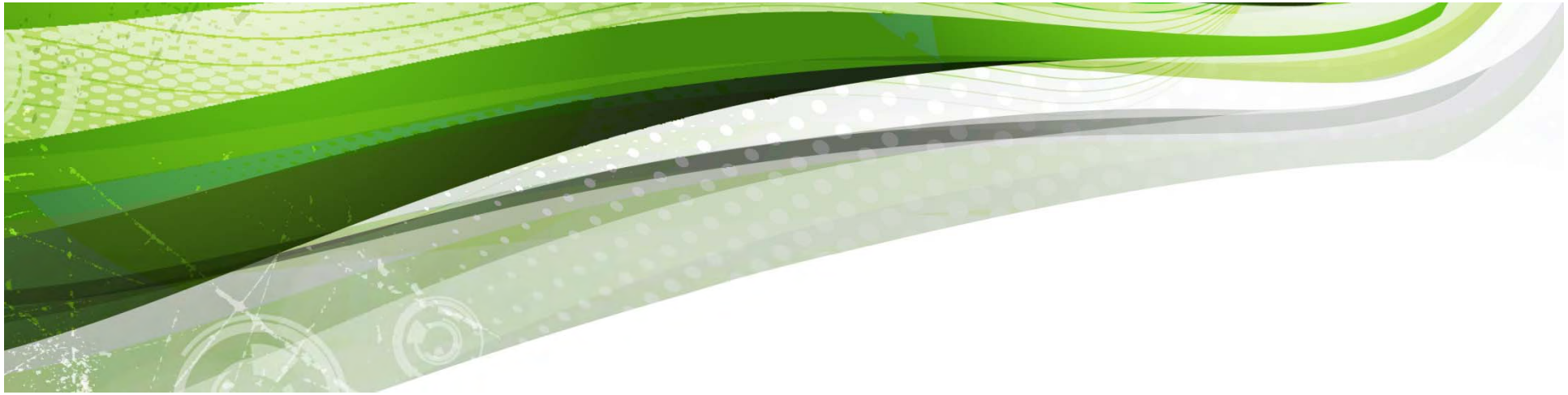
OSGP - Open Smart Grid Protocol

Inter-operability
Security issues (quick scan)
Conformance Testing

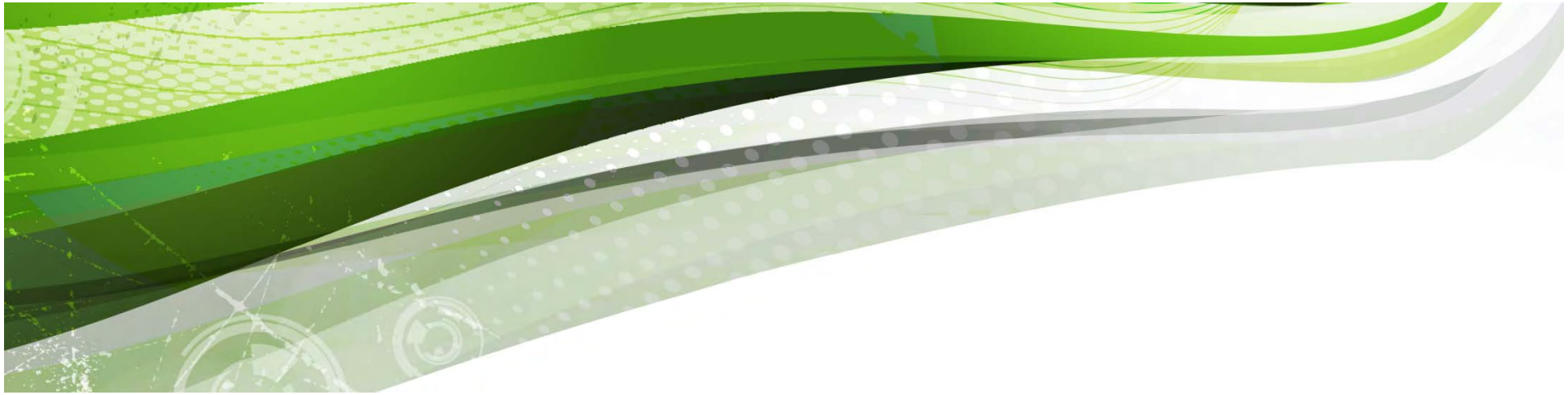


Agenda

13:00	Registration
13:15	Welcome and introduction to OSGP
13:30	The Open Smart Grid Protocol (OSGP) and its environment; Smart Metering and beyond; the future is about Smart Grids; Vision behind OSGP
13:45	OSGP support and development; The Energy Service Network Association (ESNA); Sharing the knowledge and experience; what it will bring you
14:00	OSGP main concepts, part I; The operational and functional overview of OSGP
15:00	Coffee / Tea break
15:30	OSGP main concepts, part II; Interoperability with other Standards and Protocols; MEP, M-bus, OSGP-DLMS/COSEM functionality (including demonstration)
16:15	OSGP Information Security and Data Protection (Quick Scan)
16:30	OSGP conformance testing and inter-operability testing
17:00	Questions and Answers
17:30	End of Program

