Joint ENISA – European Commission workshop on security certification for smart grid components

Minutes of the workshop

[Deliverable – 2012-07-19]

Contributors to this report

ENISA would like to recognise the contribution of the Deloitte team members that prepared this report in collaboration with and on behalf of ENISA

- Dan Cimpean
- Pedro Cano
- Mauricio Sanchez Gonzalez

Agreements or Acknowledgements

ENISA would like to acknowledge the contribution of the participants to the joint ENISA – European Commission workshop on security certification for smart grid components to this report.

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For questions related to "Security Certification for Smart Grid Components", please use the following details:

- E-mail: Konstantinos.Moulinos@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Contents

1 Introduction

1.1 Overview

On the 27th June 2012, ENISA and the European Commission organised a Joint Workshop on Security Certification for Smart Grid components.

The **aim of this workshop** was to:

- Support the Member States in better understanding the challenges of the Smart Grid component certification process;
- Contribute in the harmonization of different certification policies followed by the Member States;
- Invite Member States 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.

The workshop was focused on the whole smart grid value chain, by following a non-technical approach that was trying to help workshop participants to identify which elements need to be certified.

Fifty seven people participated at the workshop representing different types of stakeholders: national certification authorities, EU officials, hardware and software manufacturers, energy service providers, executives from certification laboratories from EU and US, etc.

The format and the agenda of the workshop were planned to encourage an open dialog amongst the workshop participants. This dialog allowed the participants to discuss the most relevant and "hot" topics regarding the certification on smart grid components, and allowed gathering the different opinions on what could be the next steps to be followed in this field by ENISA, by the Commission, Member States and by the key smart grid stakeholders.

All the presentations can be found at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components

The agenda of the workshop was the following:

09:00 - 09:30	Registration	
09:30 - 09:35	Welcome and agenda of the day	Konstantinos Moulinos, ENISA
09:35 - 09:45	*State of Play*	Alejandro Pinto-Gonzalez
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 Underwritters 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	
13:35 – 13:40	*The ERNCIP project*	Auke Huistra, CPNI.nl
13:40 - 14:10	*Standards and Certification for Smart Grids*	Anabelle Lee Technical Executive - Cyber Security, Electric Power Research Inst.
14:10 - 15:15	Conclusions - Panel for discussion 1. Is there a need for a new standards? 2. a. if no, How can we use the existing ones? b.if yes, Who should do that? 3. How different players will get involved? 4. How to avoid reinventing the wheel?	Panel Anabelle 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

2 Morning Session-Presentations

2.1 State of Play

Mr. Alejandro Pinto-Gonzalez, DG CONNECT Policy Officer (policy developer e-signature and Internet and security) was in charge of formally opening the workshop. He is the point of contact from the European Commission (EC) for the Expert Group on Security and Resilience of Communication Networks and Information Systems for Smart Grids, an initiative in which ENISA is also actively participating.

His presentation focused on the following topics: a) the overall policy context for the NIS/CIIP, b) the **Expert Group on Security and Resilience of Communication Networks and Information Systems for Smart Grids** and c) the key outcomes of the Expert Group.

2.2 The German Certification Scheme Introduction to SOGIS - MRA

Mr. Bernd Kowalksi, Head of Department S-Secure Electronic IDs Certification and Standardisation at the Federal Office for Information Security (BSI - Germany) presented the German Certification Scheme and he gave a short introduction of the Mutual Recognition Arrangement (SOGIS – MRA).

2.3 The Norwegian Certification Scheme

Mr. Kjell Bergan, Scheme Director at Norwegian National Security Authority/SERTIT, presented the Norwegian Certification Scheme. An overview and background information for the national certification scheme were presented. In the consequence, the agreements that the SERTIT is a member of were explained in more details. Finally, the future SERTIT plans were described: a) it will apply for becoming a Qualified Participant of the SOGIS MRA and b) it is prepared with four Evaluation Facilities (ITSEFs), which will be able to conduct evaluations of Smart Grid components.

2.4 The Swedish Certification Scheme

Mr. Martin Bergling, Technical Manager at the Swedish Certification Body for IT Security CSEC, presented the Swedish Certification Scheme and information related with the Swedish Certification Body for IT Security (CSEC). The CSEC key tasks of the were presented and its current activities as well. It is in the CSEC's plans to create protection profiles for USB memory (encrypted storage), VPN, Firewalls and Smartphones.

