Security in Smart Metering Systems under the Smart-Grid Perspective

Obaid Ur-Rehman, Natasa Zivic, Christoph Ruland

IEEE BlackSeaCom, May 27-30, 2014, Chisinau, Moldova

University of Siegen
Chair for Data Communications Systems
Univ.-Prof. Dr. Christoph Ruland
Hoelderlinstraße 3
D-57076 Siegen
http://www.dcs.uni-siegen.de

Outline

- Evolution of Smart Meters
- Evolution of Smart Metering
- Need for Smart Grids
- State of the Art in Smart Metering
- Social Concerns
- Commonly used Smart Metering Architectures
- Smart Meter Security Issues
- Smart Meter Gateway / German BSI Protection Profile (PP)
- TERESA Project
- Model Driven Engineering approach to security
- Security Patterns - BSI PP

Evolution of Smart Metering

- Intelligent buildings are not imaginable anymore without smart metering devices.
- Smart metering is used for the provision of instantaneous as well as accumulative metering information to the service providers
  - on commodities such as electricity, gas and water.
- This information is also made available to the customers in order to help in the reduction of costs, energy consumption and emission of CO_2.
- The customers' energy consumption behavior can be adapted dynamically using smart metering devices to balance the power generation and distribution in the smart grid.

Evolution of Smart Metering

- Liberalization of the metering market requires few strong security and privacy requirements for the metering data.
- Governmental organizations are responsible for the permanent correct delivery of metering data and are able to control and maintain the metering devices.

Customer Roles

- A customer has flexibility and can choose to be in one or more of the following roles:
  - Manufacturer of energy
  - Distributor of energy
  - Provider of meters
  - Provider of metering services
  - Consumer of energy
  - Seller of energy

Aims of the Liberalization of the Energy Market

- There are several aims of the liberalization of the energy market,
  - To save money of the consumers by allowing the competition between energy providers.
  - The energy manufacturers and energy providers get up to date information on how much energy of which source is consumed by the customers. Therefore load profiles and a frequent online access to the metering devices are needed.
  - To influence the behavior of the consumers in order to save energy.
    - Therefore consumers should have the possibility to continuously monitor their energy consumption behavior.
  - To strengthen the bilateral trust between the consumer and the producer and to converge on the overall goal of reduction of CO_2 emission.

Metering in the Past (or Now)

- Example: Electricity Meters

What is a Smart Meter?

- Measures the energy consumption.
  - **Digital Measurement** – Very precise.
  - **Memory** – Storage of consumption over a period of time and not just the latest overall consumption value.
  - **Transmission** – Transmits the measurements over a network to remote entities.
- Consumer can see, and therefore, adjust his own power consumption.
- Power provider can adjust the rates and service charges, e.g., expensive rates in peak hours.

Key Features of a Smart Meter

Two-way communication

Smart meters have the ability to send and receive data from the utility. The data is usually sent through cellular network, Wi-Fi, power lines or Radio Frequency.

Time of Usage (TOU)

Smart meters enable the utility to analyse peak consumption time and bill their customers a premium rate for the peak time usuage and also vary the pricing based on demand.

Source: Frost & Sullivan analysis

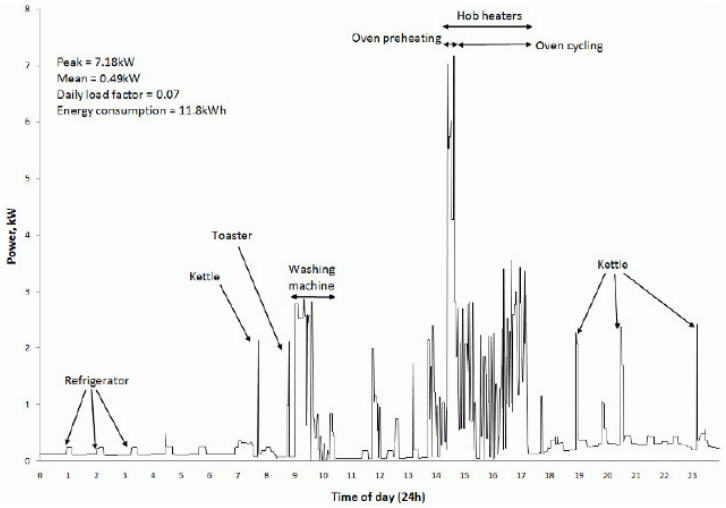
Outage Detection

The system also detects power outages and fluctuations thus making it easier to service and repair the faulty lines.

Key Features

Some of the other features of smart meters are tamper detection, accurate meter readings, power quality monitoring, remote switch off/on and selling electricity back to the grid.

Smart Meter - Consumption Report



Wood G, Newborough M. Dynamic energy-consumption indicators for domestic appliances: environment, behaviour and design. Energy Buildings 2003;35(8):822.

Smart Grid

- Smart Metering Systems are sub-systems of Smart Grids
- A smart grid is a modernized electrical grid that uses digital information and communications technology to gather information, such as the information about the behaviors of suppliers and consumers, in an automated fashion in order to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity.

The need for Smart Grid

- The current grid is getting outdated.
  - It was good enough to serve its purpose so far.
  - Due to advancement in technology, an advanced (smart) grid is required, with many new features including,
    - Self healing
    - Accommodate electricity generation and storage options
    - Consumer oriented
    - Resilient to theft and attacks
    - Optimized operations
- Inaccurate billing hits utility revenue streams
    - Makes financial planning difficult
    - Complicates customer debt management and collection
    - Annoys customers!
- Keep pace with advancement in technology

Smart Metering

- The term smart metering is different from smart meters.
  - Smart meter is a device that measures and possibly stores the consumption of a commodity
  - Smart metering, on the other hand, is referred to the whole infrastructure including,
    - Smart meters
    - Communication networks / infrastructure between the smart meters and other related entities such as,
      - The energy consumer
      - The meter operator
      - The supplier of energy or the utility and the meter data management systems

Need for Smart Metering

- Load Profile
  - A load profile is a plot of the variation in the energy demand versus time.
  - The load profile is useful for power generation companies where it is required to know, in advance, how much energy will be required at a certain time period or over certain duration of time.
- Remote Readout
  - Smart metering also helps in reducing time and costs involved in visits to each and every customer's premises and to record the energy consumption status.
  - This is now done via the ability of remote readout (either automatic or activated transmission of the consumption of the measurements).

