

Smart grid security certification in Europe

Challenges and recommendations

December 2014





About ENISA

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

For contacting ENISA or for general enquiries on Critical Information Infrastructure Protection, please use the following details:

- E-mail: resilience@enisa.europa.eu
- Internet: <http://www.enisa.europa.eu>

For questions related to certification of smart grids, please use the following details:

- Dr Konstantinos MOULINOS, Expert in Network & Information Security - Resilience and CIIP, European Agency for Network and Information Security Agency – ENISA
- Address: 1 Vass Sofias & Meg. Alexandrou, Marousi, GR-151 24, Athens, Greece
- Email: resilience@enisa.europa.eu

Follow us on

Facebook: <http://www.facebook.com/ENISAEUAGENCY>

Twitter: https://twitter.com/enisa_eu

LinkedIn: <http://www.linkedin.com/company/european-network-and-information-security-agency-enisa>

Youtube: <https://www.youtube.com/user/ENISAvideos>

RSS feeds: <http://www.enisa.europa.eu/front-page/RSS> Acknowledgements

Contributors to this report

The European Union Agency for Network and Information Security (ENISA) would like to recognise the contribution of the DNV GL team members that prepared this report in collaboration with and on behalf of ENISA:

- Hans Baars
- Robert Lassche
- Robin Massink
- Hans Pille

On behalf of ENISA, Konstantinos Moulinos worked together with the team in order to prepare this report.

Agreements or Acknowledgements

ENISA would like to thank the following experts for commenting the report. It has to be noted that the contribution of the experts, in the list below, reflect the personal opinion of the experts and by no means do they present the official position of the affiliated organisation.

Fourati	Alia	EDF R&D
Comerford	Noel	Ernst & Young
Strabbing	Willem	ESMIG
Assaf	Nadi	T&D Europe
Hemberger	Klaus	Bundesnetzagentur (BNetzA)
Jensen	Ingo	E.ON
Weisshaupt	Thomas	Gemalto
Harner	Andreas	DKE VDE
Couet	Claire	EURELECTRIC
Feuillet	Mathieu	ANSSI
Meynet	Stephane	ANSSI
Chuzel	Julie	ANSSI
Salamon	Yann	ANSSI

Affiliated organizations are considered to represent the following actors in the smart grid eco system:

- Vendors and manufacturers
- Distribution System Operators (DSOs)
- Standardisation initiatives
- Public Authorities (with a mandate on smart grids' security)
- Research community
- Security service providers
- Industry Associations

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

ISBN: 978-92-9204-101-4, doi 10.2824/36179

Executive summary

Security and privacy issues are of major concern for smart grid users. For this reason, vendors should ensure that these two features follow smart grid devices for their whole life cycle; from the design to the decommission phase. Certification is not only a means to provide assurance to the smart grid users that security and privacy have been taken into account but also to create trust to the entire smart grid supply chain.

This report provides insight on security certification of smart grids. It contains information about several certification approaches; it describes the specific European situation, discusses the advantages and challenges and provides recommendations to involved stakeholders towards a more harmonised European smart grid security certification practices framework.

The report describes the need for harmonised European smart grid certification practices which cover the complete smart grid supply chain, and are supported by a European platform based on M/490 SGAM¹ (Smart Grid Architecture Model) and the concept of smart grid chain of trust. Part of this report is the analysis of the available security certification schemes for smart grids and the approaches used in Europe. This way we have generated an overview that depicts which certification schemes can be used to create this chain of trust. During this analysis it came up that there is not a single, existing, scheme that can cover the entire chain of trust, and that not all parts of the chain can be completely covered for every smart grid use-case. Additionally, it appeared that there are multiple initiatives in different Member States that take different approaches to achieve the same goal. For this reason, we use the common denominator of the features of the different existing certification standards in order to introduce a certification meta-scheme for the smart grids in Europe.

The major gaps and challenges of a European smart grid certification scheme revolve around the fragmentation and different approaches in Member States, as well as the lack of EU guidance by a trusted oversight body. At this moment it will be difficult to create a security certification scheme that

¹ SGAM is an abbreviation for the Smart Grid Architecture Model proposed by M/490 standardisation initiative, and is widely accepted as the common reference model architecture for smart grids not only at European but also at international level. The group coordinating this activity is the CEN-CENELEC-ETSI Smart Grid Coordination Group (SGCG)

completely confronts the identified challenges, but an approach can be outlined that describes how to go from the current fragmented situation to a more harmonised one at the EU level. This approach allows for the national specific approaches and requirements, while providing possibilities to adopt European based requirements to facilitate harmonisation, and benefit from joined standardisation efforts.

Taking into account the needs, as expressed in various referenced resources, we also outline the properties of the 'ideal' smart grid cyber security apparatus. To achieve this 'ideal' situation a set of recommendations is addressed to the main stakeholders; the Commission, the certification bodies, the Member States and the private sector. The most outstanding recommendations are:

Harmonised EU smart grid security certification practices

More harmonised and coordinated EU smart grid certification practices will act as an umbrella and should contain elementary properties that national schemes need to have. European accreditation bodies will be used for confirmation of national schemes. This will ensure that there is not a single certifying authority, and the process remains impartial. Next to this, private sector will help in keeping up with the latest technology specific requirements and guidance consolidated by technical committees. The committees should amend the slow moving standards with detailed protection profiles or security requirements. Updates in national schemes should be announced so that they can be incorporated in national profiles. This way the maturity of the national schemes can evolve over time.

The Commission together with the Member States should promote certification by allowing for commercial advantages for the private sector when following practices which lead to more harmonisation across Europe (e.g. criteria for E.U procurement activities). The certification practices should provide European guidance, facilitate national legislation and be actively promoted as a means for more harmonization.

National implementation of specific smart grid use cases based on a chain of trust

Each Member State should be able to map its preferred national standard/scheme to the EU platform and refer to this national standard for details. They should also be able to amend or expand on the European security requirements to provide the flexibility to incorporate national specific requirements. The national profiles should be created by national groups, but could be based on the published schemes of other Member States. The national profiles can contain the national specific technical requirements regarding the needed security features related to the applicable use cases used in that Member State. Additionally they should contain test procedures for the national specific requirements, and define the required testing levels for the national use cases aligned with the international SG-IS² framework risk levels.

Oversight

It is recommended to create a EU steering committee with oversight competences on smart grid certification, the definition of pan European security requirements' and the development of national schemes. It should be responsible for centralised storage and the publication of smart grid certificates and adopted schemes, to facilitate clarity on what is certified and how. It should provide implementation guidance and recommendations based on the most recent best practices and informative standards.

The EU steering committee will have only a coordination role and act as an advisor to the certification bodies, making sure the latest threats are reflected in the security requirements definition process.

² This framework is described at the M/490 SGCG Smart Grid Information Security deliverable.



To this end, this committee will take feedback from the private sector, and lessons learned during the certification processes of other nationalities.

The steering committee should create and maintain a landing page with specific explanations for all stakeholders about smart grid security certification concepts, their place in the chain of trust and how to implement a smart grid certification chain of trust on a specific smart grid use case.

Table of Contents

Executive summary	iv
1 Introduction	1
1.1 Overview	1
1.2 Policy context	1
1.3 Scope	2
1.4 Target audience	2
1.5 Structure of this document	3
1.6 Method	3
2 The need for smart grid certification	4
2.1 State of play	4
2.2 Market drivers	4
2.2.1 How certification works (success stories)	5
2.2.2 And how it does not work (failure stories)	5
2.3 Stakeholder needs	6
2.4 Desired properties of an 'ideal' certification scheme	9
3 Standards and certification schemes	12
3.1 List of standards and schemes	12
3.2 Meta-scheme	14
3.3 Qualitative analysis of examined certification standards	15
3.3.1 Operation certification scheme	15
3.3.2 System certification scheme	16
3.3.3 Development certification scheme	16
3.3.4 Component certification scheme	17
3.4 How are schemes currently applied in the EU?	18
3.4.1 Germany	18
3.4.2 United Kingdom	18
3.4.3 France	19
3.4.4 Other Member States and EFTA countries	19
3.4.5 European cooperation for Accreditation (EA)	19
3.4.6 SOG-IS	21
3.5 Key findings	22



4	A Chain of trust for the smart grid	23
4.1	The supply chain view of the smart grid	23
4.2	Analysis of the smart grid chain of trust	23
4.2.1	Certification and the chain of trust	24
4.2.2	Adoption of SG-AM for a chain of trust model	25
4.2.3	Security requirements	26
4.2.4	Definition of risk levels aligned with the SG-IS framework methodology	27
4.3	Conformity assessment and its relation to testing	29
4.4	Description of certification scheme relations loosely based on SG-AM model	31
4.4.1	Business layer	32
4.4.2	Functional layer	33
4.4.3	Information layer	33
4.4.4	Communication layer	34
4.4.5	Component layer	34
5	Gaps and Challenges	36
5.1	Gaps and challenges related to the needs	36
5.2	Gaps and challenges related to the desired properties	37
6	Recommendations	40
7	Conclusions	44
8	References	46
8.1	Related ENISA papers	46
8.2	Legislation	46

1 Introduction

1.1 Overview

The introduction of smart grids increasingly leads to more automation. Where in the 'old' grids automation was owned by the grid operator itself and took place on a dedicated network, in a smart grid environment multi entities are connected together. Those entities own cables, solar panels, wind turbines, biomass plants and so on, and they all need IT connections to exchange data with each other to ensure the right decisions are made from an individual economic and technical perspective. While the equipment has evolved to facilitate the data exchange with more intelligent and automated or remote controlled devices, the practices regarding manufacturing and maintenance of devices are still similar to the ones that were on a dedicated network. This created a gap, where the level of security did not grow together with the increased automation and interconnections of the grid.

For this reason, cyber security certification of the smart grid has gained popularity as a means to further enhance the security that these complex systems already offer to their users. The need to foster the development of security certification schemes for product and organisational security was one of the key findings of ENISA's 2012 report on *"Smart grid security: Recommendations for Europe and Member States"*. In this document, ENISA recommends:

"By raising the level of security and mitigating risk, accreditation and certification schemes would increase end consumers' confidence in smart grid services and systems and accelerate their acceptance. Moreover, certified service providers can be easily compared allowing for marketing strategies...."

Certification in smart grid cyber security therefore also delivers a competitive advantage for both suppliers and service providers.

1.2 Policy context

The recently published Cyber Security Strategy of the European Union³ clearly identifies the shared responsibility of all stakeholders and the need for all actors to protect themselves in the context of growing dependency on information and communications technologies. The need to develop industrial and technical resources for cyber security is mentioned among the strategic priorities and actions, and in this context:

"A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. The Commission will promote the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses."

³ Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

The abovementioned excerpt from the EU Cybersecurity Strategy is aligned with the findings of the workshop organised by ENISA in 2012 where the experts clearly expressed the need for more harmonised smart grid certification practices as a means to lower the costs of certification and break down the trade barriers.

1.3 Scope

The objective of this document is to provide technical advice, recommendations and good practices for security certification for smart grids. Strategy, architecture guidelines and framework alternatives are presented as recommendations which set the basis for the smart grid certification requirements.

This document does not solve all the political and legal issues related to implementing such smart grid security certification obligations. Good practices of existing certification schemes and regulations in the smart grid environment are presented as potential guidelines. The problem definition and the need for certification point out in chapter 2, form the basis for this document.