OSGP
Open Smart Grid Protocol

Inter-operability at different levels

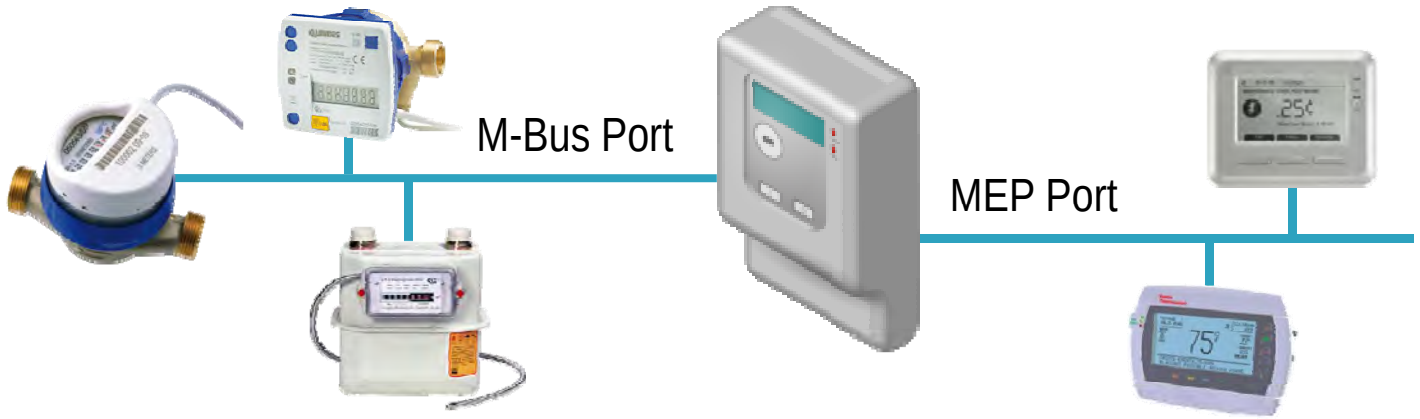


Inter-operability at different levels

- Where systems meet – “The interfaces”
- Head-end of Utility
- Data-concentrator (regional)
- OSGP devices including OSGP Smart Meters (local)

Overview M-Bus and MEP

- OSGP devices can contain optional communication ports, such as:
  - M-Bus Port :
    - Allows connection of up to four M-Bus devices such as gas, water or heat meters
    - OSGP device stores consumption data collected from M-Bus devices along with any alarm or status messages
    - Data and messages are sent to utility central service center through network
  - MEP - Multipurpose Expansion Port:
    - Serial communication port to provide access to the meter's data
    - Bi-directional port at the meter board level
    - Third parties can develop external MEP devices that interface to the meter



OSGP
Open Smart Grid Protocol

M-Bus Port

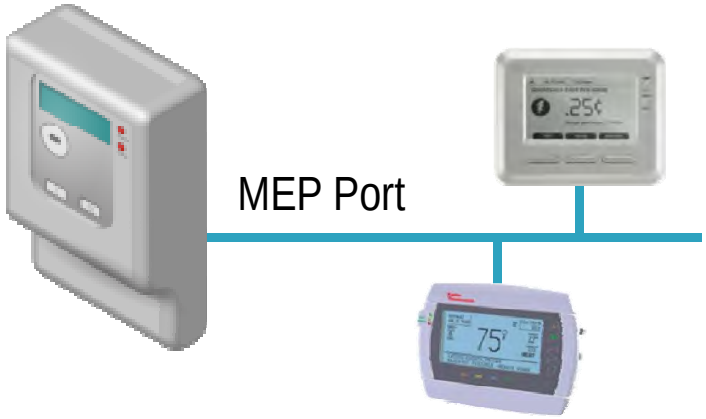
- OSGP device performs functionality of M-Bus, according EN 13757-2 and -3
- Billing data collected during scheduled polling (configurable interval) of M-Bus devices or by on-demand read request
  - Scheduled read can be set to repeat daily, weekly, monthly or yearly
  - Stored as received from M-Bus device
  - Store up to a configurable number of data sets, being previous scheduled read data for all M-Bus devices combined