Manual Meter Reading

- Traditionally, the meters had to be physically visited and the meter readings had to be recorded manually
  - Mostly on a monthly basis.
- The same was true not only for meter reading but also for meter maintenance.

Electronic Meter Reading

- With the introduction of EMR, meter readers are no longer required to enter the customer premises on a monthly basis to read the consumptions.
- Most of the EMR technologies are walk-by or drive-by
  - The meter is equipped with a radio frequency (RF) transmitter which allows it to transmit the measurement to a receiver.
- The receiver is either a hand held device, installed in a vehicle or uses a tower based radio network for collecting and distributing the readings to the utility.
- The meter to receiver communication can be done over a wireless communication link, e.g., using ZigBee

Automated Meter Reading

- AMR totally eliminates the need for even anyone to pass-by a meter. The meter has the ability to communicate the energy consumption information automatically to a remote readout center over any of the following wired or wireless communication channels,
  - Wireless Radio Frequency (RF) communications, such as, ZigBee, Wireless Meter-Bus (MBUS) etc.
  - Mobile data networks (such as GSM, GPRS)
  - RS-485, Ethernet, Digital Subscriber Line (DSL), Meter-Bus (MBUS)
  - Telephone lines (PSTN), Power Line Carrier (PLC)
- Automated Monthly Reads
- One way outage detections
- Tamper detection

Advanced Metering Infrastructure

- It would not be wrong to call AMI as a revolutionary step rather than an evolutionary step from AMR.
- AMI is the next generation infrastructure which includes,
  - Smart meters
  - Home area networks
  - Communication networks between different meters
  - Communication networks between the meters and the utilities
  - Building management systems
  - Meter data managements systems etc.
- AMI support two way communications between the meter and the utility (or meter operators).
- This allows the meter to be remotely instructed, e.g., to instruct for a remote connect/disconnect or updated for a new service or protocol support based on remote software update.

Advanced Metering Infrastructure

- Two way communication
  - Measurement Reporting
  - Remote Command Executions
- Time based power rates
- In House Display (IHD)
- Remote meter programming (remote software update)

Need for Security!

- With so much data transmission involved, the confidentiality, integrity and authenticity of data can be compromised.
- Security should be included in the design!
  - Right now security patches are applied when needed

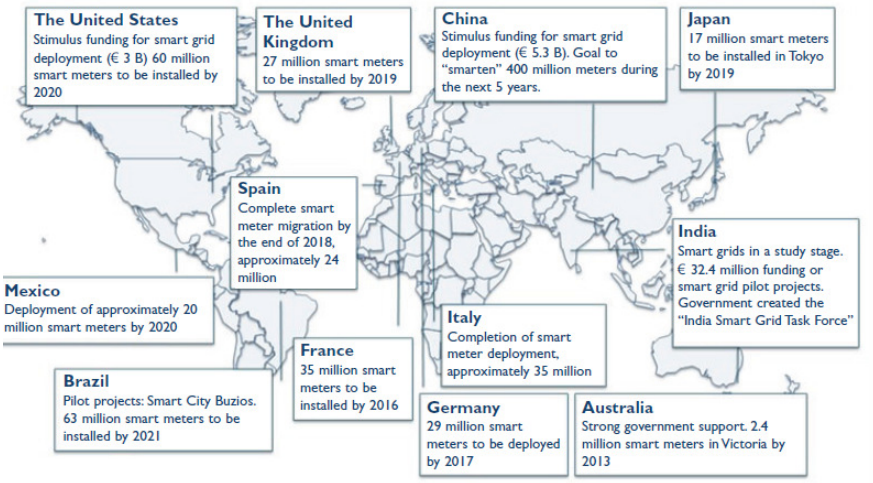
Smart Metering Future Roadmap in Europe

- Since 2008, a European Commission Directive requires energy companies to supply more and better quality information to the consumers about their energy usage, and smart meters is the solution for this.
- From a customer viewpoint, the case needs to be made for cost saving benefits that will deliver a payback over a reasonable amount of time.
  - The same sort of argument is made for fitting home insulation or installing domestic solar panels.

Smart Metering Status in Europe

- At the end of Q3-2012, eleven European countries had developed regulatory roadmaps for the full-scale introduction of smart meters.
  - Sweden, Italy and Finland completed deployments in 2009, 2011 and 2013 respectively
  - Estonia and Norway will be ready by 2017.
  - France and Spain have set the target for 2018
  - Austria, Ireland, the Netherlands and the UK aim for nationwide rollouts to be completed during 2019/2020.
  - Denmark and Malta are on track for full coverage of smart meters before the end of this decade by supporting rollouts by state-controlled electricity companies.
  - Cyprus, Poland, Portugal and Romania are also leaning towards regulation-driven smart meter rollouts.
  - Germany prefers that rollouts should be industry-driven

Smart Metering Projects Around-the-World



Source: Frost & Sullivan analysis

Consumer/Customer Reactions

- There are mixed reactions from consumers about smart meters and smart metering technology.
- The utilities are trying to make their case in favor of smart metering by trying to prove consumer support.
- Some independent and citizen privacy protection and healthcare organizations trying to prove their case of consumer dissatisfaction.
- Different surveys have been conducted both by governmental and non-governmental organizations.

Customer Comments – For Smart Meters

- Smart Metering Implementation Programme, Department of Energy and Climate Change, UK
  - "We had an old fridge freezer, 30 years old, never realised it was using so much electricity, I worked out it was using 30 - 40p a day. We replaced it and it's paid for itself in a year." Owner, Family, 25 - 50, Mixed, BC1, Midlands.
  - "If you fill the kettle up takes longer to boil, you see that go up, you only put in the water you need, or you fill the kettle and make everyone a cup of tea." Owner, Family, 25 - 40, C1C2, Midlands.
  - "It's not been a case of cutting down, more of turning things off that are unnecessary." Owner, Retired, 65+, Mixed, C2D, Scotland
  - "We've definitely seen a difference, we're in credit this year." Owner, Empty nester, 50 - 65, C1, North

Privacy

- Privacy has many dimensions (NIST 7628)
  - Privacy of personal information
    - Personal information is any information relating to an individual, who can be identified, directly or indirectly, by that information
    - Privacy of personal information involves the right to control when, where, how, to whom, and to what extent an individual shares their own personal information, as well as the right to access personal information given to others, to correct it, and to ensure it is safeguarded and disposed of appropriately
  - Privacy of the person
    - This is the right to control the integrity of one's own body. It covers such things as physical requirements, health problems, and required medical devices

Privacy

- Privacy of personal behavior
  - This is the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others
- Privacy of personal communications
  - This is the right to communicate without undue surveillance, monitoring, or censorship

Smart Meters – Breach of Privacy?

