Smart grid cyber security certification

Minutes of the workshop

1 Introduction

On 30th September 2014 ENISA organised a workshop where the results of the report on 'Smart grid security certification' (to be published by end of 2014 at ENISA web site) were presented. The aim of this workshop was to share and discuss the most relevant conclusions of the report, including the proposed recommendations, with the experts that participated in the study. For this reason, an open dialog among the attendees was also planned. This dialog allowed ENISA to pulse the impression of the audience on the recommendations, to discuss on several hot topics related to smart grid security certification, and to gather the different opinions on what could be the next steps in the field.

All those experts who participated in the study were invited to the workshop, and around 50 finally attended the event. The report has been circulated amongst the participants of the workshop a few days in advance for their information. They were representatives of all the stakeholders types considered for the study: manufacturers, DSOs, TSOs, and security services providers, smart grid services providers, academia/research, public bodies, and standardisation bodies.

2 Agenda

Date, Location	**30th September 2014, Heidelberg, GERMANY**
Venue	Print Media Academy, Kurfürsten-Anlage 52-60, 69115 Heidelberg, Germany **www.print-media-academy.com**
Contact Person	Konstantinos Moulinos – resilience@enisa.europa.eu

Session: "Smart Grid Component Certification"	
13:15-13:30	Keynote Speaker The German IT security certification scheme-Bernd Kowalski, BSI
13:30 – 14:15	-Short introduction of the report: - Focus on: - the comparison criteria - the challenges of Smart Grid Component Certification identified in the Report - *Overview of the Challenges* -
14:15- 14:30	Coffee Break
14:30- 14:45	Keynote Speaker Results of a recent survey on smart meter certification, Willem Strabbing, ESMIG
14:45 - 15:30	Discussion & comments on the Recommendations presented in the ENISA report

15:30 – 15:45	*Collection of Feedback and Identification of Next Steps*
15:45 – 16:00	Plenary Discussion, Next Steps, Closing Remarks

3 Observations

3.1 Keynote Speaker: The German IT security certification scheme

Mr. Bernd Kowalski of BSI was the keynote speaker and provided insight regarding the German IT security certification scheme.

He explained that in Germany there is a growing importance regarding IT-Security Certification. The main aspects regarding the importance were;

- Economy & Society depend on availability and integrity of IT-Systems
- Lack of Privacy and Trustworthiness in mainstream products
- Public and national security affected
- Governments under pressure to set guidelines for appropriate

The German certification system is based on certification of products according to common criteria and technical guidelines conformity. Additionally, there is ISO27001 certification to certify certain IT-security processes. All labs involved in security evaluation need recognition such as ISO/IEC 17025.

The BSI offers the following certification services;

Product Certificates on the basis of Common Criteria/PP

- Smartcard hardware & software
- Digital Tachograph components
- Operating systems, firewalls, signature applications
- Biometric verification systems
- eID and electronic passport
- Smart Meter Gateway

Product Certificates acc. to Technical Guidelines

- Conformity and compatibility of IT security components

Certificates for IT-infrastructures are according to ISO 27001 on the basis of IT-Grundschutz, and the BSI-CC-Scheme has been approved under the European Accreditation System.

The presentation also provided some comments regarding the report for smart grid security certification. It was noted that privacy was not explicitly mentioned, while it is an important market driver for the smart meter in Germany. Another message taken out of this was; “The report should put emphasis on proposals on how to start European harmonisation of interoperability and then conclude to second step on security and risk assessment harmonisation” which feedback that can be taken into account regarding the focus of the report.

3.1.1 Q&A

Question: Is the German approach a good approach for all of Europe;

Answer: It is currently specific for the German market, and would need to be adapted to be successfully integrated in other Member States.

3.2 Short introduction of the smart grid cyber security certification report

Konstantinos Moulinos and Robin Massink held a joined presentation regarding the investigation into cyber security certification of smart grid. The report provided an outline on how to approach a pan European method of harmonising cyber security in the Member States.

3.2.1 The approach

The objectives of the investigation into cyber security certification of smart grid were as follows:

- Perform a desktop research regarding cyber security certification
- Qualitative analysis of cyber security certification schemes
- Identify the gaps between different certification schemes
- Produce technical advice, recommendations and good practices for certification in smart grid security.
- Provide recommendations on how to develop new or improve existing approaches to a pan European harmonised smart grid security certification.
- Discussion of approach with stakeholders
- Draft report for comments
- Addressing of comments with stakeholders
- Workshop for discussion of main topics
- Final report

In the desk research, a separation was made between certification schemes and other information. In the list of information consider were articles and investigations, security and/or smart grid standards and schemes and smart grid related security services. With further analysis to select schemes for qualitative analysis, in the end 8 out of 19 cyber security certification schemes were selected that related to the smart grid.