Data protection is of the utmost importance for the smart grid⁴. Security certification is considered as one of the measures which contributes to a safer and, as a result, a more secure processing environment of personal data in the smart grid. Many security requirements described in existing security certification standards are considered to be relevant to the existing data protection framework. However, there are many data protection requirements (i.e. consent of the data subject, the purpose definition, proportionality of collected data etc.) and tools (i.e. privacy by design, data protection impact assessment (DPIA), best available techniques (BATs), privacy seals, notifications of the processing to and audits by the national Data Protection Authorities (DPAs) and data breach notifications) which are less or not relevant to existing security certification standards.

1.4 Target audience

The target audience of this document is the European Commission and Member States (MSs) interested in open issues regarding security certification in smart grid environments. This document aims to:

- Create a common basis on which smart grid security certification can be structured
- Inform the related industry community (IT security engineers, ICS engineers and operators, national Information Security offices/agencies)
- Provide an interface between policy makers and technology specialists regarding smart grid security certification.

The stakeholders related to the findings and recommendations in this document are:

- Certification and accreditation organizations
- Regulators and policy makers
- Smart grid operators
- Standardisation Bodies (e.g. ETSI, NIST, IEC, ISO, etc.)
- Security solutions providers
- Smart grid manufacturers
- Academia, R&D
- Public bodies in the Member States involved in smart grid cyber security.

⁴ Commission Recommendation on preparations for the roll-out of smart metering systems (2012/148/EU), available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012H0148&from=EN>

1.5 Structure of this document

The document consists out of six main sections explaining in subsequent order:

1. Introduction
2. The need for smart grid certification
3. Standards and certification schemes
4. A chain of trust for the smart grid
5. Gaps and challenges
6. Recommendations

Please see “Annex A: Definitions” for a short list of definitions used throughout this document.

1.6 Method

The team has initially performed a desktop research with the objective to identify both the need for more converged smart grid certification approaches in Europe and the properties of an ‘ideal’ certification scheme. Then, they took stock of the existing security certification approaches in order to identify, analyse and then compare security standards, good practices and schemes that could be used in order to define the properties of a smart grid certification meta scheme. They analysed the results of the research and the outcome of the analysis delivered:

- Identification of gaps between the existing schemes and the ‘ideal’ one.
- Identification of gaps between different certification standards.
- Challenges involved in further harmonising the existing smart grid security approaches in Europe.
- Recommendations on how to improve the existing European smart grid certification apparatus.

Both the result of the research and the draft report were validated by the Smart Infrastructures Security Experts Community (SISEC)⁵ and a number of selected ICT and smart grid certification experts. Based on the comments received by the experts a second draft was prepared then and this new document presented in a thematic workshop organised by ENISA⁶. For the workshop, ENISA has invited experts from different stakeholder categories to assess the quality of the findings and debate the proposed good practices and recommendations. The final report is the outcome of the second round of consultation with the experts.

⁵ ENISA’s Smart Infrastructures (cyber) Security Experts Community (SISEC) includes cyber security experts from national cyber security authorities, energy and ICT industries, and possibly also selected non-EU partners. SISEC has the mission to support the overall goal to achieve a higher maturity in cyber security for the critical infrastructure of the European Union in order to increase the robustness and availability of critical infrastructure against cyber security threats.

⁶ <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/certification-of-cyber-security-skills-of-ics-scada-experts-and-smart-grid-components>

2 The need for smart grid certification

This chapter describes what specific key drivers have been identified to support the need for a more organised and harmonised European framework for smart grid certification practices, and why such a framework helps to create a chain of trust to the product (energy) delivered by the smart grid. The general need for certification in the area of smart grids has been addressed in previous ENISA documents, such as the report on Protecting Industrial Control Systems - Recommendations for Europe and Member States, 2011 and the minutes from the joint ENISA/EC workshop on the certification of smart grid components (2012)⁷. This report can be considered as a follow up to the findings and recommendations illustrated in these documents.

2.1 State of play

The following list of items summarises the current situation around smart grid component security certification as reflected during the ENISA workshop:

- Price: Current certification schemes are considered rather expensive. Several reasons have been reported for this; fragmented national policies, lack of resources, the need for repeatability and consistency of the results and the large number of components involved in the smart grid supply chain.
- Lack of a uniform approach: Stakeholders are facing a fragmented situation where different initiatives regarding the cyber security of smart grids are being developed.
- 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.
- Legal framework: There are only a few legal texts concerning security in smart grids and this is leaving enough space for grey zones and/or interpretations.
- Common Criteria:
 - is the predominant certification scheme in the market.
 - it will be unrealistic to have a Common Criteria certificate for the whole smart grid supply chain.
 - 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.
- 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 necessarily mean that when it is implemented in the system, it is configured correctly, that it functions properly, and that it does not affect the performance of the entire network.
- Training: There is no national or European wide specialised training course on Industrial Control Systems and smart grid security to educate experts on security certification matters.

2.2 Market drivers

The drivers behind certification vary widely. Security certification has historically originated from governmental agencies to ensure a level of trust in their equipment and supply chain (e.g. FIPS140-2, ISO 15408). However, industry partners have also taken it upon themselves to create certain certification schemes, such as the vendor focussed UCAIug which created the IEC 61850 certification

⁷ <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

standard that can be also applied to the smart grid industry. Here, it was recognised by several vendors that it would be mutually beneficial to create a common and impartial understanding of how devices operating in an electrical substation should interact.

In some cases, insurance companies and banks can also drive certification as a means to secure investments made, and minimise the risk of monetary or other types (e.g. reputational) of loss due to the use of substandard quality or security by their customers.

Recognition by key stakeholders is the most important aspect for a successful certification scheme. Without the recognition and endorsement of key stakeholders, a certification scheme holds little value, and any cost incurred by the certification process becomes difficult to justify.

Therefore, some schemes such as Common Criteria adopt a chain of trust, and facilitate an infrastructure where Member States are able to officially recognise each other's certificates. A different solution is to have an international users group issuing the certificate, however this can be difficult for smart grid security, as the government is a significant stakeholder and therefore it will probably need a more formalised accreditation process to accept any type of certificate.

2.2.1 How certification works (success stories)

There are numerous success stories where a properly implemented scheme has developed into a successful and mature standard that is recognised by the relevant stakeholders. A good example of this is the Common Criteria framework in the smart-card industry, where it is widely accepted.

Another success story is the implementation of NERC-CIP in US, as it helped evolve cyber security in US, and ensures that all critical infrastructures have taken a minimal set of precautions to protect their assets.

2.2.2 And how it does not work (failure stories)

Unfortunately the successful schemes have sometimes also caused a compliance culture, where asset owners first try to ensure that a minimum set of critical assets is defined, to keep cost low. The mandatory audit trails are seen as the cumbersome creation of paperwork, without much attention for the processes that should have generated it in the first place.

Another pitfall is illustrated by a security standard in the Netherlands, where the security requirements were made too general, and the insurance premiums appear to be cheaper than actual compliance to the standard.

Some SCADA standards encountered criticism because the promised interoperability seemed not to be provided by the certification scheme. This issue had more to do with how the scheme was advertised than a flaw in the scheme itself. But it should be clear that the critique the standard encountered did not improve the endorsement by the stakeholders.

Some schemes allow a vendor to write its own requirements to seek certification against, and this can provide a biased image. For example, several companies have certified their products against the scheme, but the usability of the certified configuration is said to be very limited.

Additionally depending on the scheme and requirements, certification can be a rather lengthy and costly process, (a process costing several hundreds of thousands euros and taking a year is not uncommon) and can therefore cause small players to be forced out of the market. That being said, some schemes do allow a lower security level, which is also much faster and cheaper to certify. But this will mean that the level of certified security will also be severely affected. Another reason for increased cost of certification is that there is no consensus on the certification method between

Member States. Without consensus on the method used, certification efforts have to be repeated multiple times with different methods for different Member States.

2.3 Stakeholder needs

The European Union, as well as previous studies done by ENISA and ESMIG (European Smart Metering Industry Group) backed up by stakeholders; provide statements regarding the recognition of a need for a pan European smart grid certification. Below is a summary of the various statements:

1. Solve trust issues between EU stakeholders regarding the smart grid
2. Create a common reference model for smart grid security in EU
3. Establish the basis for a minimum set of auditable controls for smart grids across Europe
4. Define an agreed method for the level of security for different criticality aspects of the grid
5. Establish a harmonised approach in the EU for smart grid component, system, and operational security to increase trust
6. Provide EU guidance for a harmonized approach that facilitates national legislation
7. Promote public and private interaction within the EU on smart grid security
8. Improve the maturity level of security in the EU smart grid
9. Establish shared responsibility in risk mitigation amongst EU stakeholders
10. Lower costs of smart grid certification in the EU
11. Address the life cycle of a European smart grid

Below follows a description of each statement with a reference to the source the statement is based upon.

Solve trust issues between EU stakeholders regarding the smart grid⁸

This relates to the different national regulations and the fragmented nature of the smart grid which makes responsibility and accountability unclear. Additionally, because of the multidisciplinary nature of smart grid systems, the supply chain of the used components and systems is quite wide, not transparent and complex. This can cause trust issues within the EU stakeholders because they cannot oversee all related risks anymore.

Create a common reference model for smart grid security in EU

The European market is becoming more mature. Member states are considering to specify their own security requirements and develop their own certification schemes to qualify their products. This could create fragmentation of the market if these activities are not developed in a coordinated manner. The development of these schemes is mainly originating from certification authorities. However, there is neither a protection profile covering the whole smart grid chain nor a certification scheme at a European level yet. The development of one reference model to harmonise the European market is therefore needed.⁷

ESMIG expressed the intention to reach a multi-stakeholder, European wide approach to identify (technological and economic) security and privacy risks emerging with the deployment and operations of a smart metering system. This was done in order to draw appropriate requirements and countermeasures for smart meter/grid use cases from asset owners.

⁸ <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide>

Establish the basis for a minimum set of auditable controls for smart grids across Europe

There is a need for a European set of requirements that can be used for reinforcing the cyber security of the smart grid.^{9, 10} This is important to create a level of security that has a common baseline across Europe, and facilitates as a common interface for the interaction regarding cyber security between Member States.

Define an agreed method for the level of security for different criticality aspects of the grid

Some stakeholders have identified that the smart grid, as a whole, contains a wide range of components. Having all these components certified is perhaps not feasible, and it is not a good indication of the security of the whole smart grid. There is a need to assess the criticality of the various smart grid parts and apply various security assurance techniques based on that criticality. For example, a smart grid component that is in a more exposed environment could in some cases have a larger impact on the security of the grid. It would therefore, in that case, be beneficial to focus more on these critical components that could have a large impact, then to spend the same amount of time and money on components that have a much lower impact on the security of the grid.

Probably the components of the critical infrastructure cannot be certified using the same method as traditional IT systems. Also a certified component does not imply a secure component, since all the risks cannot be taken into consideration. The challenge in the smart grid context is facing vulnerabilities and threats which are growing faster and faster due to the complexity of the system and the large number of interdependencies amongst its components. Certification is one method that can mitigate risks for the smart grid environment.¹¹ Care should be taken with such a certification approach that flexibility is maintained, and to allow for a risk level based on system criticality since the level of criticality of a system can differ per stakeholder and per Member State.

