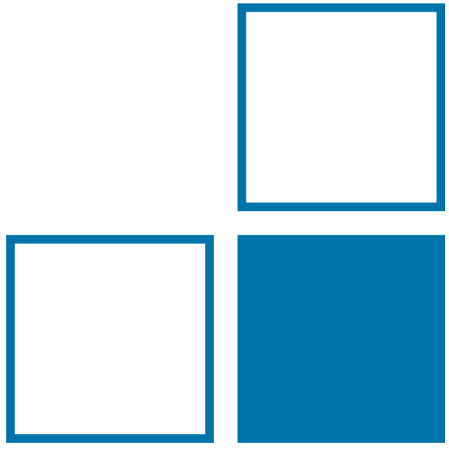
Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

IT security standards applicable for legal Metrology

Jan Wetzlich

WG 8.52 Metrological ICT-systems



Outline

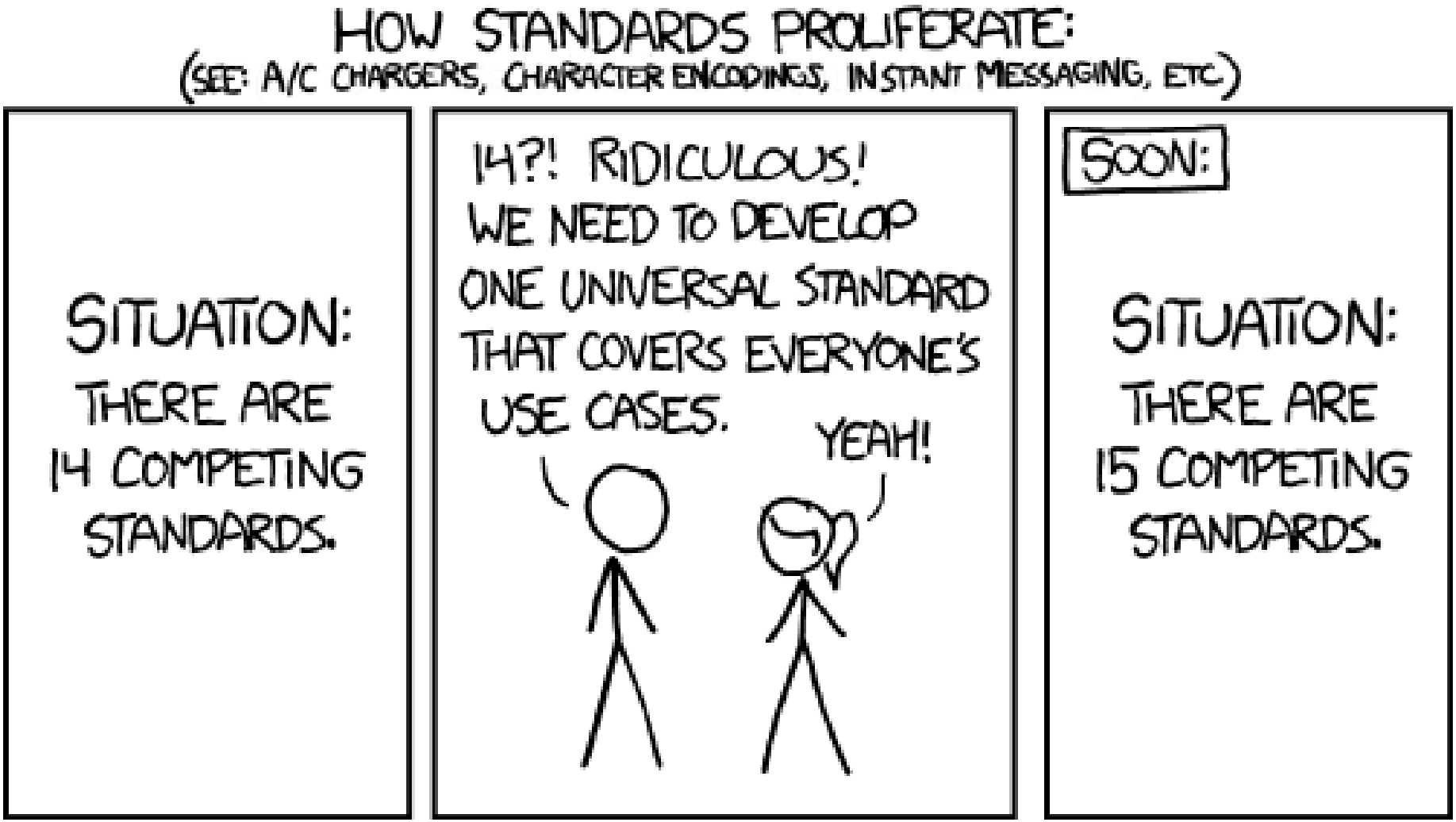
Introduction

Reports on mandate M441/M490

DLMS/COSEM

Conclusions

Introduction



source: https://xkcd.com/927/

Approach

- summarize IT standards
- reuse existing standards for legal metrology?

Relevant IT standards

- European Standards defined/identified by CEN/CENELEC
- on behalf of EU Mandate M441 (Smart Metering) and M490 (Smart Grid)
- standards can be distinguished into process-oriented and implementation-oriented standards
- Device Language Message specification (DLMS)/COSEM for smart metering (IEC 62056-5-3 / EN 13757-1)
- ISO-15408 Common Criteria and ISO-18045 Methodology for IT security evaluation (risk assesment[1])

