . . . [1] {
                <30 14>
                105 20: . . . . . SEQUENCE {
                  <06 07>
                  107 7: . . . . . OBJECT IDENTIFIER
                    . . . . . ecPublicKey (1 2 840 1 :
                    . . . . . (ANSI X9.62 public key)
                  }
                }
              }
            }
          }
          <06 09>
          116 9: . . . . . OBJECT IDENTIFIER
            . . . . . brainpoolP256r1 (1 3 3 :
            . . . . . (ECC Brainpool Stand:
            . . . . .
          }
        }
      }
    }
    <03 42>
    127 66: . . . . . BIT STRING
      . . . . . 04 10 C9 D9 3E AA CC C3 15 8C 4C
      . . . . . 2F 7A 0F DB FE 6B 54 6B B9 23 91
      . . . . . DA 82 E0 BF 01 CC 6D 5F 9D D5 D9 93 61 0C D4 52
      . . . . . 9E DA 0A 08 F0 E2 50 00 E8 FF 11 9A D6 2F 12 1F
  }
}
}
```

POST http://82.197.129.13:5921//objects/000160010aff.13270010 HTTP/1.1
Accept: application/vnd.de-dke-k461-cosem+xml;encap=cms-tr03109
Content-Type: application/vnd.de-dke-k461-cosem+xml
Content-Length: 1568
X-Inbound-Peer-Address: /10.40.0.2:53944
SES_Certificate_Id: cn=EPPC0101234567+serialnumber=1
SES_Endpoint_Id: EMT1
Date: Wed, 07 May 2014 06:45:01 GMT
Host: 82.197.129.13:5921

<?xml version="1.0" encoding="UTF-8"?>