Establish a harmonised approach in the EU for smart grid component, system, and operational security to increase trust

During previous interviews and surveys with stakeholders, it emerged that a significant portion of stakeholders expressed their doubts about the trustworthiness of the smart grid. This is backed up by previous ENISA reports, where in one of the key findings of the ENISA's 2012 report on "Smart grid security: Recommendations for Europe and Member States", ENISA recommends that:

*"Recommendation 6: Promote the development of security certification schemes for products and organisational security: By raising the level of security and mitigating risks, accreditation and certification schemes would increase end-consumers' confidence in smart grid services and systems and accelerate their acceptance. Moreover, certified service providers can be easily compared allowing for marketing strategies...."*¹²

"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

⁹ Recommendation 5: Develop a minimum set of reference standards and guidelines - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations/at_download/fullReport

¹⁰ Minimum security requirements: Development of minimum security requirements for other than Smart meters SG devices is needed. - <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

¹¹ <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

¹² http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations/at_download/fullReport

*individual component. However, mandatory standards that contain controls for the overall organization 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 the balance between the risk and the services provided by the energy industry.*¹³

ESMIG also suggests that a scheme that supports IT systems and components in the smart metering domain is desirable; *"This contributes to ensure interoperability and a commonly implemented certification scheme for Products and Systems in smart metering as initial Smart Grid deployments"*

Provide EU guidance for a harmonized approach that facilitates national legislation

A harmonized smart grid approach is needed that includes economies of different scales and sizes, can support any potential market model, and facilitates legislation on EU-Level.

Promote public and private interaction within the EU on smart grid security

It is seen as important to ensure that any adopted scheme will promote interaction between public and private parties in the EU, to ensure wide support for a scheme, and to facilitate a scheme that is not a burden on the parties involved.¹⁴

Improve the maturity level of security in the EU smart grid

The approach to security in the EU varies between Member States. The European market starts to become 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 develop in a coordinated manner.

Last year, ENISA organized a workshop on the certification of smart grid components. During this event, the experts had the opportunity to discuss the challenges of the existing security certification approaches that apply to the smart grids. One of the key findings of this workshop was that there is recognition for a need for improvement regarding the existing certification schemes in the EU.¹⁵

Establish shared responsibility in risk mitigation amongst EU stakeholders

The recently published Cybersecurity Strategy of the European Union clearly identifies the shared responsibility of all stakeholders, and the need for all actors, to protect themselves in the context of growing dependency on information and communications technologies. The need to develop industrial and technical resources for cybersecurity is mentioned among the strategic priorities and actions, and in this context: "A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. The Commission will promote the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses."¹⁶

¹³ <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

¹⁴ Recommendation 2: Foster the creation of a Public-Private Partnership (PPP) entity to coordinate smart grid cyber security initiatives - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations/at_download/fullReport

¹⁵ <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

¹⁶ European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final) - http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Lower costs of smart grid certification in the EU

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.¹⁷ The effort that has to be undertaken to ensure security is maintained across all national approaches of the EU Member States is complex, due to the different smart grid approaches and requirements per Member State. Having a different certification approach and different requirements per country will be more costly in respect to compliance as opposed to a European approach. As a product or system would have to undergo recertification for each individual Member State. Therefore there is a need for a harmonized approach that can potentially lower the cost of certification by making them exchangeable between Member States.

Address the life cycle of an European smart grid

Certification should focus on the whole life-cycle not only on the product itself: Starting from product development process, implementation and deployment of the systems and the operational process.¹⁸ Additionally, a certification scheme will need to incorporate the different types of certification that apply to the product lifecycle, as product development certification, product certification and operation certification are not subject to the same type of certification.

2.4 Desired properties of an 'ideal' certification scheme

Based on the observed market drivers, success stories and the stakeholder needs as addressed in relevant smart grid security certification documents, the team has identified a set of properties which an 'ideal' smart grid certification framework will need to have. Following is the description of these properties.¹⁹ The numbering matches the numbering of the needs described in section 2.3:

1. It provides a holistic approach to ensure trust in the supply **chain** of the smart grid. This way, it will provide clarity on what responsibility lies where.
2. It uses a common EU smart grid security **reference model** like SG-AM that is widely accepted by European Standardisation Organisations (ESOs) and Certification Bodies (CBs). There is confidence amongst the stakeholders that M/490 is a promising initiative towards market harmonization and interoperability.
3. It has a common baseline **set of requirements** described in profiles that are recognized by all participating EU Member States, making acceptance in one Member State possibly also valid in another. However, it must provide the Member States with the flexibility to define their own security requirements on top of the commonly agreed European ones.
4. It uses internationally **equivalent security and risk levels** aligned with the levels defined in an approach recognized by the EU members such as the M/490 SG-IS framework.
5. It includes support **for components, systems and operation**, so that there is one framework to describe the security for a complete smart grid system.
6. It includes conformity **testing**, functional testing and interoperability testing. Depending on the risk of nonconformity, it can be decided to perform first, second and third party assessments. However, in practice, only third party certification is seen as trustworthy for most cyber security schemes.

¹⁷ 1. Lowering the cost: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

¹⁸ 7. Certification life cycle: - <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

¹⁹ <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

7. It facilitates **public and private interaction**, for example by including Technical Committee subgroups, and having a framework coordinator as an interface between public and private bodies
8. It should **not** be EU **mandated**, but a framework providing EU guidance for implementation, and supporting national legislation. Other discussions have suggested an EU mandated scheme, but it will be difficult to create consensus about this.
9. It should improve the maturity of smart grid security in the EU, using **initiatives that align** with smart grids such as M/490 and provide guidance for proper security measures.
10. It has a **harmonized** approach which eliminates the barriers and silos created by fragmented markets. A harmonized approach is considered a major contributor to lowering the cost of certification. The shared responsibility and the risk based approach help to contain the costs as well.
11. It addresses patch management problems and it should include a **maintenance** scheme for a product or system life cycle.

During stakeholder discussions²⁰ about smart grid certification, there has been focus on the desired properties of a future certification framework; the following are some of the additional desired characteristics of this framework:

Operational in a reasonable time

It is important to promote a framework that can be implemented in the current environment, and does not rely on future developments. This is because smart grid systems are being built already, and to add security later on will be more costly and difficult. On top of this, the framework should be based on existing standards and operational (e.g. SOGIS) platforms.

Take into account new and existing technologies

Certain smart grid functionalities have requirements that are not covered yet by the existing technologies, the framework should cover new technologies as soon as they become available. Additionally, security is a fast evolving field that needs constant updating to the latest types of threats. Therefore a successful framework needs to be flexible enough to keep up to date with the latest threads.

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 schemes.

In line with the standardization efforts

Any certification initiative should be in line with the current EU standardization efforts, such as the initiatives ESMIG is taking in respect to smart meter security. Although different implementations for particular requirements could be useful for stimulating the competition, security relies also on interoperability. Therefore a successful framework should promote alignment with existing standardization efforts like M/490.

²⁰ <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>

Room for special national requirements

A scheme should be EU based, but also leaves room for special national requirements. This is necessary to accommodate the approach and legislation in different Member State, which influences the technical decision making, and therefore also has impact on the level of risk and type of requirements specified. A successful framework will have to accommodate national requirements, and make it easy to adopt by Member States by taking into account the current national initiatives.

Not a single certifying authority

It is important not to have a single certifying authority, to ensure no monopoly is created on certification, and multiple players are able to provide certification services.

Coordination

A single framework coordinator should keep oversight on issued certificates and the performance of the certifying bodies to ensure quality is maintained, and not negatively affected by race-to-bottom type scenario's that can occur in a competitive market.

Transparency

The framework should offer centralised storage of smart grid security certificates to facilitate clarity on what is certified and how. This way it is transparent for all stakeholders on what certificates are issued and where and how the chain of trust is built in specific cases.

Motivating and beneficial for the implementer

A successful framework should motivate implementers complying with the applicable certification schemes. Having an economic incentive can positively influence the adoption of a scheme. For example, inclusion of a scheme as a knock-off criterion for smart grid equipment tenders can motivate adoption.

Allow for legacy grid systems to exist side by side with smart grid systems, without compromising security

A successful framework should make sure that it allows current grids to exist, as it will be impossible to migrate all systems at once. Based on a risk analysis, it can be assessed per case if they can also be part of a smart grid certification effort.

Partial certification

There have been discussions about the possibility for a partial certification to support legacy systems and to facilitate the cases where it will be impossible to certify all components in a system. Although this approach is understandable, it will create an inconsistent view of smart grid certification, and will therefore undermine trust if not handled correctly.

Instead a framework should provide clarity on what the scope of a certificate is, and how it creates the chain of trust, so it is evident what parts are covered or not, and why certification can still apply for the use-case at hand.

3 Standards and certification schemes

A desktop study has been performed to create an inventory of available information on cyber security certification standards that are applicable to the smart grid domain. From a list of initiatives, good practices, standards and schemes, only the items that were in line with the needs described in chapter 2 have been selected. The selection criteria included answering the following questions;

1. Is it a standard that is actually applicable to smart grid devices/systems (Meaning that standards regarding general IT, or person certification are out of scope?)²¹
2. Is it a standard that applies to cyber security (meaning that safety and physical security is out of scope)?
3. Is it a standard that can support certification, audits and/or legislation (meaning that good practices and informative standards were excluded, as they cannot form the basis for certification)?
4. Is it a standard that is used in the EU (meaning that standards not used in EU were excluded, as there is apparently no support from EU Member States)?
5. Is the standard supported by public and private bodies (meaning biased or vendor based schemes were excluded)?
6. Is the standard superseded or incorporated by another applicable standard?

These criteria might be used in order to shape a European smart grid certification meta scheme which acts as an umbrella to all existing certification standards that are relevant to smart grid security. The reader, can get a detailed description of these criteria in annex G "Scheme mapping". Answering these questions yielded a list of available standards that are applicable to the smart grid domain²²:

Before going into more details concerning the available standards and schemes, we need to clarify the relationship between these two concepts: the process of certification is usually referred as certification scheme. This process uses a set of standards. As a result we can consider, that the standard is part or a subset of the certification scheme.

3.1 List of standards and schemes

ISO 9001

ISO 9001 is used as proof that an organisation works according to defined procedures to ensure quality. The security certification of a smart grid is a means to improve security, and is therefore also related to quality in the organisation. Although ISO 9001 is not a specific smart grid or security standard, its system to ensure quality within an organisation is a good starting point for connecting more cyber security and smart grid specific certifications. Therefore it can be used as an overall umbrella for attaching more specific certifications, and provides context to the position of the smart grid system in the organisation.

ISO/IEC 27001 & ISO/IEC27019

ISO/IEC 27001 is used for the certification of information security. It can be used to certify that there are appropriate high level policies and procedures in the organisation for developing, producing, building or operating smart grid systems and/or components. There is also IEC/ISO 27019:2013, which

²¹ It should be noted here that person certification is deemed out of scope for this document, as it focusses specifically on systems, and person certification is being addressed by another ENISA project. General IT is out of scope to ensure that the differentiating properties of smart grid systems are specifically addressed.

²² The reader might notice that some 'schemes' are referenced amongst the standards. This has to do with the fact that these 'schemes' are variations of well known standards.

provides guiding principles, based on ISO/IEC 27002, for information security management applied to process control systems as used in the energy utility industry, but this standard does only provides guiding principles, and no certifiable requirements.

IASME

IASME is a lighter version of ISO/IEC 27001 that is developed by CESG in the UK. It can be used for small and medium sized organisations in the UK that need to address information security, but where ISO/IEC 27001 is too complex and resource intensive to implement.