[1] M. Esche and F. Thiel, Software Risk Assessment for Measuring Instruments in Legal metrology, submitted to Federated Conference on Computer Science and Information Systems (FedCSIS), (2015)

Outline

Introduction

Reports on mandate M441/M490

DLMS/COSEM

Conclusions

Areas to cover according to EU mandate

- prevention of unauthorized disclosures of personal data
- maintenance of data integrity to ensure against unauthorized modification
- effective authentication of the identity of any recipient of personal data
- avoidance of important services being disrupted due to attacks on the security of personal data
- facility to conduct proper audits of personal data stored on or transmitted from a meter
- appropriate access controls and retention periods
- aggregation of data whenever individual level data is not required

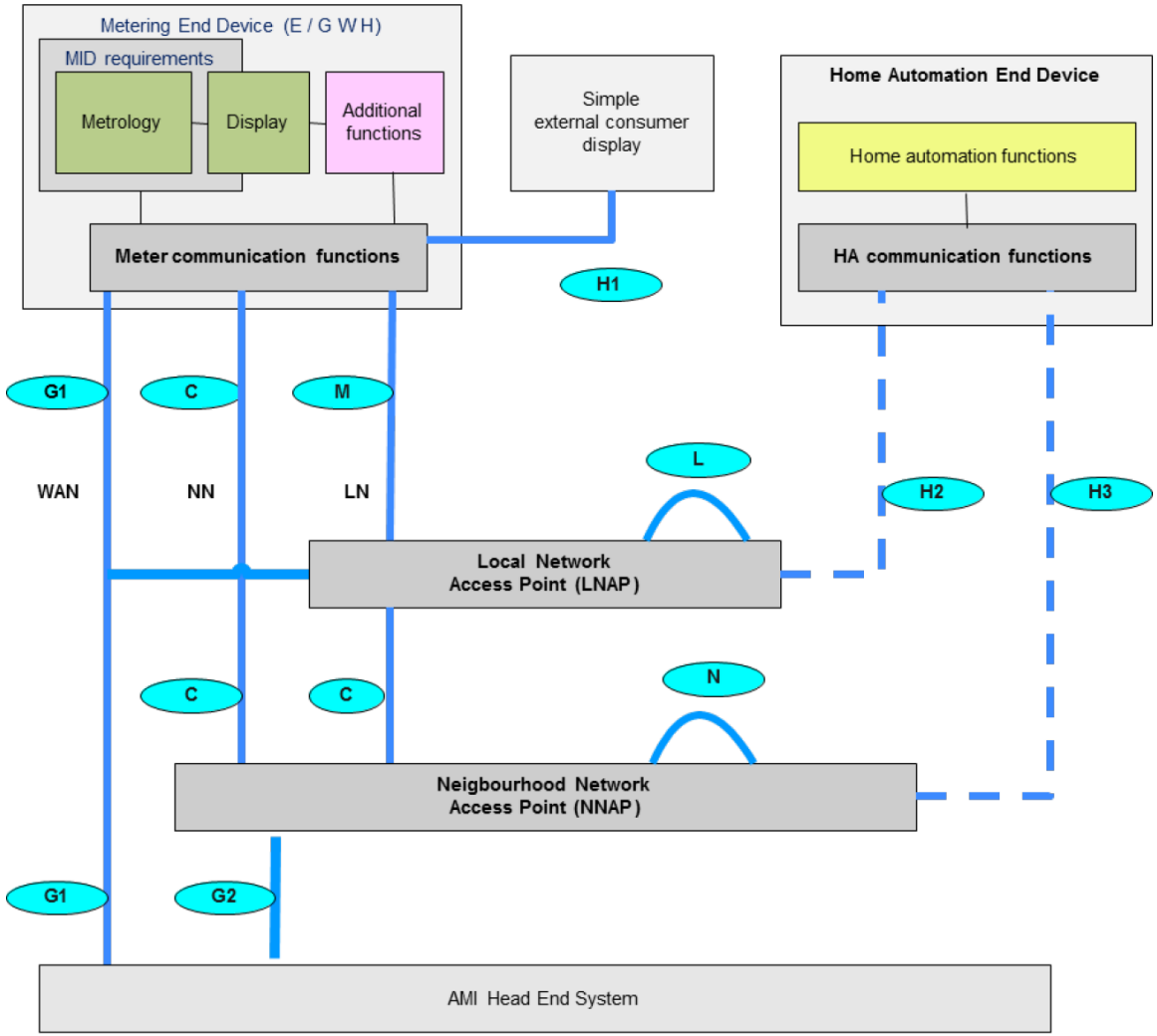
SM-CG Privacy and Security approach – part I