<ns1:object class_id="4" class_version="1" id="42" xmlns:ns1="urn:k461-dke-de-
 <ns1:attributes count="3">
 <ns2:logical_name id="1"/>
 <ns1:capture_objects id="2" count="1">
 <ns1:captu:
 <ns2:log:
 <ns2:cla:
 <ns2:cla:
 <ns2:att:
 <ns2:inde
 </ns1:captu:
 </ns1:captu:
 <ns1:buffer :
 <ns1:simpl:
 <ns1:coli
 <ns1:er
 <ns2:
 <ns
 </ns:
 <ns2:
 <ns2:
 <ns2:unsigned>0</ns2:unsigned>
 </ns2:status>
 <ns2:capture_time>2014-05-07T06:45:01Z</ns2:capture_time>
 </ns1:entry>
 <ns1:entry id="2">
 <ns2:value>
 <ns2:..
 </ns2:v
 <ns2:sc
 <ns2:un
 <ns2:st
 <ns2:
 </ns2:s
 <ns2:ca
 </ns1:ent..
 </ns1:column>
 </ns1:simple_data>
 </ns1:buffer>
 </ns1:attributes>
 </ns1:object>
 </ns1:object>

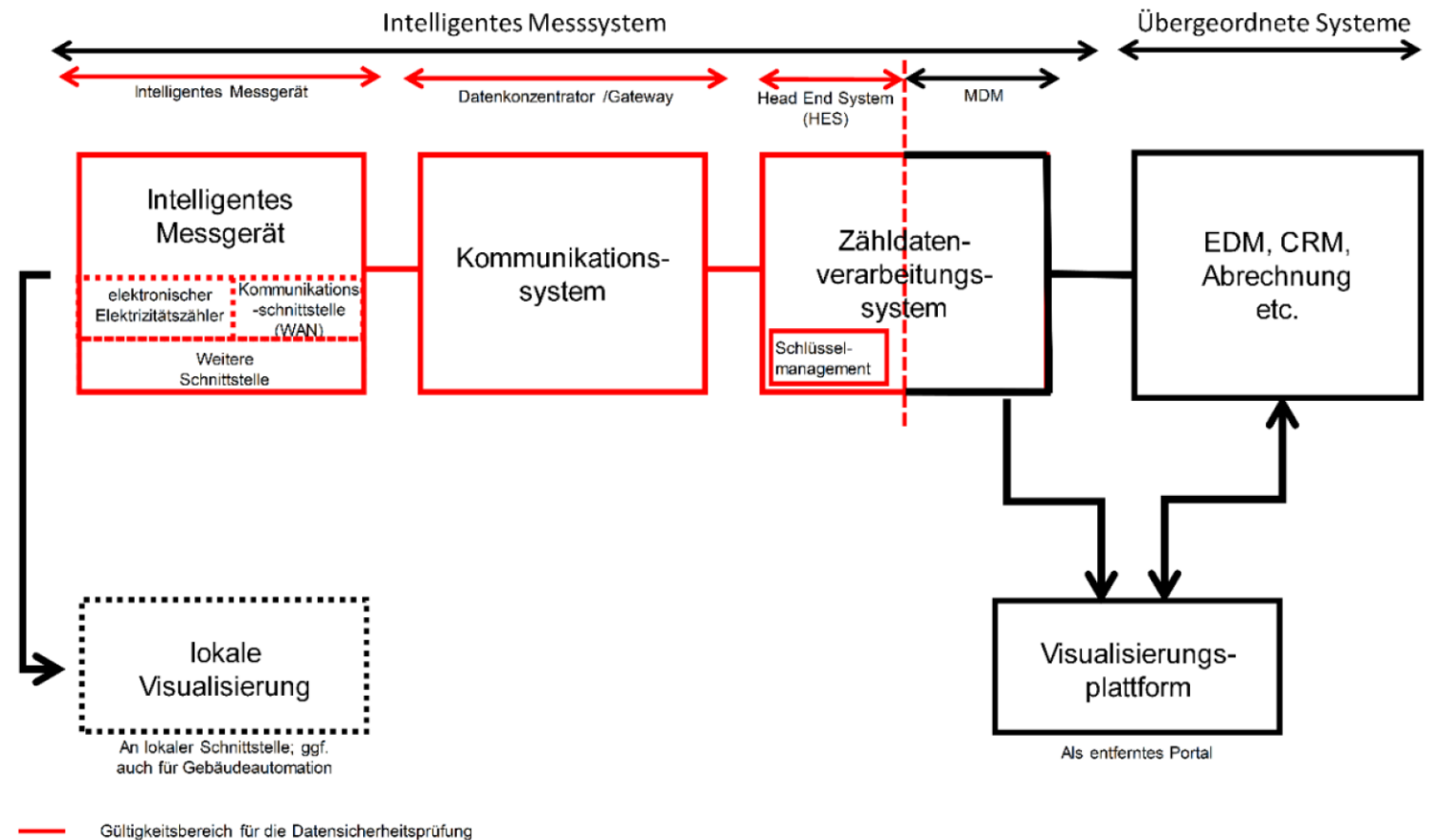
 XML

 DKE VDE DIN

01Z</ns2:capture_time>

Smart Meter Rollout Swiss

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



International

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



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 (8-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

Standardization/Certification

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



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

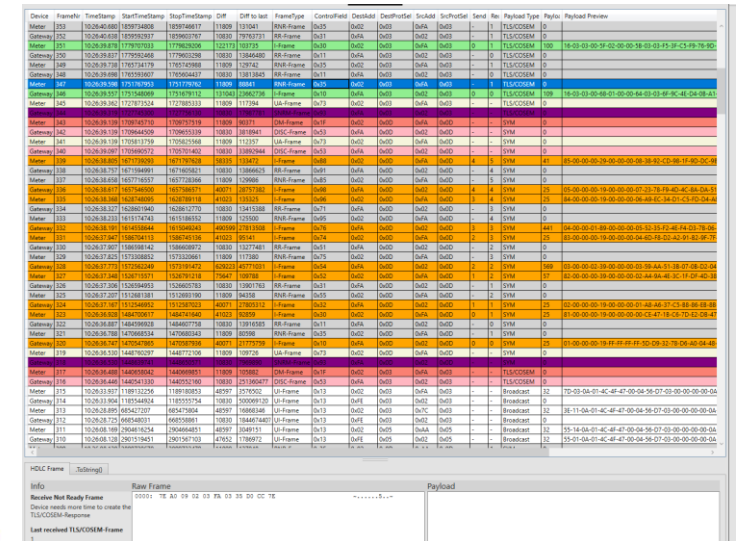
Testing, testing, testing, ...