- The **Supreme Court** in U.S. affirmed the heightened **Fourth Amendment privacy interest in the home** and noted this interest is not outweighed by technology that allows government agents to "see" into the suspect's home without actually entering the premises.
- The Court stated, **"We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search" and is "presumptively unreasonable without a warrant."**

Protests against utilities

www.stopsmartmeters.org

Stop Smart Meter Campaigns

http://citizensforaradiationfreecommunity.org/

Stop Smart Meters - Canada

coalition TO STOP "SMART" METERS

http://www.stopsmartmetersbc.ca/html/

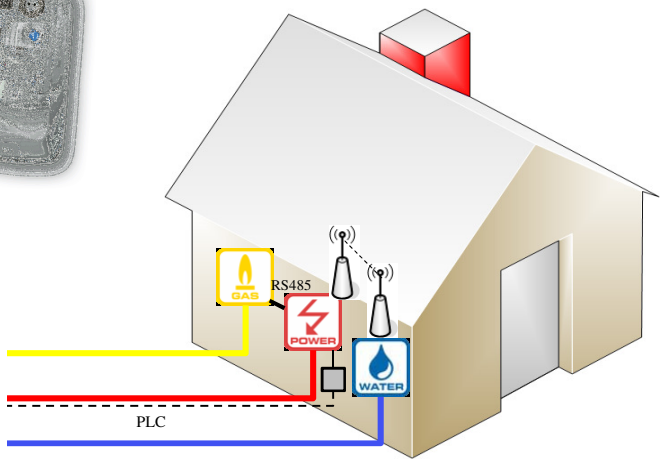
Liberalization of the Energy Market

- Before Liberalization
  - Energy subscribers/consumers
- Now
  - Energy customers
  - Customers are able to choose and to change the Energy Provider
- Everybody should be able to buy and to sell energy
- Separation of generation, sales/trading and transport/distribution of energy
- (Distribution) Network is fixed
- A frequently remote access to energy metering devices is necessary
  - Readout of measurement data
  - Administration

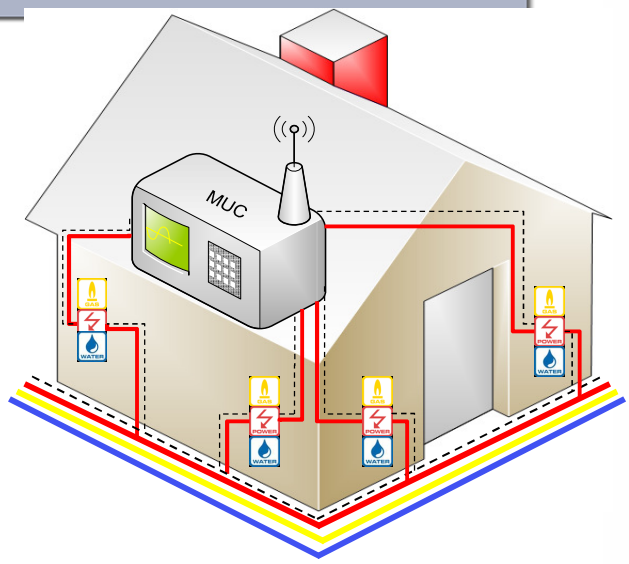
The Bigger Picture

- Before Market Liberalization
  - Energy Provider delivered and maintained the meter
- After
  - Customer can choose Metering Devices
  - Customer can choose Metering Service Provider
- Customer should have online access to the meters
- Customer should easily verify the energy invoice
- Awareness of Energy Consumption should be strengthened
- Energy producer, Provider, Distributor and Consumer should have actual overview over the actual energy situation and costs