MB, explained that the development of protection profiles should have their initiative in their local laws. Furthermore, he stated that Sweden is interested in collaborating on the creation of a protection profile for Smart Grids. He concluded his presentation stating that it must be a mandate from the European Commission, to achieve standardisation at European level.

2.5 Which parts of the value chain to be certified?

Mr. Marcelo Manca, Vice President Gov. & Ind. Affairs, Europe Underwritters Laboratories Inc., USA, developed the topic of which parts of the value chain to be certified. He stated that with the advance of new technologies, the demarcation lines between utility world and the consumer world have begun to blur, which brings new concerns to the market.

3 Morning Session – Discussion

During the morning session, Mr. **Kostantinos Moulinos** (ENISA) tried to reflect on the state of play as regards the smart grid device certification in Europe and summarize some key findings as regards the identified needs for improvement.

3.1 State of play

A list of points have been addressed by the audience:

1. *Price*: The current certification schemes are considered rather expensive. Several reasons have been reported for this:
   Fragmentation: having fragmented policies (i.e. different policies/schemas in different Member States) means that the cost of the Smart Grid components may be inherently increased as long as there is no generally accepted certification scheme at the level of European market. For this reason, a product needs different certifications in/for different countries. The same situation holds true for countries which have not entered the SOGIS-MRA.
   Resources: extra time and resources are needed to get certification done which sometimes are not justified by the Return of Investment (ROI).
   Repeatability and consistency: some experts exposed that one of the reason why certifications are expensive is because one of the requirements for the test laboratories is that the results have to be repeatable and consistent. Standards that do not provide a certification schema are most cost effective but they do not provide these guaranties. However, hold a certification does not ever mean security.
   Number of certified components: Smart grid is too complex and it consists of many different components. Having all the components certified is too expensive.
2. *Lack of a uniform approach*: The first topic addressed was that stakeholders are facing a fragmented situation where different initiatives regarding the cyber security of Smart Grids are been developed. The communication on these initiatives is needed to better understand what gaps are already addressed and what needs to be done. A comment made was that there is no standard at European level regarding the Smart Grids that allow harmonizing the European practices. As a general consideration on certification schemes, the manufacturers declared that the harmonization will make easier to promote and deliver their products in the EU market. However, certain functionalities have requirements that are not covered yet by the existing technologies (for example, protocols at application layer). Therefore, new implementation may need to be done.
3. *Long life cycle*: The certification process takes some time which usually is more than the time needed for new vulnerabilities to appear in the cyberspace. This, practically means, that the moment a product is certified it has already begun outdated due to the fact that new vulnerabilities have been revealed.
4. *Legal framework*: Most of the European energy regulators do not have the mandate for the security, and as a consequence for the security certification. This practically means, that there a few legal texts concerning the security in the smart grids and this way leaving enough space for grey zones of interpretations.
5. *Common Criteria*: Some experts noted that Common Criteria brings transparency to the process. The energy industry is facing the challenge that it is not security specialized. The value of the certification schema is that the certification shows the kind of attacks which the system has been considered. However, other experts exposed that end users take into consideration the certification and not his details.

Furthermore, it was discussed that there is no standard that will fit all needs, taking on account that Smart Grid is not mature enough yet. In that sense, it will be unrealistic to have a Common Criteria certificate for all the Smart Grid. Finally, according to the some experts, CC is generic certification framework. Therefore, to be applied in the smart grid environment, it should be extended to include specific protection profiles for the smart grid, similar to those related to the smart card Industry, where a joint interpretation library was developed.

6. *Environment of certification*: One additional topic mentioned by some experts is that certification of products is done in laboratories which are independent of the operational environment. A product can be certified but that does not necessary means that when it is implemented in the system, this is configured correctly, that it functions properly, and that it does not affect the performance of the entire network. Certification has a role, it is the first step, but it is important also to see how the devices are configured for security in the operational environment.
7. *Training*: There is no national or European wide specialised training course on Industrial Control Systems and smart grid security.