es:Testsystem

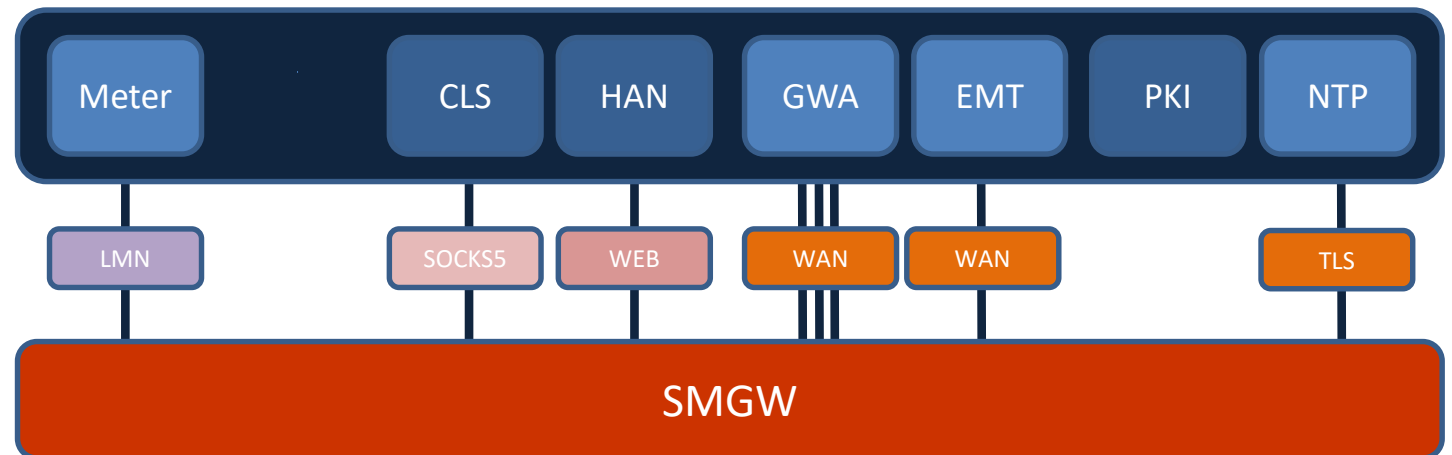
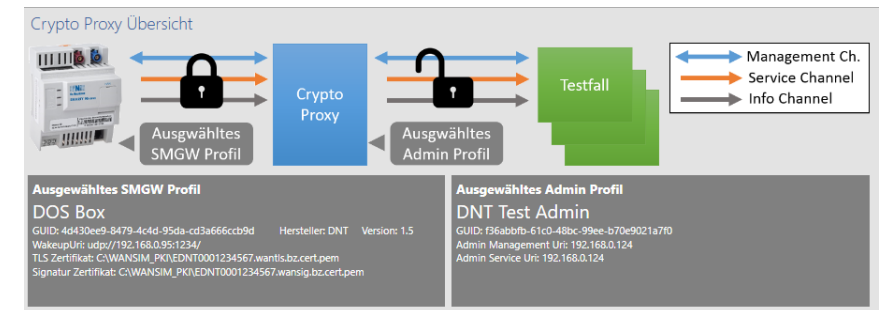
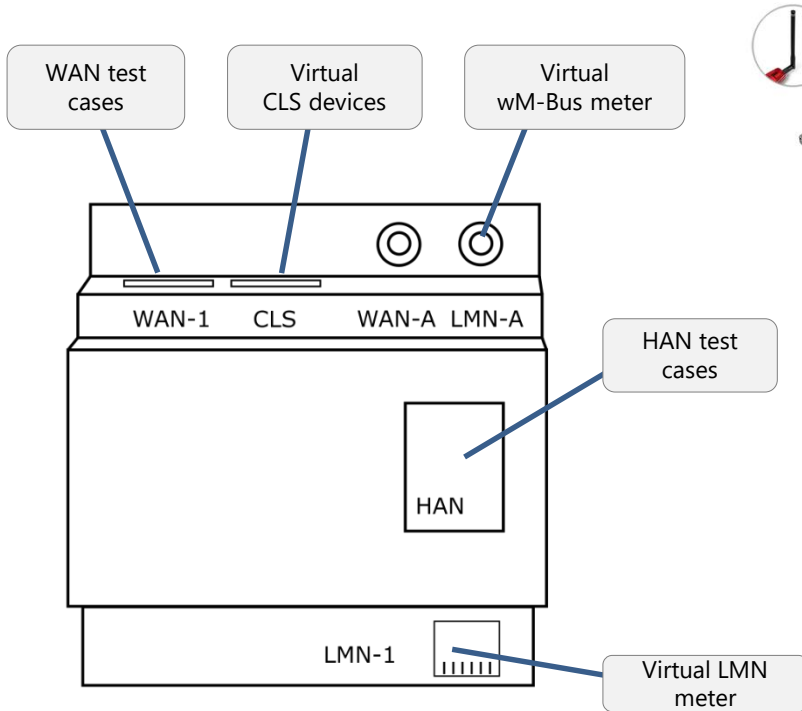


advertising block



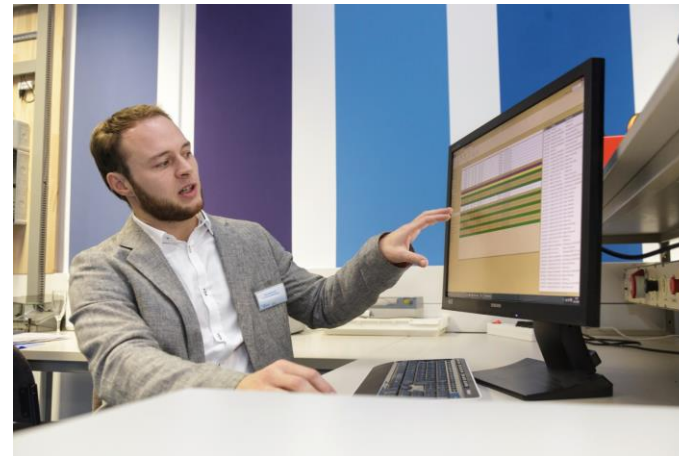
[illegible]

ToE - BSI 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, ...)



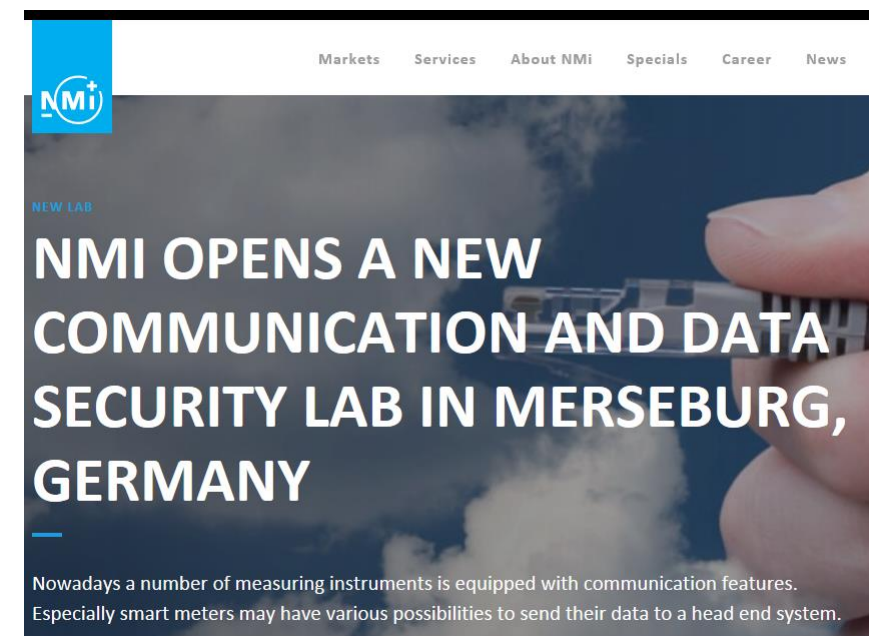