IEC 62443

IEC 62443 is a standard that is based on the ISA.99 standard and focusses on functional security. "Functional security" means that it will describe the functionality the system or component needs to possess, but does not address the technical implementation. It can be used to describe the functional security properties of a smart grid system.

It provides certification of industrial control systems (IEC 62443 part 3.3) and components (IEC62443; Part 4.2, is currently still in draft, so not certifiable yet)²³ there is however an initiative started in the IECEE²⁴ to extend certification for industrial components to IEC62443 in late 2015. The IECEE scheme does not however explain anything on how to address security certification specific details, and is mainly focused on mutual recognition and assessing tests performed at manufacturer side²⁵.

ISO/IEC 15408 Common Criteria (C.C.)

ISO/IEC 15408 is commonly called "Common Criteria" and sometimes abbreviated to "C.C." It is a framework in which computer system users can specify their security functional- and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and security evaluation laboratories can evaluate the products to determine if they actually meet the claims.²⁶ It can be used in the smart grid to verify if a product meets the claims regarding the technical implementation of those security functions.

CPA

CPA is a UK based approach for gaining confidence in the security of commercial products. It is intended to complement or sometimes replace other approaches such as Common Criteria. CPA is currently only used in the United Kingdom.

CSPN

CSPN is a French scheme defined by ANSSI (Agence nationale de la sécurité des systèmes d'information) that aims to provide a first-level security certification for IT security products. Its scope is similar to the vulnerability analysis performed within Common Criteria. Its goal is to provide first relevant results in a less complex way than Common Criteria but without guarantee of completeness.

ISO/IEC 19790

ISO/IEC 19790, is a certification standard for security requirements for cryptographic modules (similar to NIST FIPS 140-2). It is used to validate whether the cryptographic core of any security product is

²³ <https://www.isa.org/pdfs/autowest/phinneydone/>

²⁴ <http://www.iecee.org/cbscheme/cbfunct.pdf>

²⁵ - http://www.iecee.org/ppt_presentations/iecee-peer-assessment.zip

²⁶ ENISA Protecting Industrial Control Systems - Annex III. ICS Security Related Standards, Guidelines and Policy Documents [Deliverable – 2011-12-09], available for download from the ENISA website; https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/annex-iii/at_download/fullReport

properly implementing technical details in accordance to the design and specification requirements laid out in the standard itself.

A more extensive description of each of these standards is provided in "Annex B: Schemes applicable to the smart grid domain", and a full list of all the evaluated standards and Schemes is shown in Annex C: This annex also shows the reason why a particular scheme or standard was excluded.

Each certification standard has some specific properties that are applicable to a specific field of application. Below are the certification standards divided into the application fields, and described what specific properties are related to that field.

3.2 Meta-scheme

There is no uniform method available for putting together different certification schemes. There is a standard called ISO 17067 (*Annex F: ISO/IEC 17067 - fundamentals of product certification and guidelines for product certification schemes*) that provides properties for product certification schemes. But this is not a good base for mapping exercises, as it does not address the differentiating properties like practical implementation, and market reception of a standard or scheme. Therefore a different method has been used to map the schemes. The method used is based on a textual analysis of the information publicly available for each scheme, amended by the practical knowledge of the team about the schemes. Additionally, the ENISA research for cloud computing certification has performed similar research regarding cloud computing schemes,²⁷ and SM-CG has provided a document comparing some of the schemes found²⁸ that has been used for input as well.

To be able to map the different schemes, an analysis has been made regarding the available schemes by comparing the following properties:

Administrative details

- **Name**
- **Type**
- **Group/initiative/organisation**
- **Related documents**

Geographic relevance

- **Geographic relevance:** Worldwide, European, Subgroup of European Member States, and National.

Current maintenance and activity of the program working group

- **Status:** draft/final, version 1,2,3?
- **Publication date:** how actual is it, is it ongoing?

Program scope definition

- **Description:**
- **Target audience:**
- **Addressed Industry:**
- **Technical relevance of the methodology**
- **Product testing**
- **The heaviness of the program**
 - Resources needed,
 - Certification delay

²⁷ <https://resilience.enisa.europa.eu/cloud-computing-certification>

²⁸ SMCG Smart Meters Co-ordination Group 2 Privacy and Security approach - part II; Annual report 2013

- **Maintenance scheme definition for the program**

National and international accreditation body recognition

- **Recognition by accreditation bodies (ISO, IEC, other?) National and international;**
- **Definition of CB accreditation criteria**

Ability to evolve to a European certification scheme, from the current situation

Program stakeholder trust

- **Public private participation**
- **Information provision to stakeholders**
- **Use of proven methods and maintaining skills**
- **Defining security measures for the premises of developers / OAM actors**

Market drivers for the program

- **Economics:** The scheme includes measures to limit the cost and/or workload and/or duration of evaluation

The complete set of properties can define a meta-scheme, and it is part of the framework one can use to position and define the available certification and standards and schemes. The meta-scheme details regarding each examined certification standard is listed in “*Annex D.2 List of schemes*”.

3.3 Qualitative analysis of examined certification standards

There are several types of certification standards and schemes which are categorised according to the following certifications:

- Operation certification
- System (functional) certification
- Development certification
- Component certification

The following sections provide the general descriptions and main differences amongst these standards. Please see “Annex D: Scheme mapping” for a more detailed table with descriptions and comparisons.

3.3.1 Operation certification scheme

Operation certification revolves around the certification of the operation of a process according to a defined standard. It is not uncommon for a company to be certified for operation, as it is commonly used to enforce trust in the operating capabilities of a certain company.

Examined operational certifications are:

- ISO 9001
- ISO/IEC 27001
- IASME

The following unique and differentiating properties apply to operation certification:

- It focusses on a management system or management of a process
- The certification is based on documentation and audits as proof for operating according to a certain standard.

3.3.1.1 Qualitative analysis conclusion

ISO 9001 provides an auditing and certification possibility about properly documenting what processes are implemented. ISO/ IEC 27001 seems to be an international standard that is widely recognised in Europe. IASME provides a good example of a light version, but is only available as an UK based scheme.

3.3.2 System certification scheme

System certification revolves around the certification of a complete (smart grid) system, including the system hardware components, software configuration and related procedures according to a defined standard.

It is in practice difficult to maintain system certification, due to the fluent nature of a smart grid system, and static nature of certification. As a system usually is not a static entity, there will be changes and additions made during its lifetime. Certification relies usually on the fact that a certain snapshot of a system is made, and a certificate issued will apply to that specific snapshot. Any change to the system (good or bad) will invalidate the certification. Making the certification a potential cumbersome and costly task, that can discourage improvements.

Examples of system certification are: IEC-62443-3-3 (SSA)

IEC62443-3-3 provides a good overview of what aspects can be addressed in system certification.

Properties observed in system certification:

- Components are integrated into a single system.
- May consist of multiple Security Zones.
- The certification is based on a complete system, including components, configuration, procedures and people. A combination of certified components, people and procedures is used to create a chain of trust.

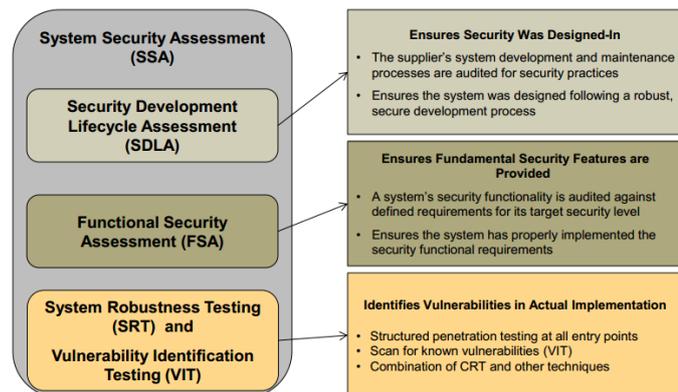


Figure 1 - IEC 62443-3-3

3.3.2.1 Qualitative analysis conclusion

There is a certification scheme for IEC 62443-3-3 called ISASecure. However, there is no certification body in Europe that supports it at this moment. Regarding smart grid systems, no other formal security certification schemes have been identified.

3.3.3 Development certification scheme

Development certification schemes are characterised by the certification of a process. The goal is to provide proof that the method used to develop a certain smart grid system, -product or -component is in line with standards.

There are multiple schemes that focus on development certification, or include it as an aspect. Especially in the field of cyber security, there is recognition for development certification as a means of providing trust in a certain product.

Examples are:

- ISO9001
- IEC62443-2-4 (Installation and maintenance requirements for industrial automation control systems suppliers, no certification available yet, since it is still in development)
- IEC62443-4-1 (ISASecure certification of product development requirements)²⁹
- CPA addresses criteria regarding secure development
- CC addresses criteria regarding secure development
- CSPN addresses a few criteria regarding secure development

Properties observed in development certifications:

- Development certification is a process certification that applies to how a product is created
- It revolves around using certified people, and certified tools to create a chain of trust³⁰
- The validation is done with process, documentation and code audits.

3.3.3.1 Qualitative analysis conclusion

ISO9001 is a high level assurance standard that a company can use to seek adherence to a documented high level of quality. This quality standard can be used for developers of systems to prove they develop code according to documented procedures. Standards such as IEC 62443-2-4 and IEC62443-4-1 can be followed to prove suppliers also meet certain security requirements when developing a device or system, but the standards are in draft, so no formal certification is possible. Additionally Common Criteria and CPA contain aspects that address the development environment of products as well, but the level of detail differs per standard and/or security level. Finally, Common Criteria does not address the certification of people.

3.3.4 Component certification scheme

Component certification revolves around the certification of a single component or product, and it is focussed on the certification of a component or product according to a defined standard or set of requirements. The examined component certification standards are:

- IEC62443-4-2 (ISASecure certification, security requirements for industrial automation control system components).
- ISO/IEC 15408 C.C.
- CPA
- CSPN
- ISO/IEC 19790

Properties observed in component certification are:

- Available from a single supplier
- Supported by a single supplier
- Can be identified by a product name and version

3.3.4.1 Qualitative analysis conclusion

CPA and CSPN are national schemes for the UK and France that can be applied. IEC 19790 is only applicable for cryptographic modules, but is also useful for guidance on testing and product requirements. C.C. covers most aspects of CPA and CSPN. C.C. is international recognised and extendable but is a framework, and therefore depends on specific protection profiles for a specific

²⁹http://www.isasecure.org/PDFs/Articles-and-Technical-Paper-Folder/ISASecure_AssetOwnerViewpoint_Oct2013_v05.aspx

³⁰ Although this holds true only for a part of the schemes above mentioned

type of product, and a security level (Evaluated Assurance Level, EAL, please see “Annex B.1 Common Criteria (CC)”) for more detail. SM-CG provided a more extensive analysis on component certification for the smart meter³¹. IEC 62443-4-2 provides security requirements for industrial control components, but currently there is no official certification scheme associated with this standard, as it is still in draft form. ISASecure is a certification scheme for IEC 62443-3-3. However, there is no certification body in Europe that supports it at the time of writing this report. There is however an initiative started in the IECEE to extend certification for industrial components to IEC62443 in late 2015. But this scheme will initially focus on components.

3.4 How are schemes currently applied in the EU?

This section gives an overview of the implementation status of smart grid certifications across Europe. Then the key findings will be presented as a means of identifying what could be used as a base towards a more harmonised smart grid security certification practices framework.