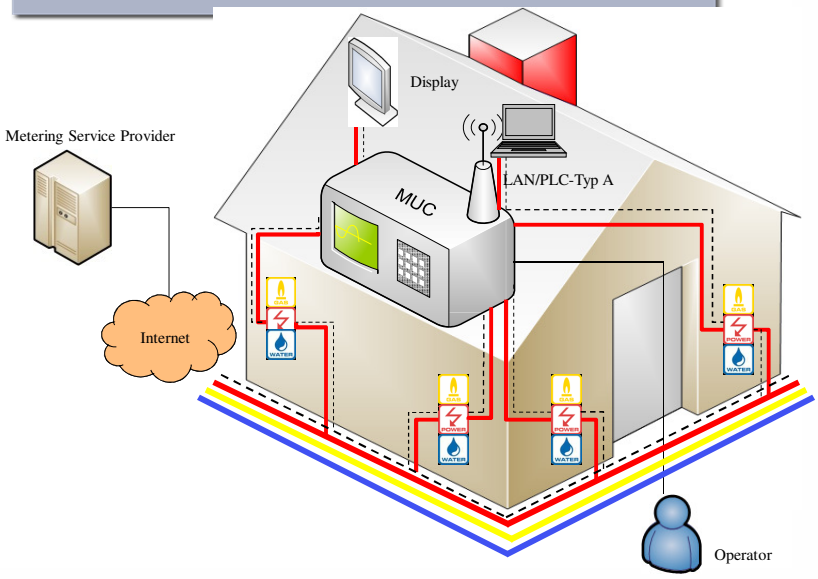
Scenario 1: Family House

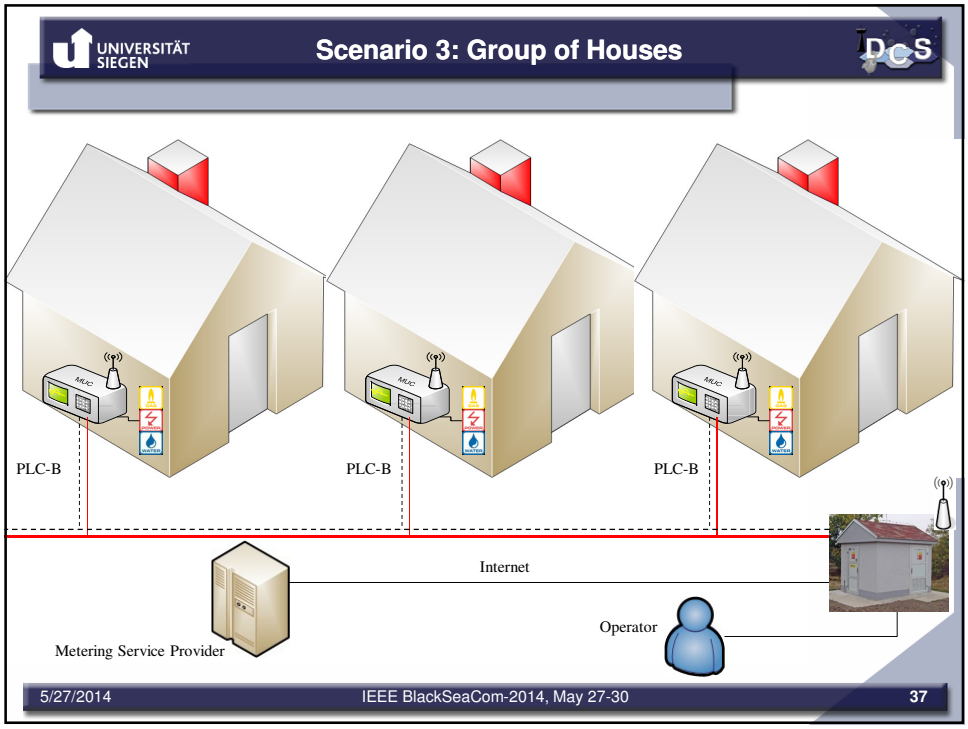


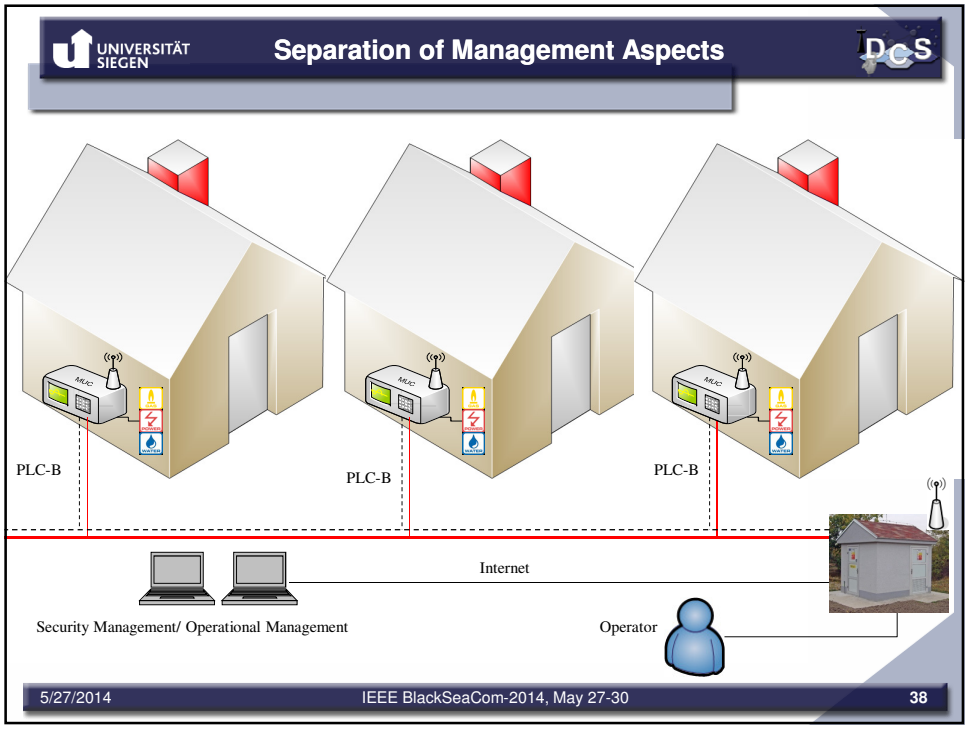
Scenario 2: Appartment House



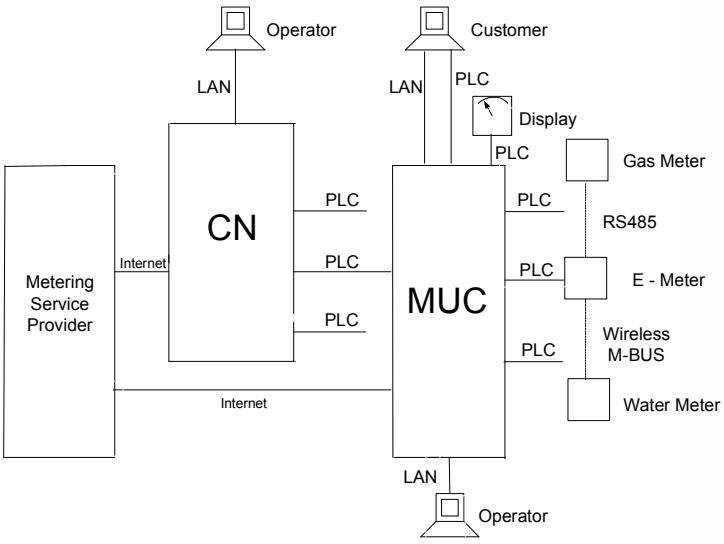
Scenario 2: Appartment House




UNIVERSITÄT SIEGEN
Scenario 3: Group of Houses
DCS
PLC-B
PLC-B
PLC-B
Internet
Metering Service Provider
Operator
5/27/2014
IEEE BlackSeaCom-2014, May 27-30
37


UNIVERSITÄT SIEGEN
Separation of Management Aspects
DCS
PLC-B
PLC-B
PLC-B
Internet
Security Management/ Operational Management
Operator
5/27/2014
IEEE BlackSeaCom-2014, May 27-30
38

Hierarchy of Metering Communication



Data Traffic and Interfaces

Data Exchange

- Metering Data
- Metrological Parameters
- Metrological Logbook
- Metrological Software
- Non Metrological Parameters, Logbook, Software Download

Data Types and Interfaces

- IEC 1107
- DLMS
- SML (Smart Metering Language)

Information Exchange

	Metering Device	MUC	Concentrator
Metrological Institute	Metrological Commands Software Download → Metrological Logbook ←		
Energy Provider	Metering Data ←		
Metering Service Provider	Metering Data ← Non Metrological Commands →	Non Metrological Commands →	Non Metrological Commands →
Customer	Metering ←		
Manufacturer	Non Metrological Commands →	Non Metrological Commands →	Non Metrological Commands →
Local Operator(s)	Metrological and Non Metrological Commands→	Non Metrological Commands →	Non-Metrological Commands →
Consumption Indicator		Metering Data ←	

Legal Requirements

Example of Germany:

- Federal Data Protection Act (BDSG)
- Telecommunications Act together with Telecommunications Data Protection Ordinance
- Tele-services Data Protection Act (TDDSG)
- Digital Signature Act (SiG)
- Verification Act (EichG)
- MID (European Metering Device)

Lawful requirements differs from country to country!!