After the desk research a preliminary draft document was made based on the findings of the desk research and the identification of the desired situation, gaps, challenges and proposed recommendations.

The draft report has been disseminated to the stakeholders for discussion. The list of stakeholders included:

- SISEC members
- Selected members of the ENISA contact list
    - Certification authorities: ANSSI, BSI, CESG, FMV, …
    - Associations: EURELECTRIC, ESMIG, T&D Europe
    - Standardization initiatives: M/490 SG –CG/SGISWG, DKE VDE DIN
    - Private sector: Alstom, ULL, EDF R&D

In total the stakeholders came back with 123 comments, and the possibility for comments will be open until the 10th of October 2014.

In summary;

- 88 comments could be processed or revised in the document
- 18 comments needed further discussion
- 17 comments were rejected (mainly due to conflicts with other comments made)

The updated made to the documents based on the contents of the comments is summarised as follows;

Processed comments

- Updated minor details and facts
- Removed unnecessary statements
- Removed statements that distract from the main topics
- Included latest findings

Discussed comments

- More complex issues
- Unclear issues

Rejected comments

- Opinions
- Misinterpretations

It should be noted that all comments have been consolidated in a document depicting the classification and methods of addressing.

The current workshop is the next step in the validation of the report, and after the collection of all comments during the workshop and any additional comments provided and stakeholder discussions, a final version of the report will be made public.

3.2.2 The report contents

The presentation regarding the report contents was also a joined effort between Konstantinos Moulinos and Robin Massink. It provided insight in the topics the report addresses in sequence to build up to the recommendations and the proposed roadmap.

Main topics in the report

- Introduction
- Why to certify?
- What to certify: Smart grid lifecycle
- What is available: SG-AM/SG-IS usage
- How it is applied in the EU
- The desired situation: Harmonization
- Gaps and challenges
- Recommendations
- Roadmap

Before going into detail regarding the topics, it should be noted what the report aims to be, and what it does not aim to be;

It is not

- A proposal for a new certification scheme
- A recommendation for the use of any particular standard

However it is

- A proposal for creation of a steering working group/ task force
- A proposal for a certification framework (chain of trust)

- A proposal for using an existing reference model (SGAM)
- A mapping between different certification standards and the SGAM layers
- A recommendation to reuse existing mechanisms
- Roadmap to implement the framework

Then a short overview of the contents of the report including the approach to smart grid security certification together with gaps and challenges towards a harmonised certification in Europe were delivered.

After this the recommendations and roadmap was provided. But there was first a change for question and discussion about the research done and conclusions made.

3.2.3 Questions

There was a short question if we propose a European level of cyber security for all member states, and the answer was that we propose a European definition of security levels, but the level of security to adopt is depending on the national situation

Jean Piere Menella, Alstom, mentioned that the reference of the SGIS toolbox should be aligned with the framework instead. This is recognised and will be reflected in the latest version of the report.

3.2.4 Other remarks

One expert referenced to the IECEE/ CB scheme by IEC and he said that it is very similar with what we propose. It should be investigated further.

There was a general comment outside of the presentation regarding the proposed approach, and how the responsibility of the member states would fit in. The delegated responsibility is something that could be met with resistance, as they would like the European Union to provide the initial approach.

3.3 Keynote Speaker: Results of a recent survey on smart meter certification

Mr. Willem Strabbing was the keynote speaker regarding the research ESMIG had done on smart meter certification. As an introduction, the main objectives of ESMIG are;

EC Standardization mandate M/441 on Smart Metering

To improve customer awareness of actual consumption in order to allow timely adaptation to their demands

By means of:

- European standards allowing interoperability of utility meters (for electricity, gas, water and heat)
- Fully integrated solutions, modular and multi-part solutions
- Architecture must be scalable and adaptable to future communications media
- Secure data exchange

The research was mainly about recommendations regarding smart meter certification. It has been based around a qualitative analysis of Common Criteria(CC), Commercial Product Assurance(CPA) and Certification de Sécurité de Premier Niveau(CSPN).

