



SEESGEN-ICT

4° GENERAL WORKSHOP

Paris - SAP Office, April 14th – 15th 2011

Evangelos Rikos (CRES):
Privacy and Security Issues





Basic concept

- Effort to move from the antiquated electricity system to a 'Smarter' grid
- Deployment of technologies and techniques (e.g. smart meters)
- Benefits:
 - Active role of each player in the system
 - More efficient operation
- Challenges:
 - Privacy and Cyber Security



Similarities and differences between Privacy and Cyber Security

- Privacy: correlated mainly to the access of third parties of the grid to customers' or other stakeholders' data
- Access could be authorized but pose privacy issues (e.g. information about habitual behaviour of consumers)
- Cyber security: mainly related to unauthorized access from intruders to the system through access from ICT infrastructures
- Anonymously and remotely
- Privacy violation, access and control gain to electricity infrastructures



EU Initiatives regarding Privacy and SmartGrids

- Different perspective between EU and the US
- In EU the privacy is considered of major importance while the US there is more emphasis on Cyber Security since there is a belief that there cannot exist also Privacy if there is no Cyber Security in the system.
- EU initiatives:
 - Establishment of an Experts' Committee (Expert Group 2) in the frame of "SmartGrid Task Force" dealing with the issue of Privacy and Data Security
- Non EU initiatives:
 - National Institute of Standards and Technology (Cyber Security Working Group-NISTIR 7268: Guidelines for SmartGrid Cyber Security)



Privacy and Data Security

- The Privacy issue arises from the need for close cooperation between different players and especially between customers and electricity companies
- Data exchange for several technical and market purposes
- Major challenges are posed especially from smart meters because they could reveal the behaviour and habits of the customer
- On the other hand for the efficient system operation requires the use of a minimum data quantity



EG2 focus and efforts

- Appropriate regulatory framework
- Experiences from other industries
- What data are necessary for the system operation and if these data are private or not and how to protect them?
- There is a gap in European standards concerning the handling and security of data in smart grids
- There are broader standards, guidelines and codes of practice in place within other industries



Data types

■ Personal data

- “information relating to an identified or identifiable natural person ('data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”¹

■ Technical data

- information gathered from metering, distribution, or transmission assets in order to assess the performance of the energy network, network problems, or potential future problems, security breaches and energy theft

¹Directive 95/46/EC European Union Directive on Data Protection



Comparison between data types

- Data could be considered as personal or technical in regards to the scope of use
- The technical data collection would be based on aggregated and anonymous data
- Consumer data is gathered from individual metering points and should be considered as Personal



Existing Regulatory Framework

- Comprises collection of rules and regulations and based on that, each country has the possibility to implement directives in national level
- From the existing framework a common approach for smart grids should be defined

Recommendation: How the data privacy issues are covered by the existing framework. If the latter is insufficient, the proposal of a new more detailed framework is necessary



Experiences from other industries

- Electronic banking
- Telecommunication
- Automated fare collection
- Road pricing



Related standards

- Physical interfaces (between devices)
- Data interfaces (data is moved from one legal entity to another)
- EC 62351 security mechanisms to the IEC suite of protocols developed within IEC TC57
- ISO/IEC joint standards in the 27000 series, provides best practice recommendations on information security management
- CENELEC are tasked under the Smart Metering Coordination Group (and Mandate 441) to identify, produce and maintain standards for electricity meters, communication protocols, home automation equipment, Electric Vehicles and other electrotechnical applications



Related standards (cond.)

- CEN is recognized by the Smart Metering Coordination group to identify, produce and maintain standards in the area of gas, water and heat meters, communications protocols for battery powered meters, and other non-electrotechnical applications
- ETSI are recognized by the Smart Metering Coordination Group for the delivery of standards in the area of telecommunications, as part of the ongoing work to fulfil the requirements of M441
- NERC (North American Electric Reliability Council) is a self-regulatory, nongovernmental organization which has responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical and efficient practices.



Summary of recommendations-Possible technical solutions

- Data aggregation
- Clear and concrete legislation framework
- Design of ICT infrastructure from its core so as not to violate privacy
- Use of Virtual Private Networks and other techniques (e.g. Power Line Communication) for increased security
- Customer's awareness when their data are monitored



References

1. *“EXPERT GROUP 2: REGULATORY RECOMMENDATIONS FOR DATA SAFETY, DATA HANDLING AND DATA PROTECTION”*, Draft REPORT, Delivered at the 5th Steering Committee meeting JUNE 22, 2010. (source: http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm)
2. Patrick McDaniel, Sean W. Smith, “Security and Privacy Challenges in the Smart Grid” Co-published by the IEEE Computer and Reliability Societies, MAY /JUNE 2009, pp. 72-74