- OSGP can recognize M-Bus alarms and status messages, such as:
  - type of counter,
  - power level,
  - permanent and temporary errors

OSGP
Open Smart Grid Protocol

MEP - Multipurpose Expansion Port

- MEP provides a secure entry point to OSGP through meter for
  - **Access to real-time and historical data** collected by meter
  - **Control and monitoring of in-home devices** from utility server
  - Extension of OSGP technology to **legacy devices**
- MEP devices typically outside meter but may be internal, powered by meter
- OSGP treats MEP interface as single device with **MEP device as Master**
- Expansion and control of MEP network beyond OSGP managed by MEP device
  Considerations for controlling a network beyond meter include:
  - Binding wireless devices to meter
  - Managing dispatch of OSGP requests to appropriate end device
  - Buffering requests and data for end devices that are not always on



OSGP to MEP Device Communication

- Implemented via **two different mechanisms**, depending on the urgency and need for acknowledgment of the data transfer
- Non-Urgent Data
  - MEP device checks for new data every time it communicates with OSGP device and **at periodic interval**. Data is not managed or cleared by OSGP
  - Non-urgent data transfers to MEP device
- Urgent (On-Demand) Data
  - Data transfer that is to occur **as soon as possible**, usually with expectation of acknowledgment of success or failure of transfer
  - Downlink data transfers and **on-demand write requests to MEP device**

Example MEP Applications

- Bi-directional communication with In-Home-Display (IHD)
  - Format and send data from meter
  - Forward pricing signals, energy alerts and messages
  - Retrieve customer overrides and send to meter

- Control Communicating Programmable Thermostat (CPT)
  - Change temperature set point based on tariff
  - Load profile home temperature and set point
  - Change set point on-demand
  - Forward pricing signals, energy alerts and messages to status lines
  - Retrieve customer overrides and send to meter

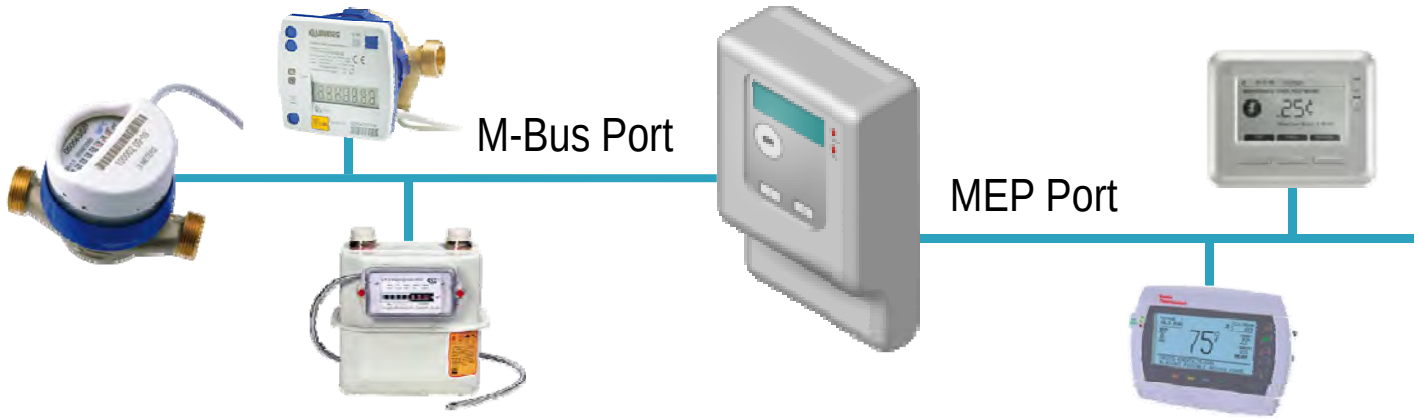
- Connect existing non-communicating meter (gas, water, etc.) to OSGP

OSGP Smart Meters are MEP Enabled for all kind of Applications - Future-proof, Secure and Inter-operable

OSGP
Open Smart Grid Protocol

M-Bus or MEP?

- M-Bus recommended for reading gas, water and heat meters:
  - When Water meters conform to M-Bus standard
  - OSGP Meter is master and can read M-Bus devices as scheduled
  - Proven solution requiring no additional software or hardware development
- MEP is recommended where flexibility is required:
  - Meter connected to a RF card that talks to in-home displays
  - Where meter protocols are not standardized