Security Requirements

	Metering Device	MUC	Concentrator
Metrological Institute	Authentication ↔ Software Download →		
Energy Provider	Authentication ↔ Metering Data ←		
Metering Service Provider	Confidentiality ← Non Repudiation of Origin	Authentication →	Authentication →
Customer	Metering Data ← Non Metrological Commands →	Non Metrological Commands →	Non Metrological Commands →
Manufacturer	Authentication → Confidentiality ←		
Local Operator(s)	Authentication → Non Metrological Commands ↔ Confidentiality ↔ Authentication → Metrological and Non Metrological Commands →	Authentication → Non Metrological Commands ↔ Confidentiality ↔ Authentication → Commands →	Authentication → Non Metrological Commands ↔ Confidentiality ↔ Authentication → Commands →
Consumption Indicator	Authentication ← Confidentiality ←	Metering Data ←	

Security Services, Mechanisms and Protocols

Non-Repudiation of Origin

- Digital Signatures
- Secure Hardware Requirements
- The digital signature will stay together with the information for the lifetime of the information
- SML Signatures
- Root of PKI is governmental metrological institute

Authentication of Data Origin of Commands

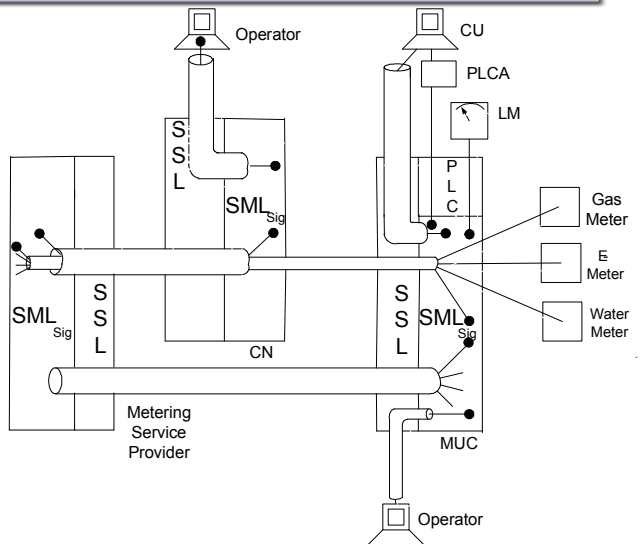
- Digital Signatures
- Certification Authority (Trusted Third Party) as root of PKI
- SML Signatures

Confidentiality

- TLS/SSL on TCP/IP-Connections
- A Certification Authority (TTP) issues the certificates
- Symmetric Encryption on Power Line Communication
- Symmetric Encryption on wireless M-Bus

Access Control

- Access control tables for
  - Commands of functions
  - Change of Access rights



Key Management - PKI

Metering Device

- Generates its own asymmetric key system during the calibration process
- Public key is read out, certified by the calibration authority, written into the metering device and published
- These keys are used for digital signatures providing long-term non-repudiation.

Concentrator and MUC

- Each concentrator or MUC generates its own asymmetric key system, the public key is read out and certified by the manufacturer and published.
- These keys are used for SSL/TLS communication.

Key Management – Public Key Infrastructure

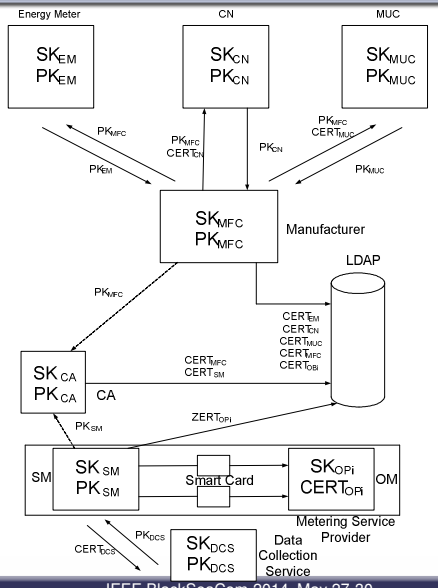
Manufacturer of MUC, Concentrator and Metering Devices

- Each has a certified asymmetric key system.
- These keys are used for SSL / TLS communication

Provider of Metering Services / Data Collection

- Security Management (SM) and Operational Management (OM)
- The security management owns a public key system
- The security management generates public key systems and certificates extended by role oriented access rights of the OM technicians.
- The private key of SM is also used for digital signatures of security relevant commands to the components.

Public Key Infrastructure



Key Management - Symmetric

User

- Password for access via LAN with TLS or PLC to MUC

PLC-Adapter and MUC

- Symmetric keys for PLC encryption (confidentiality)

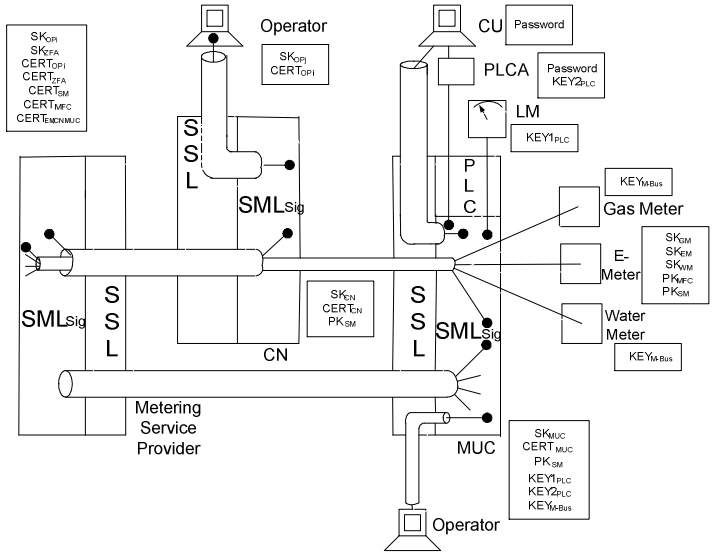
Wireless M-Bus

- Symmetric keys for wireless M-Bus encryption (confidentiality, data integrity)

Energy Consumption Display

- Symmetric keys for PLC encryption

Distributed Keys after Initialization



Use Cases

The Security-, Key- and Rights Management supports the following use cases:

- Initialization
- Reading Metering Data
- Management / Parametrization / Software Download (Metrological and Non-Metrological)
- Replacement of Metering Devices, MUC and Concentrator
- Change of Energy Provider
- Change of Metering Device Owner
- Change of Metering Service Provider
- Change of Data Collector

Smart Metering Security Issues

- Inventiveness and sophistication of the criminals and energy thieves evolve with the security technology.
- Perceived security and privacy violation of customer may lead to the customers' rejection of smart meters.

