Advanced Security and Privacy Enhancing Technologies for the Smart Grid

Smart Energy Middle East
Dubai

October, 2011
Our future-ready technologies and metering intelligence enable utilities to cost-effectively manage and conserve gas, water and electricity worldwide.

Working hand in hand with our customers, Elster engineers innovative solutions that advance the vital connection between technology and communities.”
Elster Group
Snapshot of company
Global Leadership

Global leadership positions across all Smart Grid segments and end-markets (residential, C&I and T&D)

- GAS: #1 global market share
- WATER: #1 global market share (JOINT)
- ELECTRICITY: #3 global market share
- NORTH AMERICAN AMI: #2 in cumulative shipments (JOINT)
Proven, Trusted Smart Grid Solutions

GLOBAL REACH
Operations in 38 countries, customers in >100 countries

2010 REVENUES: $1.8 B

170+ YEARS DELIVERING TRUSTED SOLUTIONS

200+ MILLION METERS DEPLOYED IN PAST 10 YEARS
Leading Utilities Choose Elster

Europe
Leading Utilities Choose Elster

North America
Leading Utilities Choose Elster

Rest of the World
Comprehensive Solutions Portfolio

Selected Elster Offerings

- Distribution automation, demand response, renewable integration

- EISERVER and partners

- EA-MS, EvoNet Manager, [ALPHACENTER], Meridian

- IP, Wired & Wireless telephony, Fiber, Broad Band Power Line Carrier (BPL), Satellite

- EA Gatekeeper, GateWay, RTU, MUC (Multi Utility Communicator)

- IP, EA RF Mesh, Evolution™, Power Line Carrier, Ethernet, RS 232/485

- Gas: Diaphragm, Ultrasonic, Rotary, etc.
- Water: Single/Multi Jet, Volumetric, Solid State
- Electricity: Single and Polyphase Electronic Meters Service disconnects / shut-off switches

- IP, EA RF Mesh, ZigBee, Blueline, Evolution™, MBus, Controllable Displays, Controllable Thermostats, Load Control Devices
Data security in smart grid - why design for security is an absolute must
The Smart Grid

Smart Grid
A vision for the future - a network of integrated microgrids that can monitor and heal itself.

Smart appliances
Can shut off in response to frequency fluctuations.

Demand management
Use can be shifted to off-peak times to save money.

Smart Grid: Critical Infrastructure
Why is Data Security important for Smart Metering?

- Meters are essential for billing and will create the “right” attention

- With the right incentives systems are hacked/attacked. Examples:
  - Entertainment Systems
  - Payment Systems

- Some key challenges for meter security:
  - Firmware Updates
  - Remote Disconnect
  - Billing process /Tariff Changes
  - Availability
  - ...
Smart Grid Security... a look at the news

Symantec: We finally understand Stuxnet

Security firm Symantec says it has discovered that the Stuxnet worm targeted specific motors used, for instance, in uranium enrichment processes. With the support of a Dutch Profibus expert, Symantec says, in a blog posting, that it has now managed to fully interpret the purpose of the Stuxnet code. Apparently, Stuxnet is designed to manipulate frequency converters which determine motor speed.

The Security Vulnerabilities of Smart Grid

Chinese Hackers Target Oil Companies

Internet security group McAfee Inc. has revealed that a group of hackers has carried out multiple attacks against oil companies since 2009. The hacking operation, dubbed "Night Dragon," aimed to steal information on operations and financing.

Minister' Integral Energy virus outbreak a threat to power grid

For MOSES

1, November 2009

7 September 2010 Last updated at 00:01

Scam fear over prepayment electricity credit

Criminals have managed to clone prepayment meter keys in order to make money by offering discounted credit to thousands of customers.

An estimated 85,000 households have been approached by doorstep salesmen since the start of the summer, according to industry body Energy UK.
Smart Grid Data Security

Home & Last Mile

Wide Area Link

Communications Infrastructures
- Wide Area Network (WAN)
  - Cellular
  - Fixed Line
  - PLC
  - Wi-Max
  - Satellite
  - LTE

Services

Meter Data Mgmt. and data storage services
- Storage
- CoS
- Mode Control

Power Backbone

Central Operations
- e.g. power plants, energy storage

Network Operators
- e.g. Asset & Outage Management

Distributed Generation

Third Parties
- e.g. Energy Efficiency, Health Care, Security, Safety, Market Control

Information/Data
- e.g. Meter reads, system monitoring, customer & contract data, alerting

= Interface Risk
EU Task Force Expert Group 2

Introduction

It was necessary for the European Commission to create a separate Expert Group covering Data Privacy and Data Security issues of the Smart Grid:

"The key deliverable is to identify the appropriate regulatory scenario and recommendations for data handling, safety and consumer protection"
EG2 – Data Security Recommendations

• Smart Grid products and solutions should be designed incorporating data privacy and security principles at their core

• Security levels need to be defined from minimum to advanced and the costs for the different security levels to be estimated

• A specification should not preclude the initial adoption of symmetric key followed by a further smooth migration to asymmetric key cryptography

• Conduct study on how to handle multi-national key management
EG2 – Results and further work

• Deliverable of the 2010 work: Expert Group issued a report\(^1\) end of 2010 on Data Privacy and Data Security (P&S) summarizing findings

• Input given to form a new European standardization mandate M490
  - CEN/CENELEC, ETSI will work on standards for Smart Grids incorporating privacy and security at core, holistic and end-to-end
  - Standard for the assessment of risks within the Smart Grid
  - Mechanism for trust provisioning in the Smart Grid that is contemporary with modern security techniques
  - Suitable standards to support all relevant legal requirements