- security requirements for Generic Use Cases
- selected Crypto-algorithms:ECDSA, ECDH, NIST standard Curves P-256 and P-384, AES 128 GCM
- covers unlinkability and unobservability
- IEC 62351 certain security aspects of protocols like TCP/IP, telecontrol in grids, RBAC, Key Management,XML data
- IEC 62443-2-4, IEC 62443-3-3, IEC 62443-4-2 (Industrial communication networks)
- ISO/IEC 15408 + ISO/IEC 18045 Common Criteria

SM-CG Privacy and Security approach – part II

- cover security and privacy within the boundaries of CEN/CLC/ETSI TR 50572

functional reference model



source: SMCG Security and Privacy Report – part II

SM-CG Privacy and Security approach – part II

- cover security and privacy within the boundaries of CEN/CLC/ETSI TR 50572
- approach to define requirements for privacy and security standards
- repository of privacy and security requirements
- application of the European Data Protection Impact Assessment (DPIA)

SM-CG Privacy and Security approach – part IV

- extended security features provide authentication of the communicating entities using:
- a ciphered challenge-response mechanism (High Level Security authentication),
- protection of both DLMS/COSEM application layer messages and COSEM data using symmetric key authenticated encryption (AES-GCM) and digital signature (ECDSA)
- EN 13757-3, Communication systems for meters — Part 3: Application protocols
- EN 13757-7, Communication systems for meters — Part 7: Transport and security services.