The descriptions regarding the smart meter certifications have been taken from the SM-CG research performed in 2013.³² Other descriptions have been based on online sources, observations and minutes of meetings of standardization meetings of several standards (i.e. IEC 62351) that were attended by the authors’ team.

3.4.1 Germany

The German Ministry of Economy (BMWi) has mandated the Federal Agency for Security in Information technology (BSI) to develop a protection profile for smart meter Gateways. The protection profile is based on Common Criteria. The level of security has been defined EAL4+, which is similar to EAL level 4; methodically designed tested and reviewed, but augmented with vulnerability analysis requirements with more stringent conditions.

Besides this component certification, the energy companies in Germany have to be compliant with IEC/ISO 27001 by the end of 2015.

3.4.2 United Kingdom

In the United Kingdom the Department of Energy & Climate Change (DECC) has defined Security Requirements and an end-to-end security architecture.³³

The Security requirements are needed for the Commercial Product Assurance (CPA), a certification that is mandatory for all smart metering products in the UK. CESG (Communications-Electronics Security Group) provides smart metering security profiles according to the CPA scheme called “smart metering security characteristics”.³⁴ The production of these profiles has been coordinated by the DECC with input by a cross-industry working group.

The UK government also promotes Cyber Essentials³⁵. Cyber Essentials is a UK government scheme encouraging organizations to follow good practices in information security. It includes an assurance framework aligned with ISO27001 and IASME, and a simple set of security controls to protect IT. It was launched in 2014 by the Department for Business, Innovation and Skills.

³¹ SMCG Smart Meters Co-ordination Group 2 Privacy and Security approach – part II; Annual report 2013

³² source: SMCG Smart Meters Co-ordination Group 2 Privacy and Security approach - part II; Annual report 2013.

³³ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/65685/7339-exp-doc-support-smets1.pdf

³⁴ <https://www.cesg.gov.uk/servicecatalogue/Product-Assurance/CPA/Pages/Security-Characteristics.aspx>

³⁵ <http://www.cesg.gov.uk/servicecatalogue/cyber-essentials/Pages/cyber-essentials.aspx>

3.4.3 France

France is considering a certification scheme called CSPN (Certification de Sécurité de Premier Niveau), that is based on Common Criteria. The scheme is used for meters and data concentrator security certification. France is considering smart grids as specific Industrial Control Systems. A law was passed in December 2013³⁶ which allows the French Prime Minister to enforce legal requirements in order to increase the security level of critical infrastructures. The decrees related to this law are currently being drafted and should be published by the end of 2014. This will apply to smart grids as well as other critical infrastructures. ANSSI (Agence nationale de la sécurité des systèmes d'information) has also published a framework for classifying Industrial Control Systems and a set of technical and organisational rules applicable to Industrial Control Systems.

3.4.4 Other Member States and EFTA countries

The Dutch national organisation of DSO's "Netbeheer Nederland", has developed the Dutch Smart Meter Requirements (DSMR). Although security and privacy were not the primary focus of the initial specification, additional security and privacy requirements have been included to the updated DSMR. The Netherlands is considering developing a protection profile based on Common Criteria. They expressed their interest to collaborate on a European level.

Norway and Sweden have the intention to develop a protection profile based on Common Criteria.

SERTIT (Sertifiseringsmyndigheten for IT-sikkerhet) is currently representing Norway as a member of the international community called "Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)". Several EU Member States and EFTA countries have indicated to prefer a European wide harmonized security approach, but will define their own level of security. Additionally, Norway is also a member of the SOG-IS agreement.

In the industry, ISO 27001 is internationally recognized, and common in Europe.³⁷ Other standards mentioned in the energy industry are ISO27002 and IEC 62443 but no formal legislation or guidance is provided.

3.4.5 European cooperation for Accreditation (EA)

EA has been appointed by the European Commission to manage the accreditation infrastructure within the EU, EFTA (European Free Trade Association) and Candidate countries. It is a non-profit association responsible for defining, harmonising and building consistency in accreditation within the European region, with the aim of reducing barriers to trade, and contributing to protecting health, safety and the environment. EA ensures that national accreditation bodies operate in accordance with the requirements of Regulation (EC) No 765/2008.

³⁶ <http://www.defense.gouv.fr/portail-defense/enjeux2/politique-de-defense/la-loi-de-programmation-militaire-lpm-2014-2019/la-loi-de-programmation-militaire-lpm-2014-2019>

³⁷ <http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=AF#standardpick>

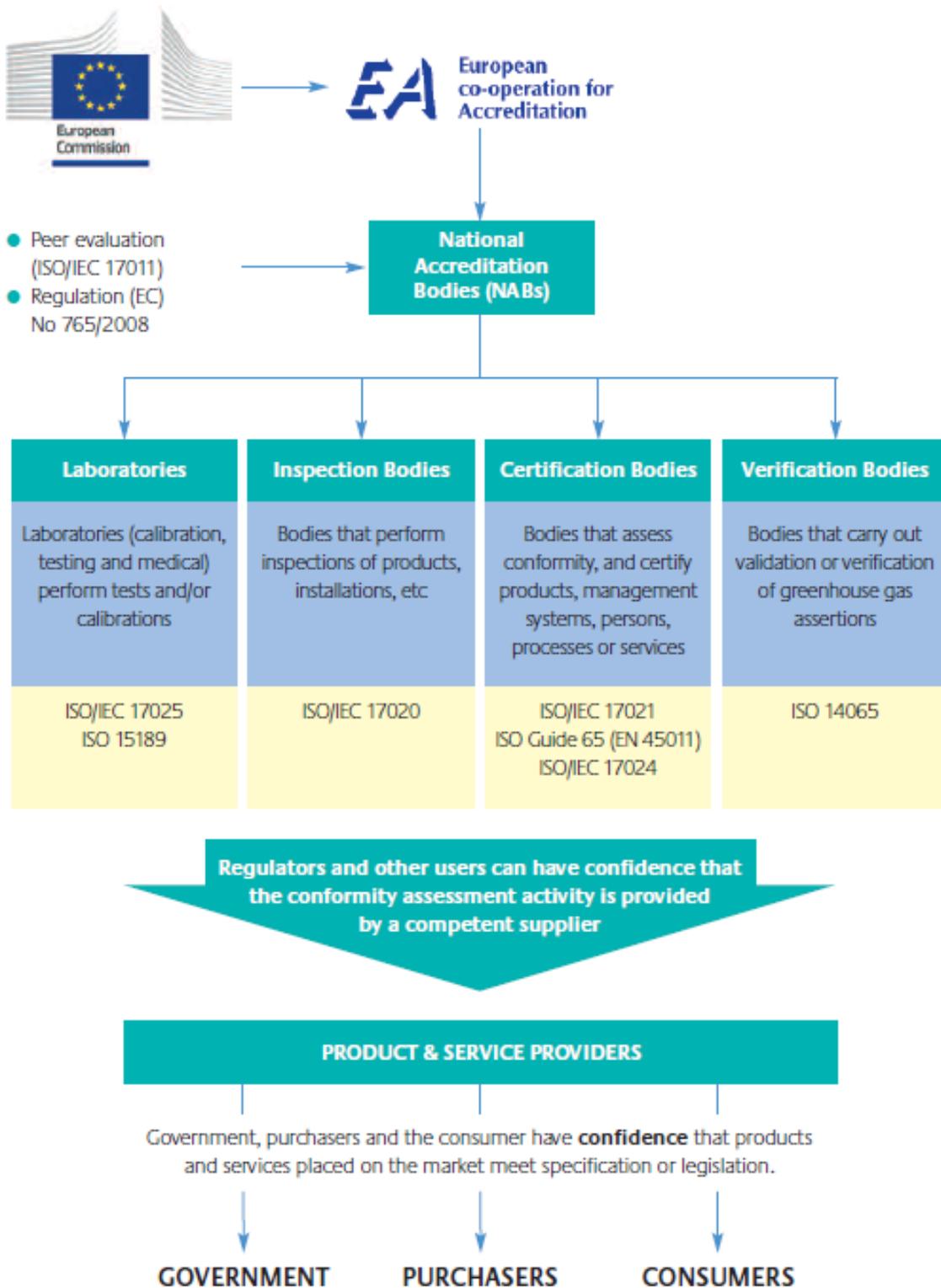


Figure 2 - EA scheme

3.4.6 SOG-IS

The SOG-IS (Senior Officers Group for Information Systems) is a Mutual Recognition Agreement (MRA) between the participants. The participants agree that IT products and protection profiles which earn a certificate can be procured or used without the need for further evaluation. It seeks to provide grounds for confidence in the reliability of the judgements on which the original certificate was based, by requiring that a Certification Body (CB) issuing Information Technology Security Evaluation Criteria (ITSEC), or Common Criteria (CC) certificates, should meet high and consistent standards.

The objectives for signing an MRA are:³⁸

- **Objective 1: Facilitating trade exchanges;** The potential advantages for economic players who wish to benefit from these agreements are as follows:
 - To make the regulatory process easier for introducing products on the importing country's market as far as the conformity assessment against the technical regulations of the importing country is performed before shipment (a reduction in the expense and time required to obtain product compliance with the importing country's technical guidelines, non-duplication of audits and inspections). Third-party conformity assessment of European products intended for export is conducted by one of the European bodies designated for this purpose (and vice versa).
 - Greater legal security and enhanced predictability in trade (fewer inspections conducted by authorities of the importing country in the exporting country).
- **Objective 2 : a tool for deregulation;** For products subject to third party conformity assessment procedures, mutual recognition agreements are clearly meaningless unless:
 - Conformity assessment bodies (CABs) have been set up with the necessary authority and technical competence to perform this work and are allowed to also perform on the basis of the third country's technical regulations;
 - The regulatory authorities decide to recognise the results of conformity assessment procedures issued by CABs located in the other party's territory.
- **Objective 3: a step for regulatory convergence;** According to the European Commission, mutual recognition agreements may have an educational impact: enhanced understanding of the technical regulations of the other contracting party and the experience gained in implementing these regulations in the context of the MRA agreement may be factors that could contribute to greater mutual understanding of each contracting party to the others' certification scheme details.

However, the usefulness is also limited due to:

- The recognition and acceptance by each of the Participants that this Agreement does not create any substantive or procedural rights, liabilities or obligations that could be invoked by persons who are not signatories to this Agreement.
- The recognition and acceptance by each of the Participants that this Agreement has no binding effect in national, international or European Union Law.

³⁸ Source: *MUTUAL RECOGNITION AGREEMENTS THEIR ROLE TODAY AND TOMORROW - a presentation on the role of mutual recognition agreements made at the Workshop on Standardization and Conformity Assessment Matters in the Transition Economies*

Please see “Annex H: SOG-IS” for more details.

3.5 Key findings

In Europe, only a few Member States (Germany, UK and the Netherlands) have developed specific security requirements for smart grid equipment. These initiatives have been developed in order to meet specific national smart grid needs and diverse national energy law requirements. As a result, there is diversity in the specifications for security requirements.

The shortage of security requirements and initiatives might be due to the fact that there is not a clear view of the amount of publicly known cyber incidents³⁹. Due to the unspecified number of incidents, there is no direct recognition of the necessity to improve cyber security from a corporate point of view. This lack of recognition is caused by the fact that private companies will not admit they had a cyber-related incident as this might damage their reputation. Additionally, cyber incidents are not easy to identify after the fact, as the systems often are too damaged or do not store enough data for effective forensic research to be carried out.