3.2 Key findings

Based on the abovementioned current situation the following needs identified:

1. *Lowering the cost*: In this respect, some experts stated that security does not come for free; therefore the impact of the cost must be considered carefully and should not be underestimated. Other alternatives not as expensive as the Common Criteria scheme could be a feasible solution. The experts have proposed several ideas on this:

a. One single European certification: As a general consideration on certification schemes, the manufacturers declared that the harmonization will make easier to promote and deliver their products in the EU market. Regarding this aspect, a possible certification scheme for Smart Grids should take as much as possible into consideration the existing technologies.
b. Security requirements: A certification scheme is a possible solution, or it may be even needed but the requirements are more important in order to avoid increasing the cost of the smart grid component production. This practically means, that only the security requirements definition should be mandatory; certification might be at the discretion of the service provider.
c. 'Light' approaches: some experts questioned whether the certification is the only solution to enforce the security of a product. Probably, there are more cost effective and quicker approaches that could apply to the smart grid. One alternative could be the procurement language helping end users what they want. The fact of following a standard not necessary means going through a certification process. Returning back to the procurement language, end users could ask manufacturers for evidences in products to verify that the standards are been followed. More agile alternatives were proposed by experts, based on quick tests

(e.g. white-box and code audits). To this respect, WIB's requirements for vendors (are suggested as a possible reference).

d. Self-certification tools: A good approach to decrease the certification process efforts in terms of cost and time is providing vendors with self-certification tools which could be used by vendors in a pre-certified process or during the development phase and also give the possibility to vendors to select for a wide range of laboratories where their products will be certified. These aspects could speed-up the process and encourage vendors to follow certification schemas.

e. Partial certification: Continuing with the values of the certification, some experts expressed that one value is guarantying compliance with mandatory requirements. Other value is for the energy network provider that has to demonstrate to customers that their data are gathered securely. Finally, consumers trust in the security requirements defined by government bodies and assured by the certification process. However, is not feasible certified all the components. Therefore, it is necessary to define a target of evaluation that contains critical functionalities and components.

2. *Training*: A specialised, pan European course on ICS, SCADA and smart grid security which might lead to certification of the involved personnel is needed. Alternatively, this certification might be part of the existing and well known certifications on standards: ISACA, ISO, etc.

3. *Scope*: Regarding the scope of the certification, some stakeholders noted that the certification of components is important. At this moment, a standard can be developed for the certification of individual component. However, mandatory standards that contain controls for the overall organisation are not defined yet. A certification scheme for the whole grid, not only for the components is needed. The security of the smart grids should be developed taking into consideration that a balance between the risk and the services provided by the energy industry.

4. *Minimum security requirements*: Development of minimum security requirements for other than Smart meters SG devices is needed.

5. *Criticality assessment*: Need to assess the criticality of the different SG parts and apply different assurance techniques based on the criticality. Some stakeholders identified that the whole smart grid contains a wide range of components where having all components certified is not feasible and is not an indication of security of the smart grid. For example, having component of the smart grid exposed on Internet is more critical than do not follow a certification process. Probably, the components of the critical infrastructure cannot be certified at the same method than traditional IT systems. A component certified does not ever mean security as all the risk cannot be taking into consideration. However, a method that take into account all risk does not exist. The challenge in the smart grid context is facing vulnerabilities and threats which are growing faster and faster. The certification in one method that can mitigate risks for the smart grid environment.

6. *One single standard*: The European market starts to be more mature. Member states are considering to develop their own certification schemes to qualify their systems. This could create fragmentation of the market if these activities do not developed in a coordinated

manner. The development of these schemes is mainly coming from certification authorities. However, there is no certification scheme at European level. The development of one accepted profile to harmonize European market is needed.

7. *Certification life cycle*: Certification should focus on the whole life-cycle not only on the product itself: Starting from product development process, expected security quality level, functionality, implementation and deployment of the systems and the operational process.

Finally, most of the participants expressed their confidence that M490[1] a promising initiative towards market harmonization and interoperability.

4 Afternoon session

4.1 The ERNCIP project

Mr. Auke Huistra, presented the current status of the thematic areas on ICS and Smart Grids within the European Reference Network for Critical Infrastructure Protection (ERNCIP). ERNCIP, aims to provide a framework within which experimental facilities and laboratories share knowledge and expertise in order to harmonise test protocols throughout Europe, this leads to better protection of critical infrastructures against all types of threats and hazards.

Apart from a generic presentation of the project, a description of the security testers/certifiers registry was roughly provided to the audience. ENISA will support this initiative by disseminating registration information to the relevant network of experts.