Initial Step - Pre Payment Meters

- UK introduced the pre-payment meters.
- Customers to pay in advance for their energy, using a special key with their electricity meter.
- The key is "topped-up" with credit every time the customer pays for electricity at an official outlet.

Pre-payment Meter Fraud

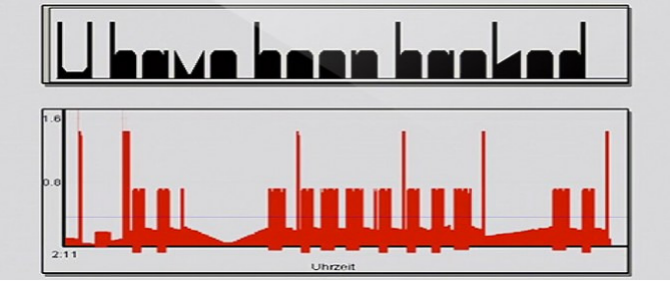
- Energy companies have uncovered a doorstep scam which seems to offer cheaper electricity meter top-ups but just ends up with customers paying twice. 114,000 customers out of 3.7 million customers of the leading energy companies have been affected by this fraud.
- The fraud involves the production or cloning of electricity prepayment meter top-up keys and sold at around 50% of the actual price.
- Criminals imitating energy company employees.
- Research has revealed that those most likely to obtain illegal top-ups are people aged 18-35, either in their 20s and living in shared accommodation or in their 30s, unemployed or on low income and single.

Hacking a Smart Meter

- At the 28th Chaos Communication Congress (28C3), Stephan Brinkhaus showed how the smart meters associated with the German energy company **Discovergy** used improperly configured SSL.
- The company also did not encrypt the consumer data.
- Brinkhaus also used the smart meter's MAC address to spoof the unencrypted packets going back to Discovergy.
- Not only was it possible to tamper with the smart meter results, it was also possible to manipulate data spikes and valleys in one report to read "U have been hacked"
- They showed that the type of LCD TV set could be identified, what TV program was on, or if a movie was playing from a DVD or other source.

Hacking a Smart Meter

- Discovergy has a web interface so consumers can plot their own data for the last three months.
- Although there was no API, no way provided by Discovergy to download the data, the researchers used a HTTP GET request to retrieve all data, finding that one value every two seconds can be downloaded.



General Threat Model for Smart Meters

- **Curious eavesdroppers:**
  - Who just want to know about the activities of their neighbors.
- **Motivated eavesdroppers:**
  - Who want to gather information for malicious purposes.
- **Unethical customers:**
  - Who want to steal electricity and not pay for the services.
- **Intrusive data management agencies:**
  - Who want to gather private information and create user profiles for marketing and economic purposes.
- **Active attackers:**
  - Who want to perform large-scale attacks. Terrorist activities fall into this category.
- **Publicity seekers:**
  - Who are more interested in getting famous rather than harming the users and gaining financial rewards.

F. Molazem, Security and Privacy of Smart Meters: A Survey, University of British Columbia

Potential Attacks agains Smart Meters

- **Network:**
  - Communication interception and traffic analysis. Traffic modification, injection, and replay.
- **System:**
  - Authorization or authentication violation. Spoofing of utility system. Compromise node, spoofing of metering device.
- **DoS:**
  - Resource exhaustion, Signal Jamming, Dropping packets.
- **Smart Meter Software:**
  - Replace the software of a smart meter.
    - Metrological
    - Non metrological

DoS Attacks

- This kind of attacks will target the whole grid or part of the grid and can be performed by an adversary sending many more than expected commands to the gateways or on the other end to the utility servers.
- This will saturate the system to an extent that it is no more able to respond to the legitimate requests.
- It will essentially shut down the grid or part of grid for essential services.
- The scope of this attack is the whole grid or parts of a grid.
- Such attacks can mostly be launched through the WAN.

Malware / Packet injection attacks

- Another category of active attacks is the injection of malware into the grid.
- This will affect the communication between devices in the grid and can compromise the billing and reporting processes.
- False bills can be generated and can cost the customers and utilities a lot of money.
- The demand / consumption status of the grid can be disrupted to destabilize the load on the grid.
- The scope of this attack is also the whole grid or its components.
- Such attacks can also be launched from the WAN.

Remote connect / disconnect

- The remote connect / disconnect facility of the smart grid can be exploited by furious attackers, bringing the grid or its components to halt.
- If launched on a massive scale, this attack can leave a lots of users disconnected from electricity, gas and water supplies.
- The scope of such attacks can be anything from a single premise to the whole grid.
- Such attacks can be launched via the WAN.

Firmware manipulation

- Manipulating the firmware of a smart meter / gateway
- Metrological firmware
  - If the metrological part is manipulated, the attacker can disrupt the billing and accounting process of the meter that is affected by the attack.
  - This includes manipulating the pre-payment functionality or reporting false consumption status to the remote readout entity.
- Non-metrological firmware
  - If the non-metrological part is manipulated, other objectives can be achieved.
  - The firmware manipulation attacks can be done by manipulating a smart meter (or a smart meter gateway) through physical access. However, such attacks can also be launched via the WAN if the gateway supports remote firmware upgrade.
  - These attacks will normally affect single user (or premises/building) but can also be launched on a massive scale by remotely manipulating the firmware of a large number of gateways.

