Privacy and Security in Smart Grids

Recommendations to the European Commission
Task Force Smart Grids - Expert Group 2

Brussels, 15th of June 2011
Bram Reinders.

Regulatory Requirements for Data Handling and Data Protection

The key deliverable is to identify essential regulatory requirements and recommendations for data handling and consumer protection by:

- **Research on current regulation and implementation**
- **Research on data handling questions**

Data transfer creates challenges for privacy and security

Is privacy of European citizens protected?

- Smart meters measure energy consumption in real time and on personal level (electricity, gas, water, heat)
- Thus creating a fingerprint of what is going on behind a specific front door
- Showing patterns over longer time

Is the information flow going through the grid sufficiently secured?

Are Smart Grids secure enough to guarantee uninterrupted electricity supply?

Status Update

Report issued with request for comments - April 2nd

- Research on right to privacy and right to protection of personal data
- Research on national implementations privacy and data protection through questionnaire Article 29 Data Protection Working Party

Public hearing conducted - May 6th

- Formal and fair commenting process for all organizations
- All comments have been reviewed and published, with the taken decisions - May 28th

Latest report issued (version 0.96) - June 6th

- Decisions reviewed during last EG2 meeting - June 8th

EC should set privacy and security standards to enable development of Smart Grids

1. Use existing legal framework for securing privacy and protect personal data
2. Enhance privacy and protect personal data
3. Encourage Smart Grids are secure by design

Use existing legal framework for securing privacy and protect personal data

- Most data from Smart Meters can be considered personal data (Opinion 183 of the Article 29 Data Protection Working Party)
- Utilize and implement decision 768/2008/EC (CE marking) for all present and future components of Smart Grid and comply to Smart Grid Information Security essential requirements
- Include requirements for the logical infrastructure of Smart Grid Components in the MID
- Have standards developed and maintained by standardization organizations (M/490)
- Have Member States enforce use of common standards
- Provide evidence to assess whether smart metering's inference with privacy is permissible (notions DPA's differ widely).

EC should set privacy and security standards to enable development of Smart Grids

1. Use existing legal framework for securing privacy and protect personal data
2. Enhance privacy and protect personal data
3. Encourage Smart Grids are secure by design

Enhance privacy and protect personal data

- Incorporate Privacy by Design and by Default in Smart Grid Development.
- Adapt a standard approach for Privacy Impact Assessment
- Constrict data retention to a minimum
- Encourage use of privacy certification schemes
- Enable Data Protection Authorities to apply a consistent set of responsibilities, definitions and principles (economic operators are responsible for compliance).

EC should set privacy and security standards to enable development of Smart Grids

1. Use existing legal framework for securing privacy and protect personal data
2. Enhance privacy and protect personal data
3. Encourage Smart Grids are secure by design

Encourage Smart Grids are secure by design

- Create awareness in Industry's top level
- Keep impact of ICT problem on energy delivery as low as possible
- Create trusted public/private network to further enhance security, with focused work package

Next steps

Process to track the execution and realization of EG2 recommendations needs to be established

- Identify which recommendations result in deliverables to be included in the work programme
  - M/490
  - Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids

- How will this be done for regulatory recommendations?

Are there future tasks for EG2 to pick up?

BACKUP 1: EG2 Key findings

General

Privacy

Security

MID

Key findings – General

- **EG2.G.1** The European Smart Grid regulation should utilize and implement decision 768/2008/EC as it will need to be harmonized to products already harmonized under NLF

- **EG2.G.2** Standards need to be developed by standardisation organisations based on a common set of use-cases taking into account the different business models across the Member States.

- **EG2.G.3** Enforcement is a key aspect of regulation. Guidelines need to be developed on monitoring and enforcement. It is recommended to address the Member States to review their regulatory frameworks.

Key findings – Privacy

- **EG2.P.1** It is recommended to confirm that in accordance with opinion 183 of the Article 29 Data Protection Working Party most data from Smart Metering can be considered personal data.

- **EG2.P.2** It is recommended that adequate measures are deployed to protect the contents and nature of this data in order to safeguard the privacy of the consumer.

- **EG2.P.3** Privacy by Design and by Default should be strongly encouraged and can be incorporated in the methodologies of parties involved in Smart Grid development when personal data are involved.

Key findings – Privacy #2

- **EG2.P.4** Performing (a form of) Privacy Impact Assessments on Smart Grid developments should be encouraged. In order to effectively perform these analyses a standard approach could be adapted to the Smart Grid infrastructure.

- **EG2.P.5** Given the variety of data storage purposes within smart metering, a single data retention period cannot be concluded.

- **EG2.P.6** EG2 recommends to perform an analysis in order to determine to which extent utilities need to retain personal data (i.e. neither non-aggregated nor anonymised) to be able to maintain the electrical grid and perform billing.

Key findings – Privacy #3

- **EG2.P.7** The following principles should apply for the purpose of data retention: (a) data minimisation (i) data collection and (ii) data retention shall in any case not exceed absolute minimum; (b) transparency; (c) empowerment of the consumer

- **EG2.P.8** The use of privacy certification schemes should be encouraged. It should be left to regulatory bodies to determine which certification scheme and structure should be used.