Common Criteria: International standard (ISO/IEC 15408) for security certification. Certification requirements for products and organizations (development & manufacturing environments) are defined in Protection Profiles. Agreements for Mutual Recognition of certificates and Protection Profiles by many countries at international level.

Commercial Product Assurance: National scheme for security certification defined in the UK and maintained by CESG. Certification requirements for products are defined in Security Characteristics and for organizations (development & manufacturing environments) are defined in Build Standards.

Certification de Sécurité de Premier Niveau: National scheme for security certification defined in France and maintained by ANSSI. Certification requirements

The main conclusions from this research can be seen in the following table;

Criteria	Description / sub criteria	CC	CSPN	CPA	ISO/IEC19790
Security requirements based on threat analysis	The certification scheme demands that security requirements are defined as countermeasures to **specific threats**.	Fully covered	Fully covered	Fully covered	Not covered
Product testing	The certification scheme requires that **functional testing** takes place by and/or is reviewed by an evaluator. *During functional testing, the functions of a product are tested; this includes security function testing, test of the user guidance, testing of protection against misuse, regression testing (re-testing after product changes), etc.*	Fully covered (depth depends on EAL)	Fully covered	Fully covered	Fully covered
	The certification scheme requires evaluators to perform **vulnerability testing**. *Examples of such tests are penetration testing, reviewing the security architecture, testing vulnerabilities based on source code, etc.* Within this context "partially covered" means that only basic vulnerability testing is performed without for example penetration testing.	Fully covered (depth depends on EAL)	Partially covered	Partially covered	Not covered
Defining security measures for the premises of developers / OAM actors	The certification scheme demands that developers take **measures to secure their premises** (e.g. through access control, human resource security …)	Fully covered (depth depends on EAL)	Optional	Fully covered	Not covered
	The certification scheme required that user guidance is provided to secure the product during operation/administration/maintenance.	Fully covered	Fully covered	Fully covered	Fully covered
Use of proven methods and maintaining skills	The certification scheme demands that **configuration management** requirements are put in place. This ensures consistency of a product's	Fully covered	Optional	Fully covered	Fully Covered

Finally, ESMIG provided the following future steps they intend to take in 2014 and beyond:

- Finish report part III in October
  - Results from ENISA workshops
  - Recommendations for approaches regarding Smart Metering
- Follow standards developments (security aspects)
- Take output from Task Force Smart Grids and apply for Smart Metering
- Work with ENISA on certification approach?

3.4 Discussion & comments on the Recommendations presented in the ENISA report

The presentation of the report continued with the presentation of the recommendations that were made in the report by Konstantinos Moulinos and Robin Massink;

After the recommendations, the roadmap was presented. There a small discussion regarding the recommendations made, but the audience seemed not opposed to the general proposed methodology and recommendations. It should be noted that in the final report, the recommendations should be consolidated, as they are now too many, which caused a limited time to discuss all of them.

3.4.1 Questions

There was a comment about privacy, and the importance of it for the smart meter, but it was unclear how it directly was related to the report. Privacy will be mentioned in the next version of the report and there it will be explained why it is considered to be out of the scope of this.

4 Conclusions

Some conclusions could be drawn regarding the presented report and the discussions during the workshop. Below are the most important ones;

- The topic is deep and technical, making it difficult for a large group to have a deep discussion without understanding all the variables.
- There have been no comments regarding the proposed approach to have an EU body for guiding the process of smart grid certification.
- There have been no comments regarding the chain of trust concept.
- There is some opposition regarding the inclusion of other methodologies, it was proposed to instead align with them as opposed to directly include.
- We have to consolidate the recommendations; they are too many – some of them might be merged.
- The issue of privacy, it needs to be addressed in the report, and its position regarding the topic of smart grid certification.

The ENISA report should be updated regarding the following aspects;

- We should emphasize that the report proposes not a specific scheme, but an approach to harmonise smart grid security certification in Europe
- The Comments of BSI should be addressed as much as possible
- Privacy should be mentioned in the document
- The recommendations should be consolidated as there are too many
- The SG-IS toolbox should be updated to be aligned the framework instead
- We should investigate the IECEE/ CB scheme by IEC

5 Future steps

Participants were notified that the deadline for receiving their written comments has been extended to 10th of October. After that, comments form both the workshop and the online cosultation, will be compiled in a list and then the final report will be drafted. The approved, by ENISA internal quality review process, report is expected to be published at the ENISA web site by the end of 2014.