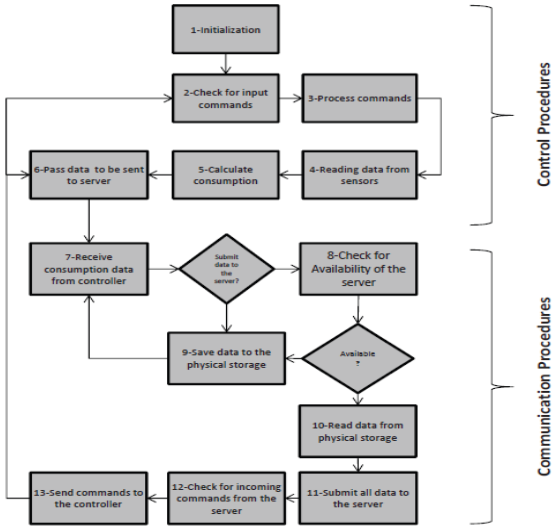
Man in the middle attacks

- In man in the middle attack, an attacker inserts himself in the middle of communicating parties.
  - The attacker makes connections with both the parties, captures their messages and relay them to the other end and makes them believe that they are talking directly to each other.
  - Thus the attacker has the freedom of either simply seeing the communication or modifying the information being exchanged between the communicating partners.
  - The man in the middle attacks can be launched in LMN or WAN.
  - If launched in the LMN, it can be used to compromise the communication between a meter and a gateway and to provide false feedback to the gateway from a meter. Thus false measurements will be transmitted by the gateway.
  - If the attack is launched in the WAN, the security and privacy of the whole communication can be compromised.

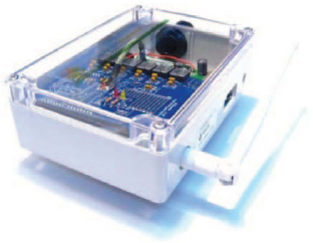
Security by Design

- A systematic method for modeling functionalities of smart meters and deriving attacks that can be mounted on them was proposed by Tabrizi and Pattabiraman.
- Method applied to a real open source meter and two attacks are implemented.
- Identify the attacks using the „Abstract Model“ of the software.
  - Abstract Model represents behaviour.
- Map the attacks to the Concrete Model
  - Concrete model is a real implementation of the abstract model
  - Tabrizi, F.M.; Pattabiraman, K., "A model for security analysis of smart meters," IEEE/IFIP 42nd International Conference on Dependable Systems and Networks Workshops (DSN-W), pp.1,6, 25-28 June 2012.

Abstract Model of Smart Meter



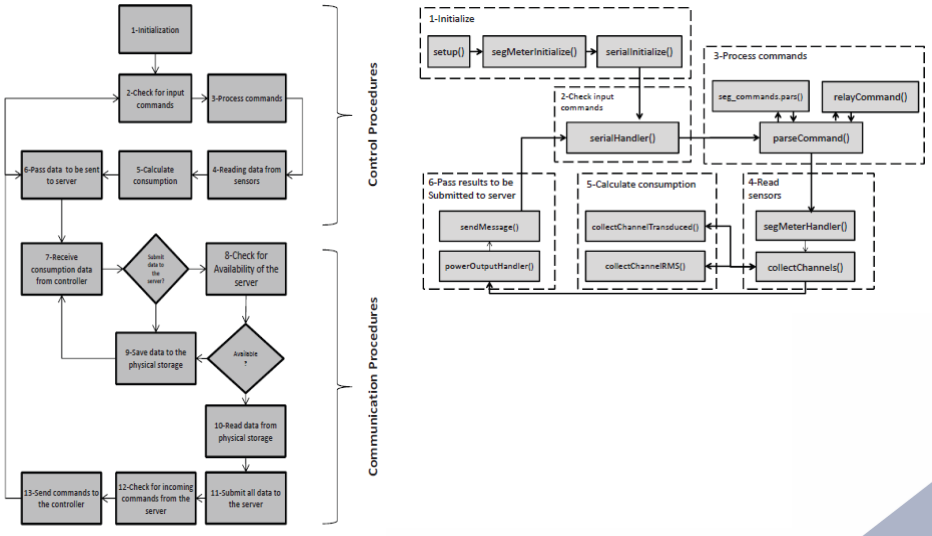
SEGMeter



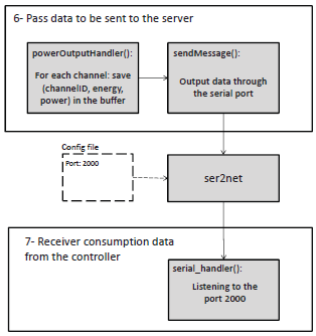
Arduino board with sensors and ATMEGA32x series microcontroller

A gateway board which has LAN and wifi network interfaces, and communicates with the utility server.

Concrete Model of Smart Meter

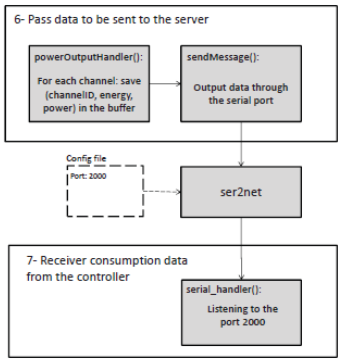


Vulnerability



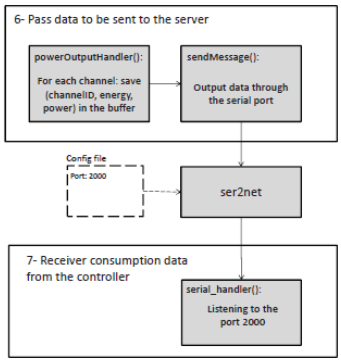
Communications Interface Attack

- This attack is associated with blocks 6 and 7 of the abstract model and targets the communication link between these blocks.
- The serial port is connected to the gateway board.
- A process called ser2net runs on the gateway board which acts as a proxy between the serial port and other processes on the gateway board.
- A a fake ser2net process is written which, at startup, replaces the original ser2net process and starts listening to port 2000.
- The fake ser2net process produces fake consumption data, and through port 2000, passes it to *serialHandler()*



