SIEMENS

The BSI Smart Metering Gateway Protection Profile – an evaluation

Keynote 1 at EIT ICT Labs Workshop SmartGridSec12

David von Oheimb, Siemens Corporate Technology

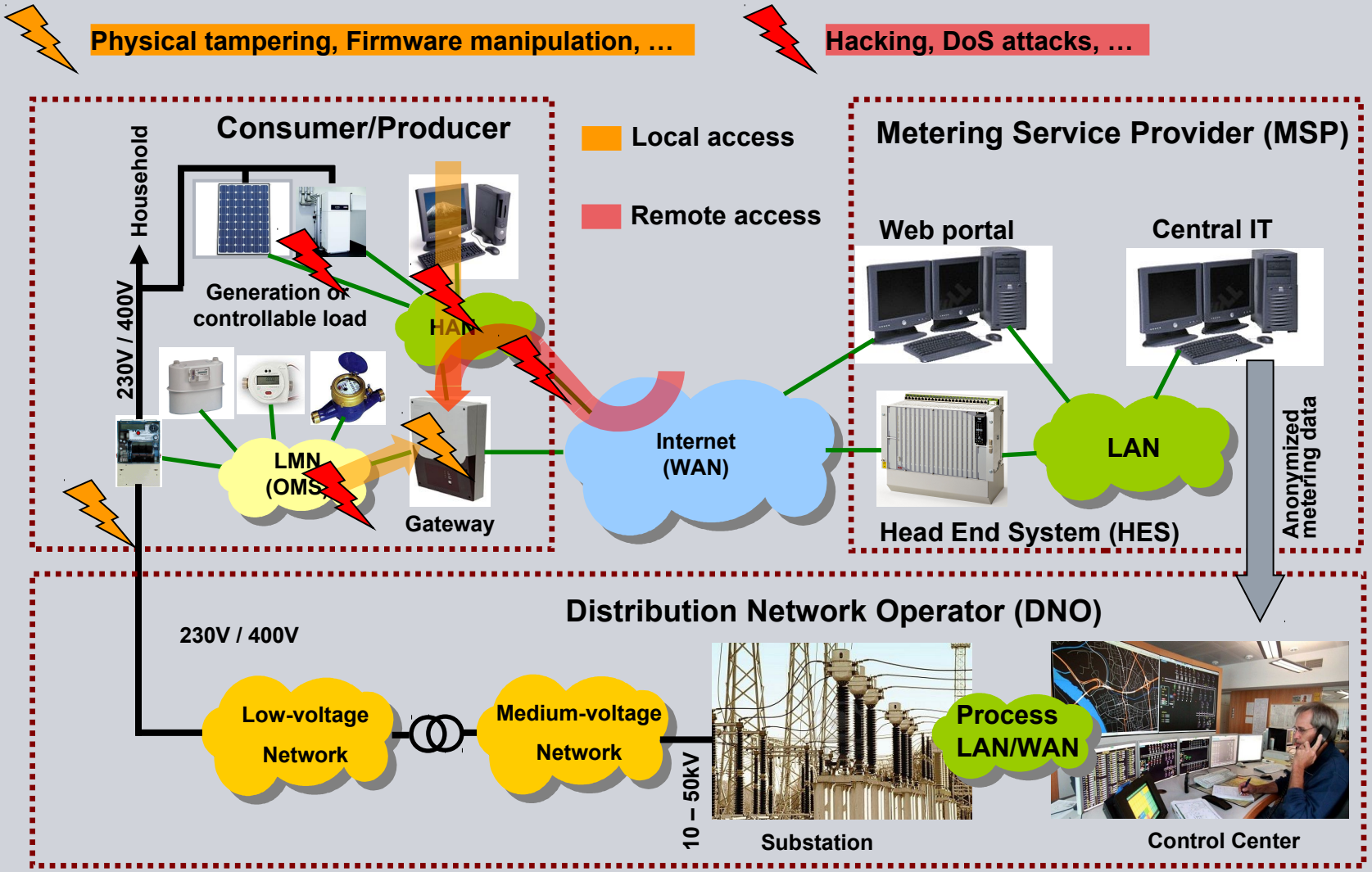
Berlin, 03 December 2012

SIEMENS

Outline

- Application context: Smart Metering (SM) and its regulation
- Certification background: Common Criteria, Protection Profiles
- Technical content of BSI's Protection Profile for SM gateways
- Some comments on the BSI's Protection Profile