4.2 Standards and Certification for Smart Grids

Ms. Anabelle Lee, Technical Executive – Cyber Security, Electric Power Research Institute., USA, developed the topic Standards and Certification for Smart Grids. **Ms. Lee** started to give an overview on the current environment, and continued presenting the current grid environment and the threats to it. She continued by mentioning some of the trends impacting security and the differences between IT and the Control Systems. She continued by addressing examples for which the US through the Federal Energy Regulatory Commission adopted standards that may be necessary to ensure Smart Grid functionality and interoperability. She concluded by providing recommendations in order to move forward.

5 Panel for Discussion

Mr. Konstantinos Moulinos, opened the panel for discussion, presenting the members of the panel for discussion. This panel was formed by:

- **Mr. Markus Braendle**, Head of Cyber Security for ABB;
- **Mr. Martin Klimke**, Infineon;
- **Mr. Richard Link**, Siemens;
- **Ms. Anabelle Lee**, EPRI.

---

[1] *Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment, http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf.*

Each panellist had the opportunity to make a very short presentation on a particular, relevant to the certification process, topic of his/her interest. **Mr. Klimke**, the Principle of Technical Marketing for Infineon Chip Card and Security, presented the solutions with regards to security that Infineon provides to the different countries depending on the focus on security these countries have. As a component provider, Infineon has focused on providing components that are produced in large numbers and for which in some cases are difficult to replace.

5.1 The future certification scheme

The panel was called to elaborate on the future smart grid security certification framework. Based on the answers received and the interaction with the audience, the following are some of the wished characteristics of the future scheme:

1. *Mandatory*: the view of the participants to the workshop was that the certification scheme should be mandatory rather than voluntary.
2. *Harmonization*: A harmonized approach which eliminates the barriers and silos created by fragmented markets is needed. The harmonised approach is considered as a major contributor to lowering the cost of certification.
3. *One unified standard*:[2] some aspects to be taken into account:
   a. *Complexity*: having a unified standard is important to deal with the actual reality and complexity of the energy industry. An industry where there are different standards that have different requirements, for each country, region or even industry segments. Furthermore, within this reality, customers do not have the knowledge of the importance of security. As a vendor it will be highly valued to have a single standard that not only covers smart grids, but industrial control as systems in general that could outline the security expectations.
   b. *Interoperability*: Another important aspect to take on account is the interoperability continues as actual state. This aspect allows the customer the ability of buying products to different vendor companies. As security is added to the systems it is important to maintain the actual interoperability.
   c. *Life cycle*: a unified and globally accepted standard should focus on the whole life cycle of the product. Is not enough to have a technical standard, but this standard should cover also from the process of developing the products, the security quality level expected, the functionality, through implementation and deployment of the systems, until the operational process. Additionally, some experts noted that there are standards that are focused on certified the development process of the product and not the product itself. The certification of every new instance of a product is more difficult than having a secured development lifecycle in place for products that assures the quality and security of the product.

[2] *Some experts stated that the German approach is not to have a Global Common Criteria Certification for the entire value chain, but to focus on the certification of the most critical components of the entire value chain.*

4. *Not a single certifying authority*: Information sharing on smart grid vulnerabilities and product certification may involve national security issues. Thus, keeping member states and the competent national certification Authorities in the lead of certification process is considered as a good practice.
5. *Easy to be adopted by the MS*: The scheme should be designed by taking into account the opinions of the MS, thus making it easy to accept it.
6. *Deal with the patch management problem*: the product lifecycle is important in term of cost and throughput as every time that a vendor provides a patch for a certified component, the component need to be recertified. Going in line with the product lifecycle, vulnerabilities and threats coming up faster than the certification and product lifecycle becoming more challenging the security for Smart Grid.
7. *Once certified not extra certification needed across Europe*: No extra certification fees should be required for a product which has already been certified in one of the MS.
8. *Take into account the existing technologies*: certain smart grid functionalities have requirements that are not covered yet by the existing technologies (for example, protocols at application layer). Therefore, new implementation may need to be done.
9. *In line with the standardization efforts:* although different implementation for particular requirements could be useful for stimulating the competition, the security cannot be defined at an abstract level and therefore has to be in line with the standardisation efforts.

Mr. Moulinos encouraged the panel of discussion and the stakeholders to address the question: Is it there a need of a single interoperable standard framework? One of the members of the panel gave his opinion stating that it is important to understand the standards that should be included in the certification of Smart Grid and how to this standards must be extended in order to cover any white spots, and not to create new ones.