Physical Memory Attack

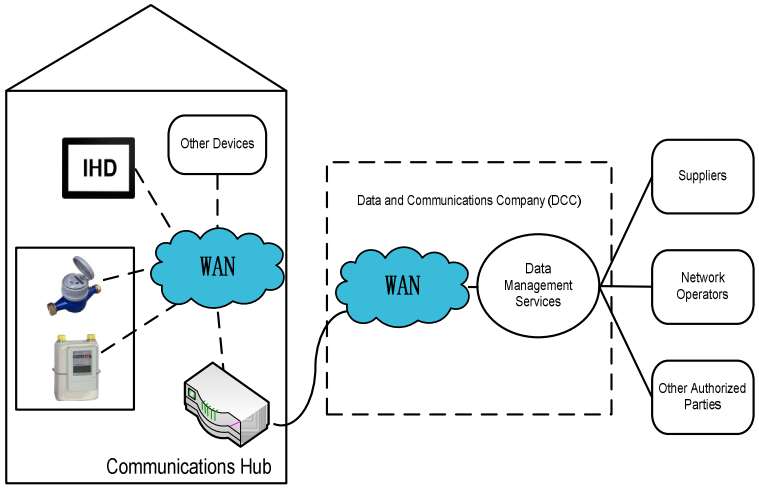
- In case of network disconnection, the status of the meter changes to 'disconnected'.
- The next time that the connectivity check is successful, the status of the meter will be changed to 'reconnected'.
- During the time period from 'disconnected' to 'reconnected', the consumption data is stored on flash memory.
- The meter continues working in 'disconnected' mode for 10 minutes and then it is automatically restarted.
- A script that deactivates the network interface, and overwrites the data file with fake data during the 'disconnected' period.
- Activating the script periodically can significantly modify the power consumption.



Smart Meter Gateway Approach in the EU

- There is currently a significant progress in many countries towards developing a Gateway based approach for Smart Metering Systems
- The meter is separated from the Gateway
- The gateway acts like a communication center for all the meters installed in the premises of the customers
- The gateway is also the first line of defense from security perspective

Smart Metering Gateway - UK

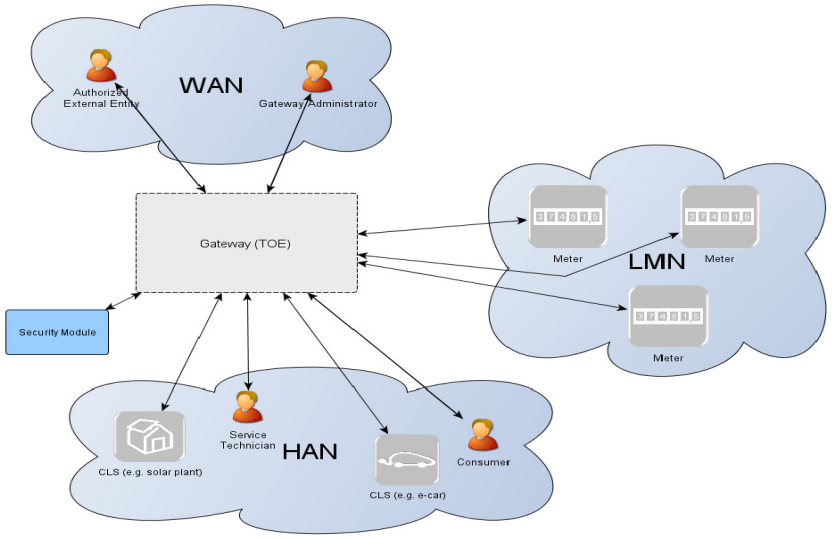


* Smart Metering Implementation Programme, First Annual Progress Report on the Roll-out of Smart Meters, Department of Energy and Climate Change, UK

German Approach

- Protection Profile for the Gateway of a Smart Metering System
  - German Federal Office for Information Security (BSI)
  - Protection profile (PP)
  - Mandatory after a transition period
  - Gateways need CC Evaluation and Certification
  - Type approval of PTB still relevant
  - Security by Design

Smart Metering Gateway - Germany



Protection Profile

- The BSI PP for the communication Gateway interfacing with the Wide Area Network, mandates the usage of a hardware based security module.
- This gateway is to reach a Common Criteria EAL4+ security level.
- The VaultIC4xxx Security Module is one of several security solutions in the industry that already offers this security level, reducing to its minimum the certification effort for the gateway manufacturer.

Security Module

- Hardware based „Security Module“
  - Key generation
  - Cryptographic operations
  - Key destruction
  - Operations for ditial signatures
  - Operations for user data encryption
  - Cryptographically secure random number generation
- These can be realised using VaultIC4xxx devices from Inside Secure.

Communication Module

- BSI PP mandates dual encryption.
  - At the application layer
  - At the communication layer
- The application layer encryption is for end to end security
- The communication module of the Gateway provides communication layer security for using SSL / TLS based security
- Can be linked to the hardware based Security Module for cryptographic services

TERESA

- TERESA: **T**rusted Computing **E**ngineering for **R**esource Constrained **E**mbedded **S**ystems **A**pplications.
  - Funded by European Commission Seventh Framework Programme
  - Duration: Nov 01, 2009 – Oct 30, 2012
  - www.teresa-project.org
- A Project to define, demonstrate and validate an engineering discipline for trust, that is adapted to resource constrained embedded systems.
  - Trust as the degree with which security and dependability requirements are met.
  - Based on Model Driven Engineering

Model Driven Engineering

- A software development methodology which focuses on creating and using domain models
  - Abstract representations of the knowledge and activities that govern a particular application domain
  - Rather than on the computing (or algorithmic) concepts
- The MDE approach is meant to,
  - Increase productivity by maximizing compatibility between systems (via reuse of standardized models)
  - Simplify the process of design (via models of recurring **design patterns** in the application domain)

Design Patterns

- A pattern is a general reusable solution to a commonly occurring problem in design.
  - A design pattern is not a finished design that can be transformed directly into code.
  - It is a description or template for how to solve a problem that can be used in many different situations.
  - Algorithms are not thought of as design patterns because they solve computational problems rather than design problems.
  - *Secure Design Patterns, Computer Emergency Response Team (CERT), Carnegie Mellon University, Oct 2009.

Secure Design Patterns

- Secure design patterns are meant to eliminate the accidental insertion of vulnerabilities into code and to mitigate the consequences of these vulnerabilities.
  - Secure design patterns address security issues at widely varying levels of specificity ranging from architectural-level patterns involving the high-level design of the system down to implementation-level patterns providing guidance on how to implement portions of functions or methods in the system.

TERESA Patterns Set

- Set of identified patterns
  - Secure Remote Readout (SRR)
    - Communication of readout data
  - Wakeup Service (WS)
    - Establish connection from WAN
  - Secure Logger (SL)
    - Security relevant log data
  - Secure Communication
    - Transport Layer Security (TLS)
    - Required by PP
  - Key Manager (KM)
    - Manage key material
  - Smart Meter Gateway Skeleton (SMGW-S)
    - Architecture
  - Random Number Generator Test (RNG-Test)

Thank you for your attention!