Protection Profile for the Gateway of a Smart Metering System
Combining privacy protection with security for the grid

Dr. Helge Kreutzmann (BSI)

12th ICC, 29.9.2011
A Possible Smart Grid
Introduction Smart Meter System

- Entities
  - Consumer
  - Grid Operator
  - Supplier
  - Producer
  - Meter Operator
  - ...

- Assets
  - TOE functionality
  - Physical implementations
Introduction Smart Meter System

- Entities
- Assets
  - Meter data
  - Supplementary data
  - Gateway time
- Meter configuration
- Gateway configuration
- CLS configuration
- ....

- TOE functionality
- Physical implementations
Introduction Smart Meter System

- Entities
- Assets
- TOE functionality
  - Handling of meter data
  - Protection of confidentiality, integrity, authenticity
  - Firewalling
  - Wake-up service
  - Privacy protection
- Management
- Physical implementations
Introduction Smart Meter System

- Entities
- Assets
- TOE functionality
- Physical implementations
  - One box solution
  - Distinct meter(s)
    - One way communication
    - Two way communication
  - ...

Diagram:
- Meter(s)
- CLS
- Display
- Producer
- GW Operator
- WAN
- Local
Assumptions

- A.ExternalPrivacy
- A.TrustedAdmins
- A.PhysicalProtection
- A.AccessProfile
- A.Update
- A.Network

authorised and authenticated external entities receiving any kind of privacy-relevant data or billing-relevant data and the applications that they operate are trustworthy (in the context of the data that they receive) and do not perform unauthorised analyses of this data with respect to the corresponding consumer(s).
Assumptions

- A.ExternalPrivacy
- A.TrustedAdmins
- A.PhysicalProtection
- A.AccessProfile
- A.Update
- A.Network

It is assumed that the Gateway Administrator is trustworthy and well trained.
Assumptions

- A. External Privacy
- A. Trusted Admins
- A. Physical Protection
- A. Access Profile
- A. Update
- A. Network

It is assumed that the TOE is installed in a non-public environment within the premises of the consumer which provides a basic level of physical protection. This protection covers the TOE, the Meter(s) that the TOE communicates with and the communication channel between the TOE and its Security Module.
Assumptions

- A.ExternalPrivacy
- A.TrustedAdmins
- A.PhysicalProtection
- A.AccessProfile
- A.Update
- A.Network

The access control profiles that are used when handling data are assumed to be trustworthy and correct.
Assumptions

- A.ExternalPrivacy
- A.TrustedAdmins
- A.PhysicalProtection
- A.AccessProfile
- A.Update
- A.Network

Firmware updates for the Gateway ... provided by an authorised external entity have undergone a certification ... according to this Protection Profile before they are issued and [are] to be correctly implemented. The external entity is authorised to provide the update is trustworthy and will not introduce any malware.
Assumptions

A. External Privacy
A. Trusted Admins
A. Physical Protection
A. Access Profile
A. Update
A. Network

- a WAN connection with a sufficient reliability and bandwidth
- trustworthy source(s) for an update of system time
- the Gateway is the only communication gateway for Meters in the LMN
- if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) it is appropriately protected
Threats – Data privacy

Power consumption of a fridge

![Graph showing power consumption of a fridge]

Power consumption several devices

![Graph showing power consumption of several devices]

Pictures with kind permission Klaus Müller, Secorvo
Threats: Who turns off the light?

Map: DeStatis/D. Liuzzo
Threats: Who turns off the light?
Threats – Overview

- Internal attacker with physical access
- WAN attacker with remote access (new in metering)

- Main aims of attackers:
  - Privacy violations, e.g. tracking of consumers
  - Billing process manipulation
  - Large scale infrastructure(s) manipulation

- High attack potential:
  EAL4 augmented by AVA_VAN.5 and ALC_FLR.2
Threats as stated in PP

- T.DataModificationLocal
- T.DataModificationWAN
- T.TimeModification
- T.DisclosureWAN
- T.DisclosureLocal
- T.Infrastructure
- T.ResidualData
- T.ResidentData
- T.Privacy
The TOE shall use the services of a **certified Security Module** for

- verification of digital signatures,
- generation of digital signatures,
- key agreement,
- Random Number Generation,
- asymmetric de- and encryption.
The TOE maintains logs:
- system log
- consumer log
- calibration log

Access rules to logs
Retention rules
Security Objectives

- O.Firewall
- O.SeparateIF
- O.Conceal
- O.Meter
- O.Crypt
- O.Time
- O.Protect
- O.Management
- O.Log
- O.Access

- Full and extended information available in PP
Security Objectives

- O.Firewall
- O.SeparateIF
- O.Conceal
- O.Meter
- O.Crypt
- O.Time
- O.Protect
- O.Management
- O.Log
- O.Access

- Data Minimisation, i.e. for each type of process data:
  - Transmission intervals
  - Recipients
  - Signature keys
  - Encryption keys
  - Pseudonymisation (if any)

- → Access Control Profiles
Legal integration

- EU directive mandating the roll out of Smart Meters
- Introduction into German law in summer 2011
  - Gateway required for large classes of consumers, e.g.
    - New installations / Large refurbishments
    - User with consumption > 6000 kWh
    - Prosumers (e.g. solar plant owners), if > 7 kW
  - Only devices certified according to PP may be installed
  - Transition period for mounted devices
- Effective as of 2013

- Introduction into European Standardization in progress
National development

- Development stipulated by BfDI (Federal Privacy Officer)

- Development under auspices of the Federal Ministry of Economics and Technology

- Collaboration with PTB (national metrology), BNetzA (Federal Network Agency) and BfDI and other agencies

- Consulting with Industry organisations:
  - Three commenting rounds with panel discussions
  - > 20 industry organisations participated
  - > 1200 comments received
Impression of an industry meeting
Technical Guideline

- Technical Guideline for Interoperability and continuous security levels

- Topics:
  - Description of the environment
  - Processes involving the gateway
  - Communication protocols
  - Access profiles
  - Public key infrastructures
  - Cryptographic requirements
  - Certification and approval process
The past, present and future

- Jan 2011 – 1st draft version for commenting
- March 2011 – 2nd draft version for commenting
- May 2011 – 3rd draft version for commenting
- August 2011 – Evaluation starts

- End of 2011 – Estimated certification and TR publication
- 2012 – Certifications of Smart Meter Gateways
- 2013 – Deployment of Smart Meter Gateways starts
Contact data

Federal Office for Information Security (BSI)
Dr. Helge Kreutzmann
Section S25
Godesberger Allee 185-189
53175 Bonn
Tel:  +49 (0)22899-9582-5244
Fax:  +49 (0)22899-10-9582-5244
smartmeter@bsi.bund.de
www.bsi.bund.de/SmartMeter
www.bsi-fuer-buerger.de