Brussels, 27th of June, 2012

ENISA SMART GRID SECURITY CERTIFICATION

Konstantinos Moulinos
Project manager
ENISA

Background

- ENISA Study on SG security, 2012
  - 10 Recommendations
  - "*Both the EC and the MS competent authorities should promote the development of security certification schemes for components, products and organisational security.*"

Aim and Objectives of the workshop

- Follow up the recommendation of the study
- Support the MS in better understanding the challenges of the security certification process
- Contribute in the harmonization of different certification policies
- Invite MS to present their national certification schemes and private sector to present their views on the matter
- Debate about the possible steps to take, at national and EU level, to speed up the secure introduction of Smart Grids

Scope of the workshop

- Not only smart meters
- Focus on the whole from production to consumption
- Not a technical workshop
- Stakeholders from all different categories have been invited
- Focus on different kinds of certification (security practices, process, h/w, s/w)

Agenda

09:30 – 09:35	Welcome and agenda of the day	**Konstantinos Moulinos, ENISA**
09:35 – 09:45	State of Play	**Alejandro Pinto-Gonzalez, EC DG-CONNECT**
09:45 – 10:05	The German Certification Scheme Introduction to SOGIS - MRA	**Bernd Kowalski, BSI**
10:05 – 10:15	The Norwegian Certification Scheme	**Kjell Bergan, NSM/SERTIT**
10:15 – 10:25	The Swedish Certification Scheme	**Martin Bergling, FMV**
10:25-10:45	Which parts of the value chain to be certified?	**Marcello Manca Vice President Gov. & Ind. Affairs, Europe Undewritters Laboratories Inc, USA**
10:45 – 11:15	Coffee Break	
11:15-12:30	Discussion 1. different national approaches to certification 2. basic steps needed to develop a certification scheme 3. relationship of certification to testing and test-beds? 4. different players and cooperation among them	
12:30 – 13:30	Lunch	
13:30 – 14:00	Standards and Certification for Smart Grids	**Annabelle Lee Technical Executive - Cyber Security, Electric Power Research Inst. , USA**
14:00 – 15:15	Conclusions – Panel for discussion 1. Is there a need for new standards? a. if no, How can we use the existing ones? b. if yes, Who should that? 2. How different players will get involved? 3. How to avoid reinventing the wheel?	**Panel Annabelle Lee, EPRI Markus Braendle, ABB Richard Link, Siemens Martin Klimke, Infineon**
15:15 – 15:45	Coffee Break	
15:45 – 16:00	Wrap Up and Future Directions	**Konstantinos Moulinos, ENISA**

Wrap up

- Multiple different approaches
- Many problems
  - Expensive
  - Time consuming
  - Do not meet the pace of vulnerqbility changes
- Vague legal framework

Where to go

- Harmonised – unified – interoperable approach
- SG as a complex system
  - Different methods for different levels of criticality level parts
- Low cost
- Looking at the whole life-cycle
- Incentives to do more – reasonable legal framework

Need to be done

- Small steps
- Information sharing – more cooperqtion
- Security testing
- Metrics

Actions

- Create a Certification for SG WG in existing European structures
- Maintain the Security testers / certifiers/certification frameworks database updated

Thank you!