Furthermore, standards are not fully mapped to technical solutions. It was suggested that multiple technical solutions must be allowed to cover more specific standards.

A concern that was highlighted is that there are different security requirements for each specific domain. This is an issue that should be taken in consideration while building the standard.

6 Wrap up

6.1 Conclusions

Certification is only a part of the security process: certification on smart grid is only part of the process to be performed in order to have a secure system.

Limited scope of the current certification schemes: Smart grids are complex systems. The current certification schemes focus on the components instead of the grid as a whole. For this reason, adding a certified device to a complex and vulnerable system adds a little to the assurance value. A scheme which encompass the assurance that a (sub)system is operating at an acceptable, as regards the security, level is needed.

Not focus only on the smart meters: the smart grid solution for smart meters is too narrow, taking in consideration that there are also new technologies as windmills, electro mobility, etc, for which no standards are defined yet. It is important that when a Security Certification on Smart Grid is built, this should also cover certification and standards for new technologies. Furthermore, minimum security requirements for other parts than the smart meters should be identified and defined.

Smart grid is part of the European critical infrastructure: that it is important to have a clear European standard for critical infrastructure, a need that has been addressed more than once, and that cannot be delayed any more.

A unified European wide approach: a certification scheme should take into consideration not only technical domains but also organisational and process domain. For this reason, before the development of a unique certification a harmonized European electricity market is needed. Taking into account that harmonized the electricity market is not an easy challenge; one approach could be the development of protection profiles with specific sections for each country. Furthermore, the harmonization process must start across Europe but also beyond the European market. According to the harmonization activity, some experts noted that the European Mandate M/490 tries to come up with an European Standard that not only brings the harmonization to the market but also assures the interoperability among components from different manufacturers.

Enhanced competition: as regards the unique certification scheme across Europe, there are two different concerns to take into consideration: cost and throughput. Therefore if one standard is developed at European level, the resources needed, like certification testing labs, to support a certification process across Europe must be able to keep all vendors capable of competing at the same level.

Information sharing: More information sharing is needed. Another concern to take in consideration is the difficulty is to share vulnerability information on Smart Grids components, due to the fact these vulnerabilities, may include issues in national security. Although there Member States have already made some advance on cyber work, it is a key point to share these advances between them.

Resources: the future certification scheme must take into account both the cost of the process and the time needed to be certified.

Security built-in approaches: smart meters will be connected by standardized network infrastructures, which will mean that they will become targets for attacks and misuse. In this sense, security must be built from the beginning and for each element until the process of patch management. This can only be achieved with the support of a Security Controller that will provide a solid foundation for Smart Meter security. A reactive approach with regards to the smart meter system is considered to be risky

Reasonable legal framework: A few smart grid security legal texts exist across Europe. Without sufficient legal framework the on-going initiatives will be developed in an uncoordinated manner. For this reason, a reasonable legal framework is needed which will

not only set the minimum security measures but also will give incentives to the involved parties to continuously improve and do more than is needed by the law.

Reasonable assurance: Certification like security testing, audit etc are methods to provide the user of a system with the assurance that the system he uses it works in an acceptable level of security. Due to their complexity, we cannot certify all the components of a smart grid. For this reason, a framework for the coexistence of the alternate assurance methods in the smart grid should be developed.

Security metrics and measurements: In order to support security experts to justify investments on security, metrics measuring the ROI on the smart grid should be developed.

The ERNCIP project was received well by the audience and many participants expressed the interest to register testing/experimental/accreditation facilities on the Inventory. Once populated, the inventory will be accessible via Internet[3].

6.2 Actions

Proposed actions:

- It was suggested that the EC and ENISA, builds an inventory on standards and practices that are actually used.[4] And that instead of creating a new regulatory framework, the EC and ENISA, focuses on the process in opposition to requirements and controls, and extends it to those white spots that are left between different standards.
- Provisions should be taken in order to maintain the testing/experimental/accreditation inventory up to date.
- Create a platform for sharing information on smart grid vulnerabilities and this way promoting the dialogue for the smart grid security certification issues.

[3] https://erncip.jrc.ec.europa.eu/

[4] *A complete list of the smart grid standards and initiatives may be found at,* https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu