SMARTMETER

A technological overview of the German roll-out

Peter Hasse

28. Dec 2012

Fraunhofer
FOKUS

Outline

1. Introduction
   - Motivation
   - German laws
   - Organizations
2. Profiles and Guidelines
   - Protection profile
   - Technical guideline
   - Overview
   - Smart Meter
3. Architecture
   - Smart Meter Gateway
   - Security Module
4. Cryptograpic Details
   - PKI
   - Encryption

About me

- Hochschule Bonn-Rhein-Sieg
- FrOSCon
- Fraunhofer Fokus - IT4Energy

Research

- Wireless backhaul networks (WiBACK project)
- Wireless sensor networks
- Evolved packet core optimization

Why?

- Italy and Spain
    - Energy theft
- Sweden, Norway
    - Automated meter reading
- Germany
    - 'Energiewende' change from fossil to renewable energy sources
    - 'Smart Grid' the intelligent energy network ?
        - Controllable local systems (CLS)
- General
    - Direct feedback of commodity consumption for the consumer
    - Communication interface for buildings
    - Third party services

Smart grid

- Role of the consumer changes to a '*prosumer*'
  - Distributed energy production - micro power plants
    - Solar, wind, biomass, etc...
  - Distributed energy storage
    - eMobility
    - In house energy storage
- Change from demand driven production to availability driven consumption
  - CLS - white goods, energy storage
  - Availability orientated contracts / scales
  - Preventing consumption peaks

There are rules!

EnWG – Energiewirtschaftsgesetz ('energy industry act')

- Deregulation of the German energy market
- Discrimination free grid access (controlled by the "Bundesnetzagentur")

[wpea]

EEG – Erneuerbare Energiengesetz ('renewable energies law')

- Roll-out of smart meters
- Offer of time/load-variable energy contracts
- Incentives for feed-in of renewable energies

[wpeb]

There are rules!

NABEG – Netzausbaubeschleunigungsgesetz ('Increasing grid development law')

- Speedup the renovation/extension of the German power grid (e.g. connection of off-shore wind parks)
- BNetzA organizes and approves federal state boarder crossing power grid projects

[wpn]

Involved German federal institutions

BMWi - Federal Ministry of Economics and Technology

- Technology, Energy, Digital Domain
- SME, Industry

BMU - Federal Ministry for the Environment, Nature Conservation and Nuclear Safety

- Environment
- Nature protection
- Reactor safety

Involved German federal institutions

BMI - Federal Ministry of the Interior

- Security, Politics, and Society
- Migration and Integration
- Public Services and Administration

BSI - Federal Office for Information Security

- E-Government
- IT base level security
- Certification, Electronic ID

Involved associations

- Energy, telecommunication, IT, housing industry, consumer protection
    - VDI, DKE, Bitkom
    - Research
    - Universities
    - Equipment vendors
    - ISPs / mobile operators

Time line

- EU-Directive 2006/32/EG for energy efficiency
- 2008 renew EnWg to liberate the measurement business
- 2010 BMWi charges BSI with the development of the Protection Profile and the Technical Guideline
- Jan 2010 new buildings and buildings after complete renovation need to be equipped with digital meters
- Jan 2011 BSI presents first draft
- Renewed EnWg orders usage of the PP
- Dec 2012 BSI publishes RC of the final version of PP and TR
- Jan 2013 deadline for comments
- Dez 2013 deadline for deployment of not conform meters

Overview

- Protection profile (PP) RC1 21.12.12
- Technical guideline TR-03109 (TR) RC1 21.12.12
  - Test specifications (TS)
- Technical guideline TR-03116-3 21.12.12 - cryptography
  - Technical guideline TR-03111 V2 28.06.12 - elliptic curves

[bsi]

Protection profile

- Based on ISO/IEC 15408
- Defines security functions and requirements
  - Physical implementation (i.e. casing)
  - Security module
  - Interfaces
  - Handling of measurement and status data
  - Data protection
  - Management functions
- Defines assets and a threat model

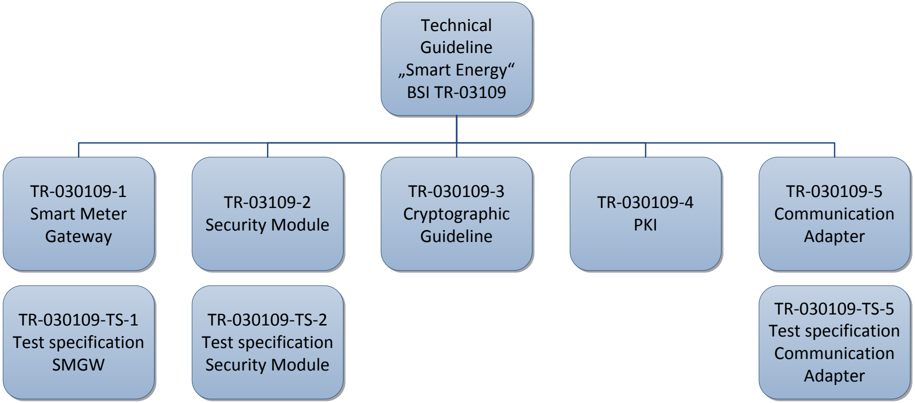
Technical guideline

Extends the protection profile with functional aspects

- Functionality
- Interoperability
- Security

Also defines testing specifications for compliance testing

Overview



Technical Guideline „Smart Energy“ BSI TR-03109

TR-030109-1 Smart Meter Gateway

TR-03109-2 Security Module

TR-030109-3 Cryptographic Guideline

TR-030109-4 PKI

TR-030109-5 Communication Adapter

TR-030109-TS-1 Test specification SMGW

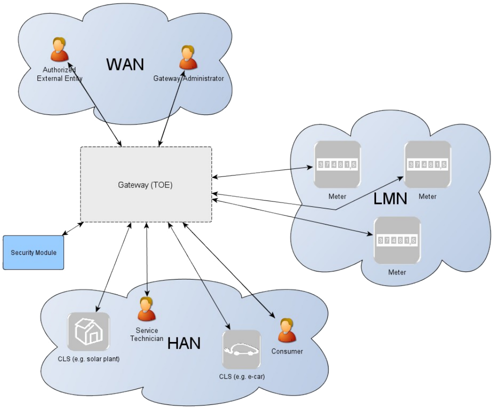
TR-030109-TS-2 Test specification Security Module

TR-030109-TS-5 Test specification Communication Adapter

Roles

- Consumer
- Grid Operator
- Supplier
- Producer
- Meter Operator
- Gateway Operator
- Meter Administrator
- Gateway Administrator
- Gateway Developer
- Profile Provider
- External entity / User

Overview



[TR-12]

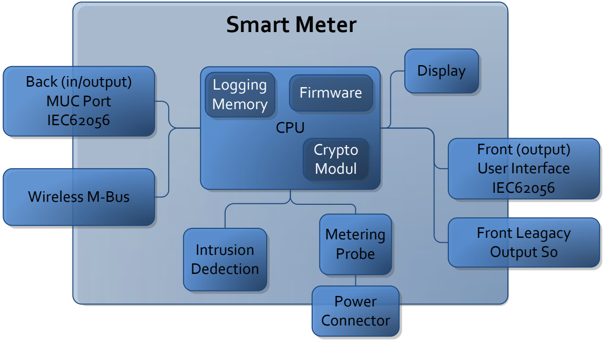
WAN

- GSM / GPRS / UMTS ...
- LAN / DSL / Cable
- PLC
- Fiber

LMN / HAN

- LMN
  - MBUS / Wireless MBUS DIN EN 13757-1
    - Encryption AES+CBC + CMAC
    - IEC 62056-5-3-8 Smart Message Language (SML) transport protocol
    - Based on OMS Specification Volume 2
  - IEC62056
- HAN
  - LAN / WiFi
  - PLC

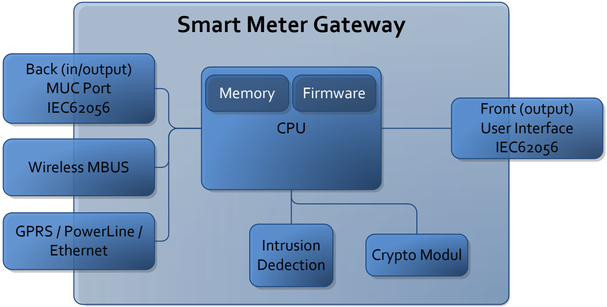
Smart Meter


Smart Meter
Back (in/output) MUC Port IEC62056
Wireless M-Bus
Logging Memory
Firmware
CPU
Crypto Modul
Display
Front (output) User Interface IEC62056
Front Leagacy Output So
Intrusion Dedection
Metering Probe
Power Connector

Tasks - Overview

- Records consumption or production of one or more commodities
- Submits records to the SMGW
- Signing and encryption for the LMN
- Needs to be calibrated and sealed

Components


Smart Meter Gateway
Back (in/output)
MUC Port
IEC62056
Wireless MBUS
GPRS / PowerLine / Ethernet
Memory
Firmware
CPU
Front (output)
User Interface
IEC62056
Intrusion Dedection
Crypto Modul

Tasks - Overview

- Handling of meter data
- Protection of authenticity, integrity and confidentiality
- Firewall
- Wake-Up-Service
- Privacy preservation
- Handling of profiles
- Separation of data from different consumer
- Firmware updates
- Management of security functionality
    - Encryption and signing via Sec Module

Privacy

- Communication concealing
- Pseudonymisation
  - Removing of meter ID's
  - GW ID's need to be removed by the GW administrator
- Data level encryption
- User authentication

Logging - What happened?

- System log
  - System events
  - Only visible to the administrator
- Consumer log
  - Access log to all private data
  - Only visible to the consumer
- Calibration log
  - Calibration relevant events
  - Only visible to the administrator
  - Kept for the whole lifetime of the Gateway

Time

- Over trusted TLS channel
- Only from trusted external time source
    - no GPS, DCF77,... time source
- Reject on to high deviation (max 3%)

Security features

- Memory encryption
- PACE based communication with security module
- Firewall

Communication

- Outgoing connections only (except wake up packet)
- Provides TLS secured channel for all outgoing connections
  - Metering data to gateway administrator
  - Metering data to external party
  - CLS to external party (TLS proxy)
  - Error notification to the administrator
  - Configuration from gateway administrator (via wake up)

Service interfaces

- RESTfull COSEM Webservice
- COSEM interface classes defined in IEC 62056-6-2
- Access via HTTP
- XML transfer syntax
- Addressed via tree structure
- ASN.1 encoding

i.e. https://mysmartmeter.foo.bar.com:2342/smgw/cosem/ldevs/ebsi0112345678.sm

Wake-up-service

- Packet needs to be signed
- Packet needs to have a recent time stamp
- No reply on accept or reject
- Only connection to preconfigured address

Firewall

- Separation between LAN, HAN and WAN
- No services allowed on the WAN interface
  - Except wake up packet

	HAN	LMN	WAN
HAN	X		X
LMN			
WAN			X

Overview

- Cryptographic service provider
- Storage for certificates and keys
- Separated from the SMGW
- SmartCard or soldered module
- PACE between SM and SMGW

Cryptographic Support

- Key generation
- Cryptographic operation
- Key destruction
- Operation for signatures
- Operation for user data encryption
- Random number generation

TR-03116-3

- eCard-Project of the German government
    - Cryptographic guideline for infrastructure of intelligent metering systems
    - Defines the cryptographic mechanisms, primitives and key length
    - Annual update to keep track with the state of development
- SM-PKI
    - National Root-CA
    - Sub-CA end user certificate assurer
    - End user certificates
- Signatures based on ECDSA
- TLS for transport layer security

TLS

- TLS version $>=$ 1.2
- No fall back allowed
- Max 48h per session
- Allways mutual authentication
- Methods
  - ECDSA and ECKA
  - NIST-Domain-Parameter and Brainpool-Domain-parameter
  - Signature generation based on PACE, ECKA-DH, ECKA-EG, ECDSA

Random number generator

- DRG.3 / 4
- PTG.4
- NTG.1

Initialization

- Meter
  - By Vendor or by SMGW
  - Initial exchange on connection to SMGW
- Gateway
  - Intial key set by vendor
  - Can be changed by operator / administrator
- Security Module
  - Either by vendor before integration
  - Or after integration via SMGW

Hashing functions

Method / Parameter	Requirements	From	To
Root-CA			
Signature	ECDSA-With-SHA384	2013	2019+
EC-domain-parameter	NIST P-384	2013	2019+
Sub-CAs			
Signature	ECDSA-With-SHA256	2013	2019+
EC-domain-parameter	NIST P-256	2013	2019+

Meter - Gateway

- TLS “if possible”
  - Fallback to preconfigured symmetric cypher for unidirectional meters
  - Data encryption with derived key + MAC
  - AES CBC / AES CMAC
- Encryption, signing and authentication in the meter
- Re-keying ever two years
- AES CMAC 128 bit

Links

- Bundesregierung - energiekonzepte.
- Technische richtlinie bsi tr-03109 smart energy, May 2012.
- Energie wirtschafts gesetzt.
- Wp - german renewable energy act.
- Netzausbaubeschleunigungsgesetz.

Sorry most links are German.

Thanks!

Thank you! Any questions?

twitter: @d3rp3t3r
mail: peter.hasse@fokus.fraunhofer.de mail@derpeter.net