Context of the Smart Metering Gateway (GW) with attack points



SIEMENS

History of Germany Smart Metering GW security regulations

- In September 2010, the BMWi (Bundesministerium für Wirtschaft und Technologie) commissioned the BSI (Bundesamt für Sicherheit in der Informationstechnik) to provide a Protection Profile for SM Gateways.
- According to the Common Criteria (CC) approach, the SM Gateway Protection Profile (PP) shall define the minimum security requirements for Smart Metering gateways in an implementation-independent way.
- Since mid-2011, partly to ensure interoperability of Smart Metering devices, several more detailed supplementary guidance documents (TR: Technische Richtlinie) are under development.
- Several commenting rounds with industry have been executed; high amount of feedback has been partly considered in revisions.
- Deadline according to EnWG (§21e.(4) Energiewirtschaftsgesetz) for mandatory use of certified SM gateways was end-2012, but postponed by at least two years due to significant delays in the definition process.

SIEMENS

Common Criteria (CC) for IT security evaluation

Common Criteria

product-oriented methodology

for IT security assessment

ISO/IEC **standard** 15408

Current version: 3.1R3 of July 2009

Aim: gain confidence in the security of a system, via impartial review

- What are the objectives the system should achieve?
- Are the measures employed appropriate to achieve them?
- Are the measures implemented and deployed correctly?

SIEMENS

CC: Security Targets and Protection Profiles

Security Target (ST): defines extent and depth of the evaluation

for a specific product called *Target of Evaluation (TOE)*

Protection Profile (PP): defines extent and depth of the evaluation

for a whole class of products, i.e. firewalls

STs and PPs may inherit ('*claim*') other PPs.

ST and PP specifications use **generic** "construction kit":

- Building blocks for defining *Security Functional Requirements (SFRs)*
- Scalable in depth and rigor: *Security Assurance Requirements (SARs)*

typically layered as *Evaluation Assurance Levels (EALs)*

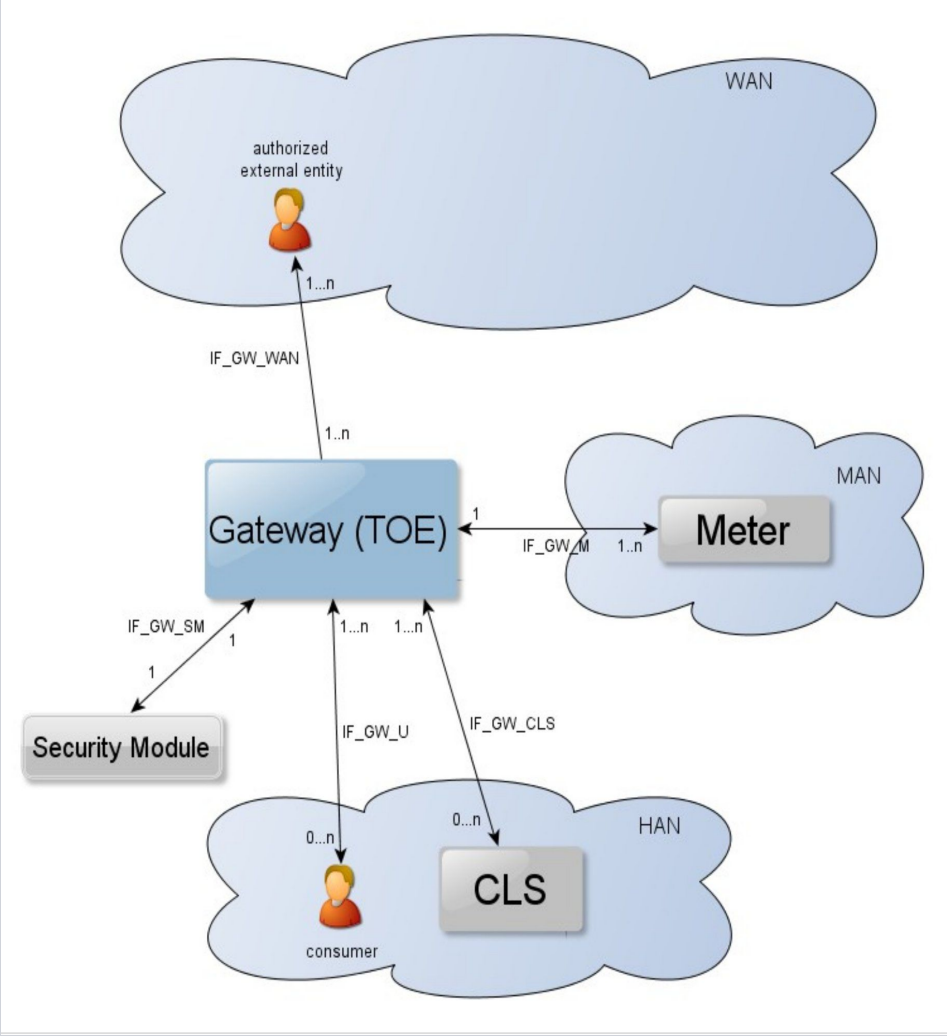
BSI PP for the Gateway of a Smart Metering System: TOE definition (1)