The identified smart grid security requirements focus on Home Area Network (HAN) and Grid-End applications. This is mostly due to the fact that, at the moment, the key driver behind the development of the smart grid, is the roll-out of the smart meters which are devices oriented to service end user needs. Based on the desktop research, the team couldn't identify security requirements for other than the HAN parts of the smart grid (e.g. substation automation and protection, EMS, DMS etc.) in European Member States.

Furthermore, the production process of these profiles varies among Member States; in Germany the profile has been developed by a public Authority (BSI) while in Netherlands the private sector has the leading role. This might have an impact on the acceptance level of the profile by the industry due to different degrees of private sector involvement in the security requirements' making process.

Although there are organisations supporting European wide certification such as EA and SOG-IS, there is no legislation enforcing a particular scheme.⁴⁰ Common Criteria have nevertheless been adopted in almost every country, although they are sometimes amended or replaced by other national schemes to support specific national needs. In some but not all European Member States there is some form of public-private participation regarding security certification for the energy industry. This situation also illustrates the difference in attitude among EU Member States, where some feel the need to instate legislation before EU mandates, while other Member States prefer to use the guidance of the EU to decide what scheme to adopt.

There is currently no harmonisation, there are different methods, schemes and different levels of security defined per Member State, but there is some synergy in the adopted schemes primarily based on the Mutual Recognition Agreement (MRA) concept. There have been national initiatives to improve cyber security for the smart grid by adopting a certain certification approach.

³⁹ Examples of root causes for such cyber incidents might include: human errors, system failures, natural phenomena, malicious actions and third party

⁴⁰ Germany is going to mandate ISO27001 in 2015.

4 A Chain of trust for the smart grid

4.1 The supply chain view of the smart grid

To be able to create trust regarding the security of the smart grid, it is necessary that the stakeholders are confident in the aspects deemed relevant. Certification is a formal means to create confidence, and thus trust in the relevant aspects, by means of a standardised validation process.

A typical supply chain as described in the needs (see 2.3) that can be applied to the smart grid domain is shown in Figure 3.



Figure 3 - Typical supply chain

It is important to note that a single certification scheme spanning across the entire smart grid supply chain is quite complex, and requires a lot of actors to work together. As such, a large scheme is usually too complex, in practice it is split up into separate schemes that are specific for the separate steps in the chain. To be able to trust this supply chain, certification can then be used to create a chain of trust. By ensuring that each step in the supply chain follows certain security rules, a trusted environment can be created, where it can be assumed that a system is being operated in a secure manner. However, if a step in the chain is compromised, it can cause a security breach, that could affect the rest of the chain as well.

Figure 4 shows a mapping of security certification on the smart grid supply chain.



Figure 4 – Supply chain certification

This chain can only be trusted if the certification scheme used for the certification itself is also trusted by the stakeholders. The trust in a certification scheme or lack thereof, is a common issue and there are multiple solutions to solve this. On a national level, trust in a scheme is commonly created by following guidelines such as ISO/IEC 17067 that is used for product certification schemes. (For a detailed explanation of ISO 17067 please see “Annex F: ISO/IEC 17067 - fundamentals of product certification and guidelines for product certification schemes”). This allows for the certification body that applies the scheme to receive formal accreditation by a nationally recognised accreditation organisation. Such a national organisation is subsequently recognised by an international forum of accreditation organisations, therefore effectively creating trust in the certification scheme. A similar hierarchy is depicted in **Error! Reference source not found.**

The process describing the details regarding accreditation, certification, related organisations and their interactions are detailed in “Annex E: Description of accreditation and certification”.

4.2 Analysis of the smart grid chain of trust

This section provides a definition and reference model of a chain of trust for the smart grid. Then it explains how the smart grid can be mapped on existing security certification standards and practices using this chain of trust. Additionally it describes how a risk based analysis can define the level of security of a smart grid, and how a smart grid certification scheme can be validated.

4.2.1 Certification and the chain of trust

“Figure 5 - Smart grid chain of trust” is a depiction of the complete supply chain for a system in a smart grid environment⁴¹ based on the analysis of the smart grid stakeholders involved in development, production, integration and operation, and the model outlined by the standard IEC 62443 (please see B.6 IEC62443 for details on this standard and its relevance to the chain of trust concept).

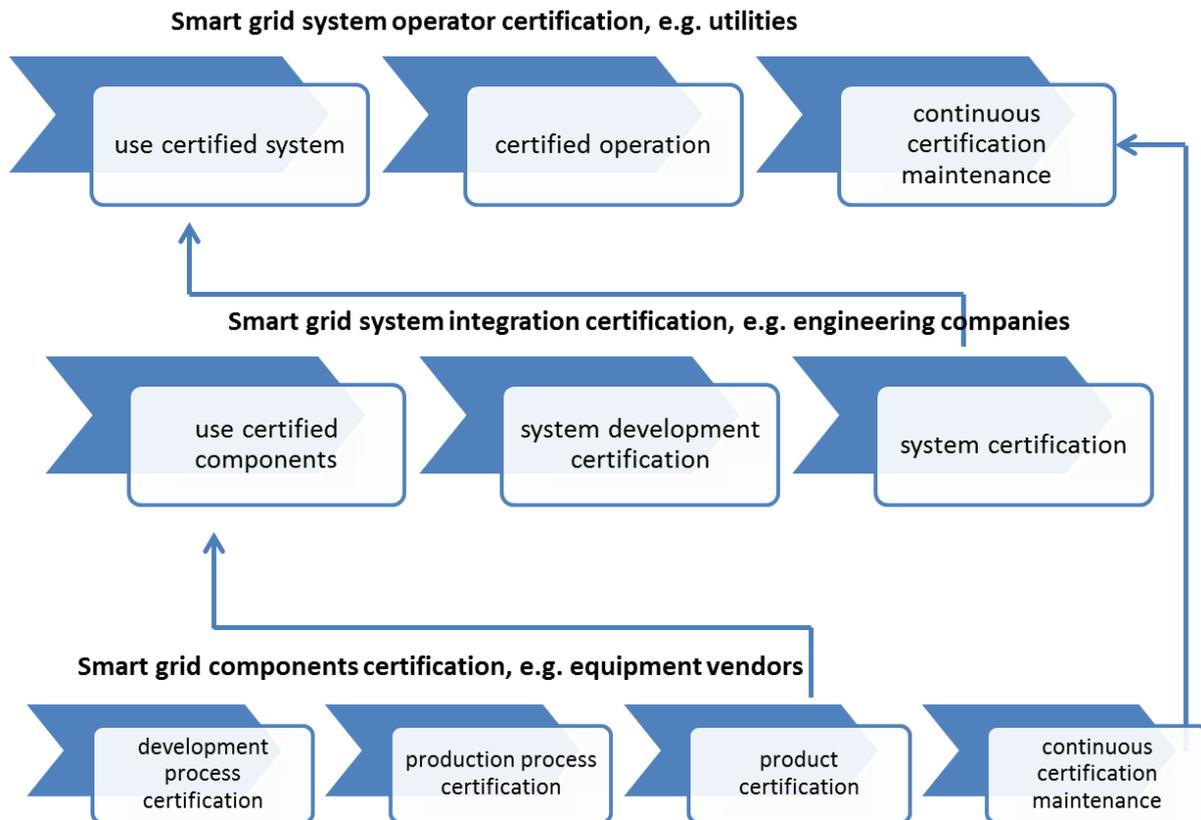


Figure 5 - Smart grid chain of trust

According to this model certification takes place at three levels:

1. Smart grid operator certification.
2. Smart grid system integration certification
3. Smart grid component certification,

A smart grid may suffer from complexity in respect to system design, which makes it different to standard ICT components as far as certification is concerned. A smart grid is geographically spread over a large area and there are multiple interconnections on different parts of the system. A smart grid can communicate with a Home Automation Network (HAN), Decentralised Energy Resources (DER) or an energy trading system. These interconnection can occur on numerous parts of the system, and exchange low or high level data with parties that can have different levels of trust. These interactions should not affect the chain of trust, and this is theoretically feasible as long as guidelines and best practices for third party interconnections are respected and implemented in line with NIST IR 7628 and ISO27002.

⁴¹ It should be noted that such a system does not encompass the complete European smart grid, but will be a system that is a part of it. The system described here has a system responsible, and will interact with other smart grid systems on different abstraction levels.

Cyber threats evolve over time. Vulnerabilities in hardware and software and new attack factors are a reason of daily concern. There is need for continuous certification maintenance to stay up to date with the latest known attack factors. This need is recognised by the stakeholders (see 2.3) and the certification lifecycle will need to be taken into account when looking at what should be certified. “Figure 5 - Smart grid chain of trust” includes the lifecycle by taking into account component and system maintenance in the form of the block ‘continuous certification maintenance’. Maintenance is commonly reviewed by equipment vendors who supply patches, and smart grid system users, who apply patches and expand on the system. System integration does not commonly include a maintenance scheme, as it is normally applied as a project with a discrete deliverable (e.g. deliver a working system x at date y). Therefore continuous certification maintenance for system integrators is left out of this figure.

4.2.2 Adoption of SG-AM for a chain of trust model

The SG-AM Framework and reference model aims at offering support for the design of use cases for smart grids. Support takes place by following an architectural approach which allows for a representation of interoperability viewpoints in a technology neutral manner for both current smart grid implementations and the implementations of the smart grid rolled out in the near future.

The SG-AM model can be applied for individual and interacting entities across the smart grid domain, and provides insight on how a stacked layer of security, can provide a layered approach for smart grid security. It relates back to the defence in depth strategy, where secure components (component layer), secure communication between components (communication layer), and a secured information and function layer, provide a layered model of smart grid cyber security. It also provides insight where security standards possibly overlap or complement each other.

It can be concluded that SG-AM meets the requirements for different certification standards for smart grids. Existing certification schemes address the issue of certification of smart grid chain elements (see Figure 6) separately. “Figure 6 - chain of trust model” shows an interpretation of the SG-AM model combined with the earlier introduced chain of trust (Figure 5) that can be used to map different standards and schemes suitable for smart grid security certification.

A chain of certificates which covers all aspects depicted in Figure 5 (e.g. vendor development, production and product security combined with secure system development, and secure operation) supports the enhancement of trust for the whole smart grid supply chain.

The level of security that is covered by the individual certificates can then be related to the place of the certificate in the value chain and the SG-AM model, and the role it will fulfil within the smart grid chain. This means that the model below can be used to give insight into dependencies, how certificates relate to each other in the smart grid, and provide a means to assess the impact of the security level used in a specific part.

It can also be used to provide insight into how security should be mapped on a specific SG-AM use case. For example, when a SG-AM use case is created for a smart meter chain, the SG-AM use case model can help in mapping the types of certification required to build a chain of trust within the smart meter SG-AM use-case. This approach provides a way to relate an SG-AM model based use case to specific certification schemes, and provides context to the coverage of an, existing or to appear, smart grid related certification scheme.