<https://www.nmi.nl/data-security-of-smart-meters/>



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



NMi Smart Meter Test Lab Merseburg, Germany



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

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

- 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

Version: 1.1

Date: 17th July 2016

Authors: SM-CG Task Force on Privacy and Security / ESMIG

AMI ... advanced metering infrastructure

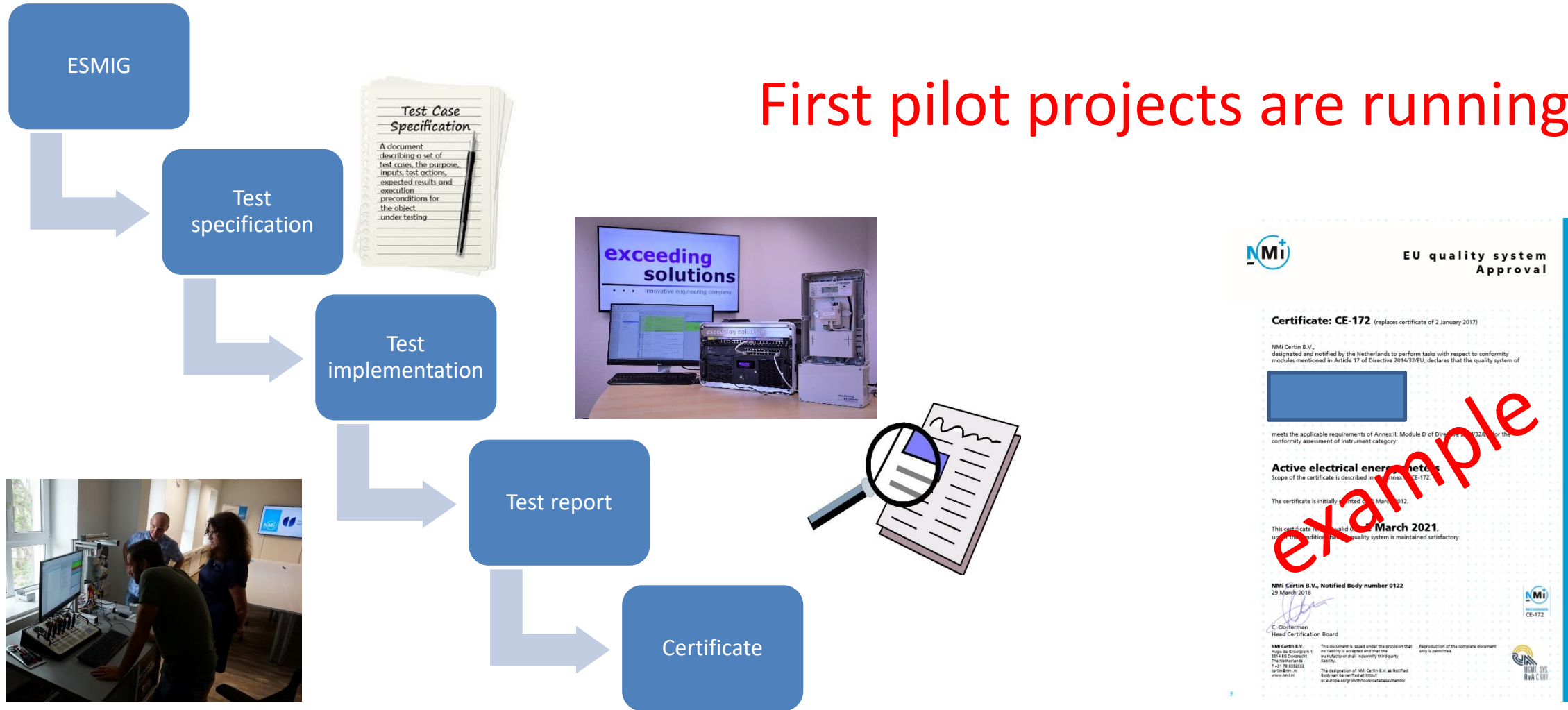
11/10/2019

Electricity & Energy 2019 | November 5-8 | Eilat, Israel



ESMIG ... 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?



Cooperation – Smart Metering