TOE: the local gateway between

Metrological Area Network (MAN)
with meters for commodities

Home Area Network (HAN)
with consumer display and CLS

Wide Area Network (WAN)
with authorized Service Providers



SIEMENS

BSI PP for the Gateway of a Smart Metering System: TOE definition (2)

- **The TOE of the SM PP is a gateway** serving as the communication unit between devices of private and commercial consumers and *Service Providers* of a commodity industry (i.e., electricity, gas, water).
- *Service Providers*: the Gateway Operator, Meter Operator, Metering Service Provider, Grid Operator, Commodity Supplier and others.
- Typically, the Gateway will be placed in the household or premises of the consumer and enables access to local meters and *Controllable Local Systems (CLS).*
- The gateway collects, processes and stores meter data and is responsible for the secure distribution of this data to external parties.
- It protects all critical information using digital signatures and encryption.
- It also serves as a firewall and should have a fail-safe design.
- It contains a mandatory user interface with access control.

SIEMENS

BSI PP for SM GW: List of major requirements (1)

1. Communication security

- Transport-level protection on all channels, with **mandatory use of TLS v1.1**
- Application-level confidentiality, integrity, and authenticity protection
- Firewall functionality: GW is connection initiator with optional wake-up mechanism

2. Cryptography support, mandatory use of Hardware Security Module (HSM)

- Elliptic Curve Cryptography (ECC-256)
- Advanced Encryption Standard (AES-128)
- Secure Hash Algorithm (SHA-256)
- Random number generation (according to BSI AIS 20 / AIS 31)

3. Local key/certificate management with mandatory use of full-blown PKI

- Generate public/private key pairs and secret keys internally
- Store private/secret keys confidentially
- Send public keys in CSR to a sub-CA of the PKI
- Receive certificates from sub-CA
- Store certificates in a tamper-proof way
- Full certificate chain checking including CRLs
- Update of outdated or compromised key material

SIEMENS

BSI PP for SM GW: List of major requirements (2)

4. Meter data handing

- Secure time-stamping of meter data
- Secure logging of application-level events
- Pseudonymization of personal data to support data protection requirements

5. Device management

- Tamper protection and detection
- Secure incident logging
- Secure GW software update
- Key management for connected meters and CLS

6. Local user management

- Authentication of users
- Access control (for consumers and administrator)

Assurance Requirements

EAL4 (methodically designed, tested and reviewed), augmented by

- *AVA_VAN.5 (Advanced vulnerability analysis; resistance to high attack potential)*
- *ALC_FLR.2 (Life-cycle support; flaw reporting procedures)*

SIEMENS

Comments on the BSI's SM GW PP

- Clear security requirements for the gateway
- High assurance level of critical system component
- Strong national standard ensuring interoperability
- Real-time communication support and DoS protection not addressed
- Technical detail: Multiple layers of protection, comprehensive PKI, mandatory use of HW crypto module and point-to-point connections
- Potentially high costs per GW device, installation, and system operation


Questions?
Comments?