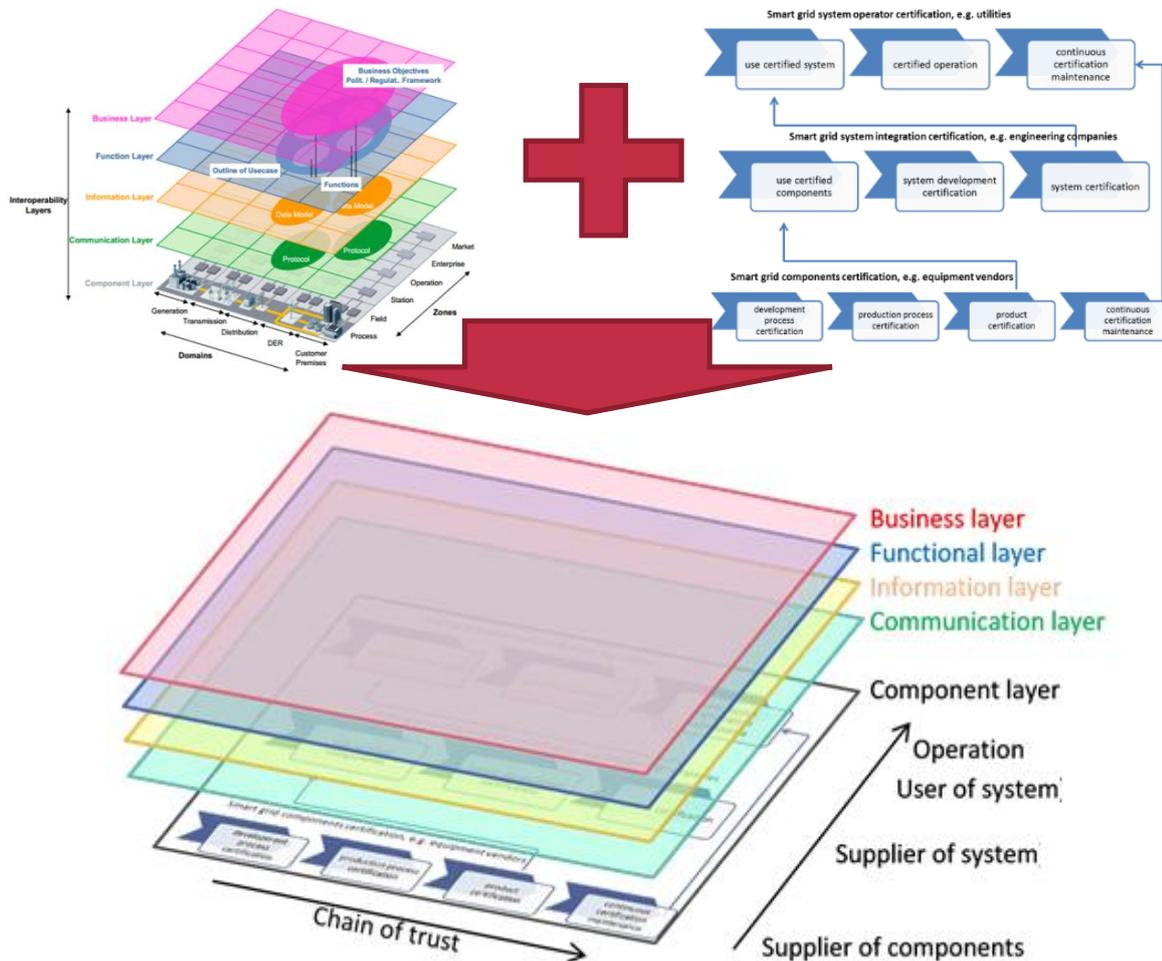


Figure 6 - chain of trust model

The model in Figure 6 is a graphical representation of how the described chain of trust could be applied to an SG-AM use case. This image seems to imply that the complete chain should be applied for each layer, for a complete security certified smart grid, but the SG-AM model was not intended to describe a complete smart grid prototype, but provides a method to create a common reference model for a smart grid use case. Only after such a SG-AM use case is defined the suggested chain of trust model described in figure 5 can be applied for each layer in the use case.

It should also be recognized that the model does not imply that the SG-AM use case and its related layers are in an one-to-one relation with the layers of the chain of trust model. It is merely a graphical representation that demonstrates the different levels where different certification schemes can reside; these layers are not meant to be fully aligned with the layers used in the SG-AM model.

4.2.3 Security requirements

Having defined the reference model, the next step towards more harmonised smart grid security certification practices is to define the security requirements of European wide technical communities (e.g. EURELECTRIC, ESMIG). There are only three⁴² identified sets of security requirements in the European market. The definition of these requirements is beyond the scope of this document, but

⁴² Germany, the Netherlands and UK, see section 3.5

could be based on profiles like the Common Criteria protection profiles or the CPA Security Characteristic.

4.2.4 Definition of risk levels aligned with the SG-IS framework methodology

To be able to minimize the cost of certification, one can take into account the criticality of the component subject to certification. This way, the proper level of depth and thoroughness of evaluation can be determined. A risk-based approach can help to focus certification efforts on smart grid use cases, and therefore provide insight into the appropriate level of security. Additionally, a European approach for the level of security will facilitate in a common reference model for all Member States. This section will describe an approach of how the M/490 SG-IS framework can help to answer the question "what to certify?".

In 2012 the Smart Grid Information Security (SG-IS) working group of the Smart Grid Coordination Group (SG-CG) provided a methodology to help define security requirements through a Use Case based approach. The SG-IS toolbox provides Smart Grid Use Case stakeholders an easy and pragmatic way to identify their security needs and identify gaps in use case recommended standards to deploy security requirements as needed. In 2014 this is renamed to the SG-IS framework. The use case model utilized by SG-IS is based on the SG-AM framework, and is therefore usable to perform risk assessments on SG-AM use cases. Therefore it is a useful methodology to align with when defining the risk levels within the chain of trust.

The SG-IS framework describes in detail how to assess use cases, lists the relevant assets categories and identifies a model for determining the Risk Impact Level (RIL) of specific information assets in a use case. The following picture summarizes how the methodology is intended to be applied.

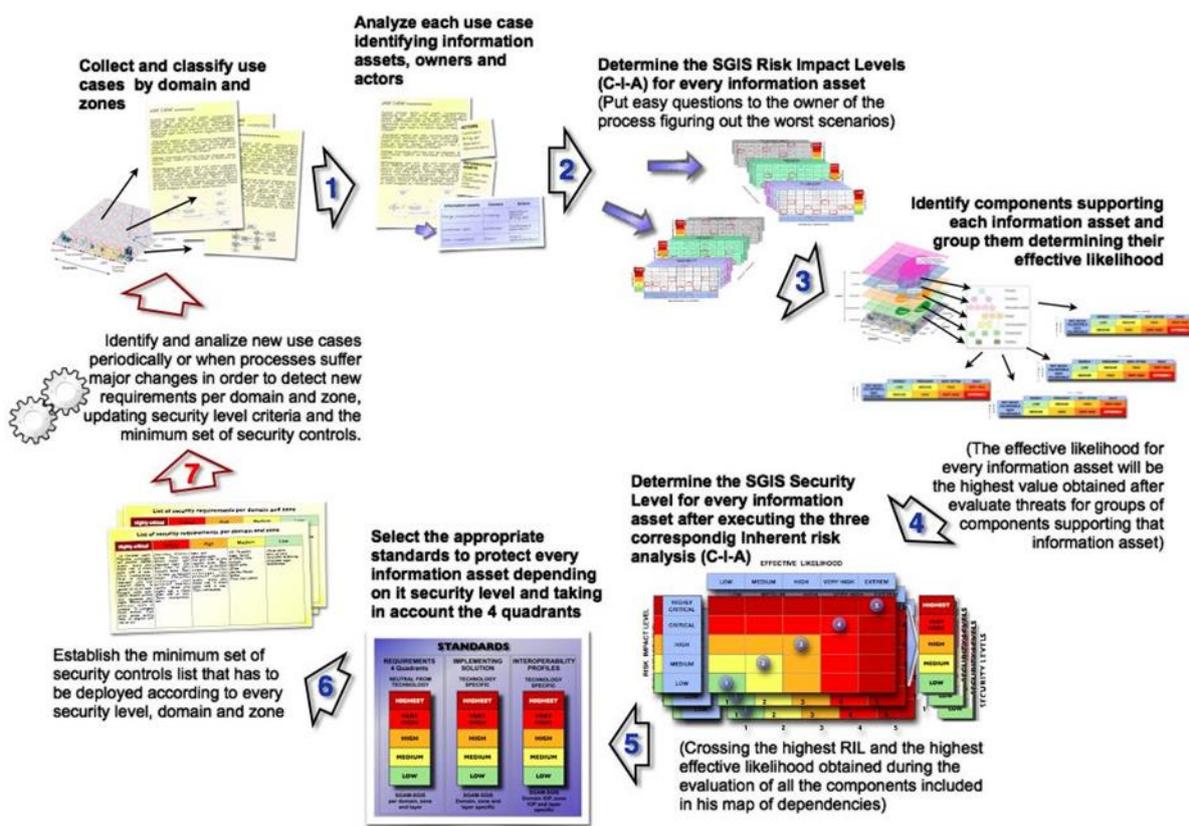


Figure 7: Methodology for security requirements definition

Using the SG-IS methodology can help to focus certification efforts on the smart grid use case with the highest risk impact level.

4.2.4.1 Risk impact levels

The Risk Impact is established by analysing how incidents related to a particular information asset affect the process where it is involved. Different incidents produce different impacts, so the highest impact identified in all the possible scenarios determines the Risk impact level for the analysed information asset. The result is expressed in a scale from 1 to 5 where level 1 is the lowest possible and 5 the highest risk impact level.

4.2.4.2 Risk Impact Categories

Security incidents against information assets affect their involved processes in different ways. The SG-IS Impact Analysis methodology identifies six different types of affectation or categories. Categories should be evaluated independently using the scale defined above (from 1 to 5).

There are six categories that are evaluated in this process to identify the risk impact produced by security incidents. Two of these categories are subdivided in subcategories. More categories and/or subcategories could be added at this level in order to get a deeper and more specific risk impact analysis in smart grids. The figure below shows the described categories criteria and its risk impact levels:

RISK IMPACT LEVELS	HIGHLY CRITICAL	regional grids from 10GW	from 10 GW/h	from 50% population in a country or from 25% in several countries	international critical infrastructures affected	not defined	company closure or collateral disruptions	direct and collateral deaths	permanent loss of trust affecting all corporation	>50% EBITDA
	CRITICAL	national grids from 1 GW to 10GW	from 1 GW/h to 10GW/h	from 25% to 50% population size affected	national critical infrastructures affected	not defined	temporary disruption of activities	collateral deaths	permanent loss of trust in a country	<50% EBITDA
	HIGH	city grids from 100MW to 1GW	from 100MW/h to 1GW/h	from 10% to 25% population size affected	essential infrastructures affected	unauthorized disclosure or modification of sensitive data	finances from 10% of EBITDA	direct deaths	temporary loss of trust in a country	<33% EBITDA
	MEDIUM	neighborhood grids from 1MW to 100MW	from 1MW/h to 100MW/h	from 2% to 10% population size affected	complimentary infrastructures affected	unauthorized disclosure or modification of personal data	finances up to 10% of EBITDA	seriously injured or incapacity	temporary and local loss or trust	<10% EBITDA
	LOW	home or building networks under 1 MW	under 1MW/h	under 2% population size affected in a country	no complimentary infrastructures	no personal nor sensitive data involved	warnings	minor accidents	short time & scope (warnings)	<1% EBITDA
		Energy supply (Watt)	Energy flow (Watt/hour)	Population	Infrastructures	Data protection	other laws & regulations	HUMAN	REPUTATION	FINANCIAL
	OPERATIONAL (availability)				LEGAL					

MEASUREMENT CATEGORIES

Figure 8 - The risk impact evaluation table measures impact levels on SG process for one specific asset

The SG-IS Framework provides a way to identify security requirements for specific Use Cases and SG assets. Then the asset owner can determine the level of security for his asset, based on the methodology proposed and the risk appetite, by using the SG-IS framework.