- **EG2.P.9** To protect consumer rights and enable effective use of Smart Grids DPAs need to be involved in the process.

Key findings – Privacy #4

- **EG2P10** Non-compliance with privacy limitation criteria might have an adverse effect on smart grids deployment in a given electricity market. Both enactment of a regulatory framework and a practice that respect these limitation criteria will minimise such a risk.

- **EG2.P.11** Commission provides evidence that allows to assess whether smart metering's interference with privacy is permissible. In addition, it is recommended that specific measures are taken to ensure the adequate protection of personal data in smart metering.

Key findings – Security

- **EG2.S.1** Creation of a trusted network of public and private organisations, where information about incidents, threats, vulnerabilities and good practices will be shared intensively.

- **EG2.S.2** The impact of ICT problems on energy delivery should be kept as low as possible. This would mean that failures within parts of the infrastructure must not lead to blackouts, etc…

- **EG2.S.3** The European Commission should play an important role in creating awareness of the importance of security while implementing smart grids.

Key findings – Security #2

- **EG2.S.4** It is recommended that the European Commission coordinates the foundation of national certification authorities for smart grids prior to a rollout of devices.

- **EG2.S.5** Within a trusted network the European Commission can promote and facilitate: the development of security guidelines for Smart Grids, the certification of products and services test facilities; Research & Development

- **EG2.S.6** The level of experience and awareness can be increased within a trusted network of public and private organisations by providing (online) training and information facilities.

Key findings – MID

- **EG2.M.1** Include requirements for information security and data protection in Smart Grid measuring devices in the MID

- **EG2.M.2** Guidelines should focus on requirements for the logical infrastructure. Especially the standardization of interfaces, the implementation of security by design and data privacy principles in MID relevant devices.

- **EG2.M.3** It is recommended to further develop the ESMR/ESGR[1] in order to set up essential requirements (should be worded precisely enough to create legally binding obligations) and a technical standard for Smart Metering / Grid

[1] ESMR = European Smart Meter Requirements; ESGR = European Smart Grid Requirements

BACKUP 2: EG2 Concepts

Privacy by Design and by Default
Privacy Impact Assessment (PIA)
Constrict data retention to a minimum

Involve Data Protection Authorities

Encourage use of privacy certification schemes

Create Awareness on Industry's top level

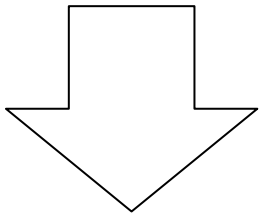
Keep impact of ICT problem on energy delivery as low as possible

Create trusted public/private network to further enhance security…

Incorporate Privacy by Design and by Default in Smart Grid Development

Make Privacy a core functionality of:

- IT Systems
- Accountable business practices
- Physical design and network infrastructure



- Enables consumers to control the use of their personal data
- Improves transparency about the processing for the consumer

Adapt a standard approach for Privacy Impact Assessment (PIA)

A PIA prevents redesign and adaptation of systems, services or processes. Key steps are:

1. Describe service or application
2. Identify how privacy could be harmed
3. Assess probability and impact of these risks
4. List technical/organisational controls
5. Document the resolutions

Endorse and control content by central and independent authority

Constrict data retention to a minimum

Purpose	Scope	Length	Kept by
Network maintenance	Personal Anonymised Aggregated	Strictly necessary national law	Utility
Billing and payments	Summed up usage	13 months	Utility and Energy market supplier
Billing complaints	Detailed personal data	National law	Consumer
Tax records	Summed up usage		Utility
Tax breaks	Detailed personal data		Consumer
Value Added Services	Upon consent	Upon consent	Any interested
Policy making	Anonymised Aggregated	unlimited	Public authorities

Involve Data Protection Authorities in legistative process of Smart Metering

- Involve DPA's in 11 states that have not yet implemented EC2006/32 into legislation
- Perform PIA's on existing and planned infrastructure achitectures
- Provide DPA's with a consistent set of responsibilities, definitions and principles

Encourage use of privacy certification schemes

- Transparency and trust to customers
- Legal security for the responsible actors

- Regulatory bodies should determine which certification scheme and structure should be used

Create Awareness on Industry's top level

- The European Commission takes the lead
- Addresses CEO level of Electricity and Telecommunications Industry
- Organizes Top Conference with all strategic players

Assignment

Develop a joint public-private roadmap to secure smart grids

Keep impact of ICT problem on energy delivery as low as possible

- Systems can black start on all levels
- All functionalities are robust and resilient
- Less-than-critical processes do not endanger more critical ones
- Processes can handle disruptions
- Failures within parts of infrastructure do not lead to blackouts

Create trusted public/private network to further enhance security…

- Share information about incidents, threats, vulnerabilities and good practices
- Enable participants to make accurate risk assessments
- Make use of existing organisations:
  - ENISA
  - EuroSCSIE

… with focused work package:

- Develop security guidelines for Smart Grids
- Certificate products and services
- Develop test facilities for new architecture and its components
- Enable Research & Development for security and privacy
- Develop (online)-training to raise the level of experience.