• Essential regulatory requirements and recommendations
  - research on current regulation and data handling questions
  - How can the privacy and data protection issues be covered by or fit into the existing EU privacy and data protection framework?
  - Draft report available\(^2\) – issued mid 2011

Comparison of Crypto-Systems in Smart Metering

**Symmetric Encryption**
- ✔ Easy to integrate
- ✗ Keys to be pre-shared
- ✗ Scales rather poorly
- ✔ Fast computation

**Asymmetric Encryption**
- ✗ Requires special infrastructure
- ✔ No shared secret needed
- ✔ Excellent scalability
- ✗ Comparatively complex

**Solution**
Initiate encryption with asymmetric cipher, generate random symmetric and continue with symmetric cipher
Possible Security Architecture

- Holistic and End-to-End security concept protecting the complete Smart Metering Infrastructure

<table>
<thead>
<tr>
<th>Secure Firmware Management Process</th>
<th>Trust Provisioning at Factory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Layer Security</td>
<td>Signed Data and Signed Commands</td>
</tr>
</tbody>
</table>
Asymmetric Security is feasible | Elster proves

- Elster has proven asymmetric security works
- On constrained devices (e.g. battery powered residential gas meters)

- Technologies:
  - Certificate based security concept
  - ECC 256 bit asymmetric encryption
  - AES 128 bit symmetric encryption
  - SHA-256 hash algorithm
  - ECDH key exchange
  - ECDSA digital signatures
  - Module/meter authentication
Privacy Enhancing Technologies for the Smart Grid – why privacy is coming
Meter Data as Personal Data

Source: Elias Leake Quinn, Smart Metering & Privacy: Existing Law and Competing Policies, Spring 2009
Granularity of data compared

6h profile / 1 sec reading  6h profile / 15 min reading

Level of detail (almost) identical

Source: Klaus J. Müller, Gewinnung von Verhaltensprofilen am intelligenten Stromzähler, DuD 6/2010
Benefits of Privacy Enhancing Technologies (PETs)

- PETs ensure processing of personal data is minimized while business models are not affected.
- PETs reduce amount of personal data needed and hence lowering the operational costs and liabilities for data protection.
- PETs are a key enabler for Smart Metering rollouts by addressing the unsolved privacy challenge with technology.
PET – Elster Proof of Concept
Privacy Preserving Loss Detection

Privacy preserving data aggregation: individual values cannot be revealed

Individual values encrypted in privacy preserving manner

Secure connection
Privacy protected connection
Privacy Enhancing Protocol

### Traditional Reading

<table>
<thead>
<tr>
<th>Meter</th>
<th>Encrypted</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meter 1</td>
<td>0xA4BFDF..</td>
<td>615</td>
</tr>
<tr>
<td>Meter 2</td>
<td>0x1D8F3B..</td>
<td>231</td>
</tr>
<tr>
<td>Meter 3</td>
<td>0x335505..</td>
<td>968</td>
</tr>
</tbody>
</table>

**Sum of Reading**: 1814

<table>
<thead>
<tr>
<th>Meter T</th>
<th>0x4DDA56..</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1816</td>
</tr>
</tbody>
</table>

### Privacy Enhancing Reading

<table>
<thead>
<tr>
<th>Meter</th>
<th>Encrypted</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meter 1</td>
<td>7B50EF0E</td>
<td>?</td>
</tr>
<tr>
<td>Meter 2</td>
<td>F25F1B8</td>
<td>?</td>
</tr>
<tr>
<td>Meter 3</td>
<td>02C2650</td>
<td>?</td>
</tr>
</tbody>
</table>

**Sum of Reading**: 1814

**Delta**: 2

### Gas Reading

<table>
<thead>
<tr>
<th>Meter</th>
<th>Encrypted</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meter 1</td>
<td>0xAE634B..</td>
<td>344</td>
</tr>
<tr>
<td>Meter 2</td>
<td>0xFFB51F..</td>
<td>933</td>
</tr>
</tbody>
</table>

**Sum of Reading**: 1277

<table>
<thead>
<tr>
<th>Meter</th>
<th>Encrypted</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meter 1</td>
<td>7B50EDFF</td>
<td>?</td>
</tr>
<tr>
<td>Meter 2</td>
<td>F252F476</td>
<td>?</td>
</tr>
</tbody>
</table>

**Sum of Reading**: 1277
PET Use Cases for Smart Grids

• Loss and Fraud Detection
• Micro Generation and Storage
• In-Home Appliances
• E-Mobility
• Integration to Gas and Water Infrastructures
• ... and more to come!
Summary

Privacy Enhancing Technologies (PETs)

- PETs ensure processing of personal data is minimized while business models are not affected

- PETs reduce amount of personal data needed and hence lowering the operational costs and liabilities for data protection

- PETs are a key enabler for Smart Metering rollouts by addressing the unsolved privacy challenge with technology

See the Elster Whitepaper on Privacy Enhancing Technologies for Smart Grids
Conclusion
Smart Grid Data Security and Privacy becoming reality

- Technical means that provide the required level of Data Security and Privacy have been identified
  - No “new” technologies: systems exist and are used widely in other industries (e.g. telecommunication)
- However, most of today’s Smart Metering systems do not offer the full set of needed functionalities
- Especially manufactures need to pick up the challenge in order to enable the transition to new technologies
- Pilots need to be conducted to obtain reliable field experience data

Security and privacy enhancing technologies exist. They need to be implemented!
Thank you

Ali Mouslmani / Kim Arlund Nørgaard
Regional Director MENA / VP Sales and Marketing
ali.mouslmani@ae.elster.com / kim.norgaard@elster.com