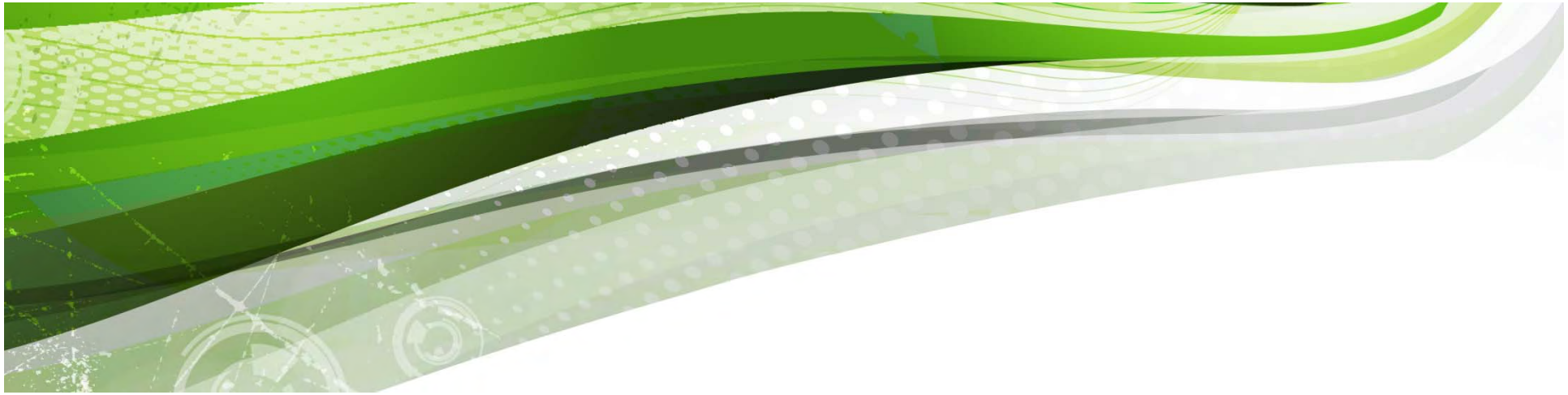


OSGP-DLMS/COSEM Interoperability

- Presentation by GuruX

Security “Risks and Measures”

Access Control
Authentication
Encryption



Overview

- The head-end security features
- Security keys and key management
- Protocols over Secured Interfaces
- Secure firmware updates
- Business Processes implementing the Security Policy
- Conclusion

Utility Networks Must Be Secure

- Every operation requires some level of security
  - There should be no unsecured interfaces or access to the system

- Secrecy is *NOT* Security
  - “Secrets” are not secure over time
  - Multi-year deployments, multi-utility deployments
  - Many people involved — trust no one
  - Information and software is easily shared on the Internet

- Security must protect Privacy as well as Access

Security is End-to-end and Comprehensive

- Everything is secured
  - No manufacturing “back doors” around security
  - Devices are always in a secured state
  - All interaction with devices is secured
- Security begins in the factory
- Security is multi-layer
- Keys are random
  - For example, knowing the unique key of one meter gives you no information for finding the unique key for another meter
- Unique keys NEVER have to be distributed to field employees

Multi-layer Security

- Devices are always in a secure state
  - Utility-unique security and device-unique security
- Utility-unique security - the state after manufacture
  - Secured with a unique utility-specific key
    - Common to all the utility's meters; different from all other utilities
  - Limited access to device functions (for example, no firmware download allowed)
  - Used to access devices the first time for provisioning
  - Once disabled, devices cannot be modified using this key; instead the unique key must be known and used to access the device
  - Typically, if devices are shipped pre-provisioned, they will be set to leave the factory with device-unique security enabled

Multi-layer Security

- Device unique security - the state after provisioning
- Unique keys are randomly generated at manufacture time
- Knowing the unique key of one device gives you no information for determining the unique key of another device
- The system installation process is designed such that these keys NEVER have to be exposed to human beings
  - They can be transferred between software and never exposed to human being
  - They can remain encrypted and safe in the utility's IT systems

Security – Protocols

- All transfers within OSGP are encrypted and authenticated
  - Encrypted with high speed stream cipher
  - 8 byte digest appended to each message to authenticate sender
  - Details in OSGP specification
- Every request and response is signed with a digest to verify its source
- Authentication keys are updated using increments; they are NEVER sent in the clear

Recommended Key Protection Mechanisms

Security Begins in the Factory

- At manufacture time:
  - Keys and passwords generated by manufacturing test machines
  - Stored in an encrypted database
  - Factory employees do not have access to database
- At shipment time:
  - Manufacturing software creates an encrypted file containing the serial numbers of the devices along with the unique security keys and passwords
  - The decryption key for file is unique and is passed to the utility separately from the file itself

Motor behind OSGP

OSGP Conformance Testing (DNV KEMA) and Certification (ESNA)

OSGP
Open Smart Grid Protocol

ESNA

Motor behind OSGP

Questions and Answers

OSGP

Open Smart Grid Protocol