Outline

Introduction

Reports on mandate M441/M490

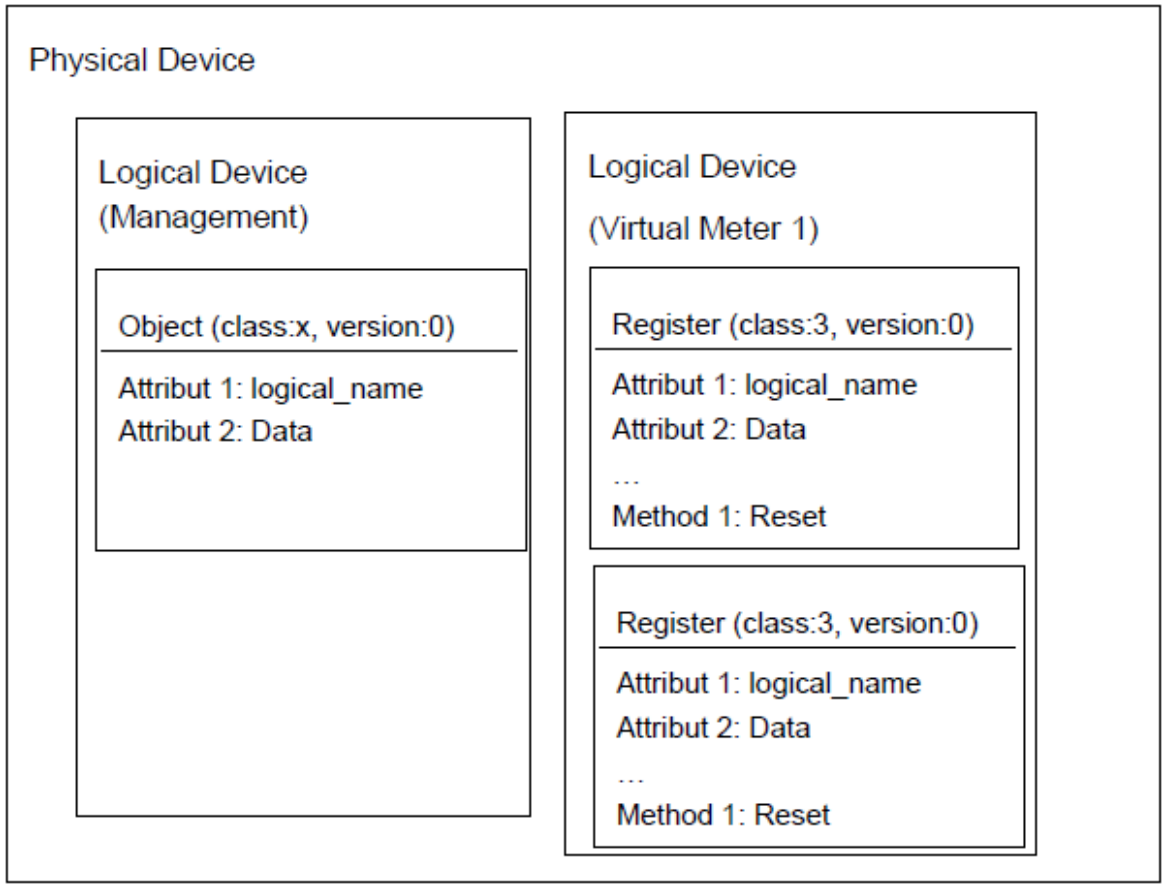
DLMS/COSEM

Conclusions

DLMS/COSEM

- based on object modelling of application data and OSI-model
- COmpanion Specification for Energy Metering (COSEM)
- Device Language Message specification (DLMS)
- IEC 62056-5-3,62056-6-1,62056-6-2

COSEM


Physical Device
Logical Device
(Management)
Object (class:x, version:0)
Attribut 1: logical_name
Attribut 2: Data
Logical Device
(Virtual Meter 1)
Register (class:3, version:0)
Attribut 1: logical_name
Attribut 2: Data
...
Method 1: Reset
Register (class:3, version:0)
Attribut 1: logical_name
Attribut 2: Data
...
Method 1: Reset

Outline

Introduction

Reports on mandate M441/M490

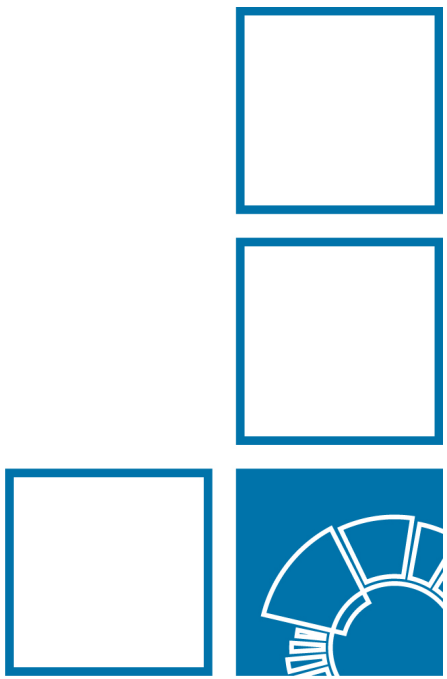
DLMS/COSEM

Conclusions

Conclusions

- use of presented implementation-oriented standards could fullfill certain requirments of MID and WELMEC-Guide
  - basic requirements (type U/ type P)
  - data transmission (extension T)
  - longterm storage (extension L)
- if used for conformity assesment the coverage of essential requirements must be shown
- process oriented standards however are not in line with the product oriented approach of MID and can only be considered as a starting point

Any comments?



Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Abbestraße 2-12
10587 Berlin

Jan Wetzlich
Telefon: 030 3481 7479
E-Mail: jan.wetzlich@ptb.de
www.ptb.de