As both the SG-AM model and the SG-IS framework are recognized by Member States as an accepted approach for describing the smart grid and the relevant risk levels, they provide a good basis for a European framework which contributes to more harmonised smart grid security certification practices.

Combining the two (SG-AM and SG-IS), one can build a chain of trust for a specific national use case, as well as the level of security needed for this use case. This way a Member State can describe its own use case and perform a risk assessment, both based on an accepted EU methodology.

This is an important piece of the framework for smart grid security certification, as it addresses the following needs;

- A common reference model for security in the EU.
- An agreed method for the level of security for different criticality aspects of the grid.

The next step is then to define how the level of security for each part of the chain of trust is to be evaluated. For this, existing certification schemes can be selected on national level. Based on the national use cases stakeholders can take decisions regarding scheme implementation, specific requirements, and validation activities.

4.3 Conformity assessment and its relation to testing

To be able to certify the security of the smart grid, asset owners will need to provide proof that security requirements set by the technical committees are met. Such proof is usually generated by assessing (or testing) the conformance to this set of security requirements. In this respect conformity certification, conformity assessment and testing are commonly used interchangeably. To understand what certification is, and how it relates to terms such as conformity assessment and testing, this section explains their relation. For a more in depth view, please see Annex G: Conformity assessment and testing. Additionally, ISO provides a comprehensive overview online: http://www.iso.org/iso/casco_building-trust.pdf.

Conformity assessment can be undertaken by the supplier of a product or service, its purchaser and other parties who might have an interest such as insurance companies and regulatory authorities. It is convenient when talking about conformity assessment to refer to the parties as follows:

- First party (1st party) – the person or organization that provides the object which is being assessed;
- Second party (2nd party) – a person or organization that has a user interest in the object;
- Third party (3rd party) – a person or body that is independent of the person or organization that provides the object, and of user interests in the object.

A 1st party conformity assessment is perceived as less trustworthy than a 3rd party assessment. Therefore, in relation to the risk that nonconformity poses, a choice is made to what parties are allowed to perform the assessment. An SG-IS framework aligned approach (described in section 4.2.4 4.2.1) can help to decide the risk for a specific scenario and associated assurance level.

The following items are the most common conformity assessment activities.

- **Inspection** is the examination of a product design, product, process or installation and the determination of its conformity with specific requirements or general requirements.
- **Certification** by a certification body formally establishes that a product, service, organization or individual meets the requirements of a standard after evaluation.
- **Accreditation** provides independent attestation of the competence of an individual or an organization to offer specified conformity assessment services (e.g. testing, inspection or certification).
- **Testing** is the determination of a product's characteristics against the requirements of the standard. Testing can vary from a non-destructive evaluation (e.g. X-ray, electrical, etc.) after which the product is still fit for use, to a destructive analysis (e.g. chemical, mechanical, etc.) after which the product is no longer fit for use.

There are different types of aspects that can be focussed on while testing. The most common are:

- **Conformity testing:** testing to assess the compliance of the test subject to standardised requirements.
- **Functional testing:** testing to assess the ability of the test subject to provide the functionality that is required by the assessment. The required functionality of the test subject is usually described in a standard that the assessment refers to when performing the tests.
- **Interoperability testing:** testing to assess the ability of two or more systems to exchange information and to make mutual use of the information that has been exchanged.⁴³

With respect to smart grid cyber security, all three aspects play a role. Conformity testing needs to be performed to ensure that smart grids comply with requirements set by the EU, Member States and users of smart grid systems.

Functional security testing needs to be performed to support the implementation of cyber security in the grid, as conformity testing normally does not focus on the validation of security functions that the device can support. For example, the conformity security requirement is for a device to have access control, but the functional security requirements can be that access control should work in a specific manner.

Interoperability testing is an important aspect of conformity assessments of communication standards. For example, an encryption mechanism needs to be interoperable between smart grid devices to be useful. If interoperability testing is skipped for an encrypted communication channel, the system can be conforming to all security requirements, and have been functionally tested, but can still not be able to use the encrypted channel because the devices are not interoperable.

Penetration testing

A more specific form of testing that is common in security tests is penetration testing. This type of testing revolves around the exploitation of possible design flaws and weaknesses to compromise the security of a device. Such tests do not focus on a specific test book, but rely more on the creativity of the tester, and the time there is available to perform a penetration test. Penetration testing can be incorporated as part of a functional test, by describing it as a negative test case for a functional requirement. For example, the validation by the following functional requirement can be tested by a penetration test; "the device under test shall not provide means to circumvent the access control mechanism". Such a requirement can be validated by a negative test scenario, where the device will be subjected to a penetration test in an attempt to circumvent the access control mechanism.

A successful smart grid cyber security certification practices framework will need to include all 3 topics, conformity testing, functional testing and interoperability testing. It should also address penetration testing as part of the functional tests. Depending on the potential severity of the security risk if a product is not conform, it can be decided to perform first, second or third party assessments. However, in practice, only third party certification is seen as trustworthy for most cyber security schemes.

The different conformity assessment techniques can be combined with the Risk Impact Levels described in the previous section. This way, it is possible that some certification cost can be decreased because it is expected that less critical devices might not be subject to certifications but to less expensive conformity assessments (see annex G for a summary on conformity assessment and testing).

⁴³ ITU-T Z.450 - Quality aspects of protocol-related Recommendations - <http://www.itu.int/en/ITU-T/publications/Pages/structure.aspx>

4.4 Description of certification scheme relations loosely based on SG-AM model

This section describes a loosely based mapping of security certification schemes, related to the chain of trust model described in section 4.2.1. It is not possible to exactly map the schemes to the SG-AM model, as it would not provide a picture that does justice to the scope of the different certification approaches. Therefore the domains in the original SG-AM model have been replaced by stages in the product lifecycle; **development, production, operation and maintenance**. The zones in the SG-AM model have been replaced by the product ownership stages that a product goes through during **production, integration, acceptance and operation**. In this way the model should provide guidance of where to place a certification scheme in the smart grid chain of trust. The layer definitions from the SG-AM model have been kept intact, and should help to understand the level of abstraction of the standard.

The following layers are described by the SG-AM model:

- Business layer
- Function layer
- Information layer
- Communication layer
- Component layer

Below follows a description of each layer generally aligned with the SG-AM model⁴⁴, and suggested which of the identified certification schemes can be applied to that layer.

⁴⁴ SG-AM model described at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf on page 27

4.4.1 Business layer

The business layer represents the business view on the information exchange related to smart grids. SG-AM can be used to map regulatory and economic (market) structures and policies, business models, business portfolios (products and services) of market parties involved. Also business capabilities and business processes can be represented in this layer. In this way it supports business executives in decision making related to (new) business models and specific business projects (business case) as well as regulators in defining new market models.

On the business layer, the focus of security is around the business- and corporate regulatory processes. They are high level, and provide controls for management and decision makers that can be used to steer and implement more detailed procedures and technical requirements.

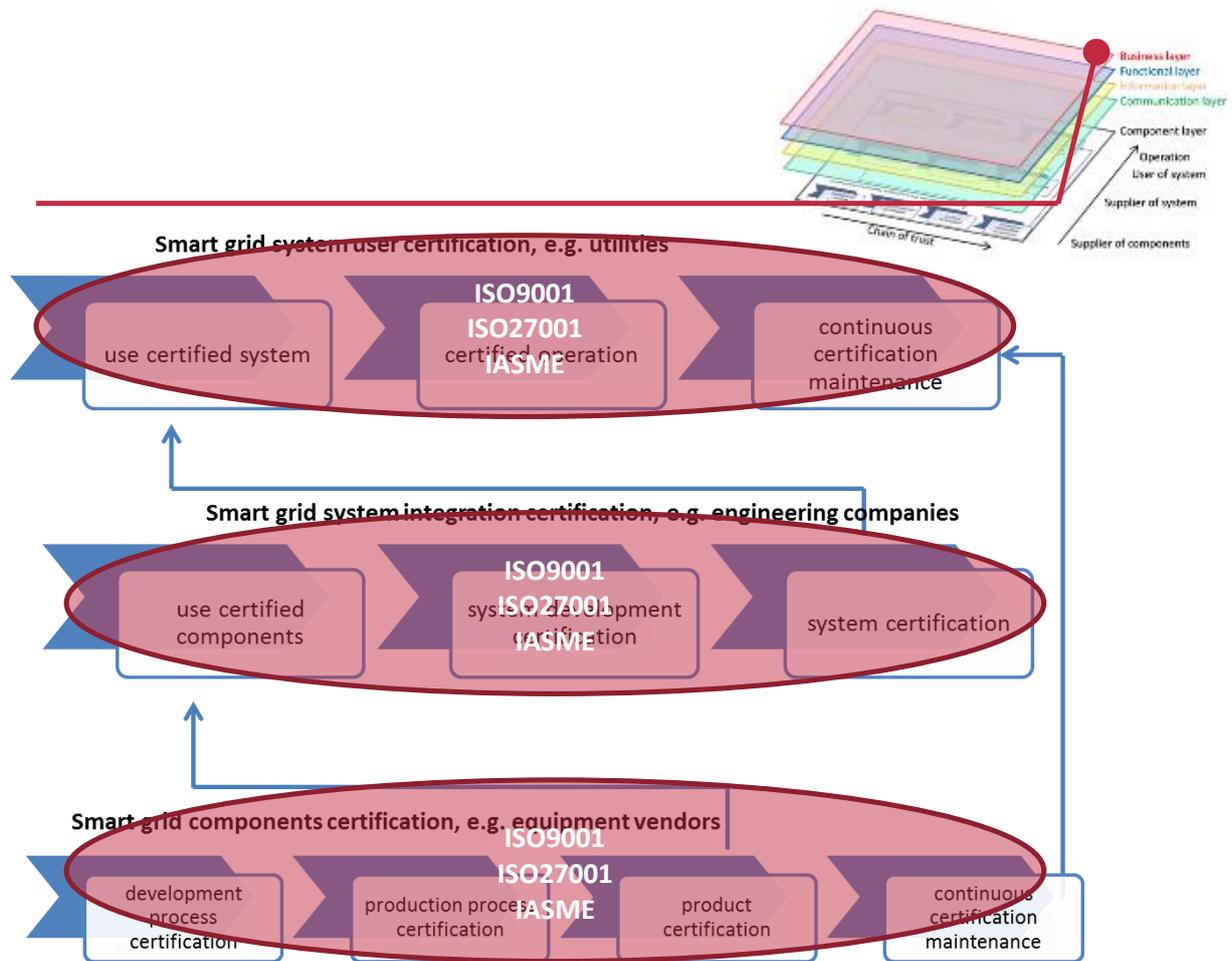


Figure 9 - business layer

4.4.2 Functional layer

The functional layer describes functions and services including their relationships from an architectural viewpoint. The functions are represented independent from actors and physical implementations in applications, systems and components. The functions are derived by extracting the use case functionality which is independent from actors.

IEC 62443 provides requirements and guidance for security functions for industrial control systems. Unfortunately not all parts of the standard provide formal certification schemes. Additionally, the standard focusses on security requirements and design, but does not go into detailed descriptions of components and communication protocols. Below is a mapping of the different parts to the trust chain.

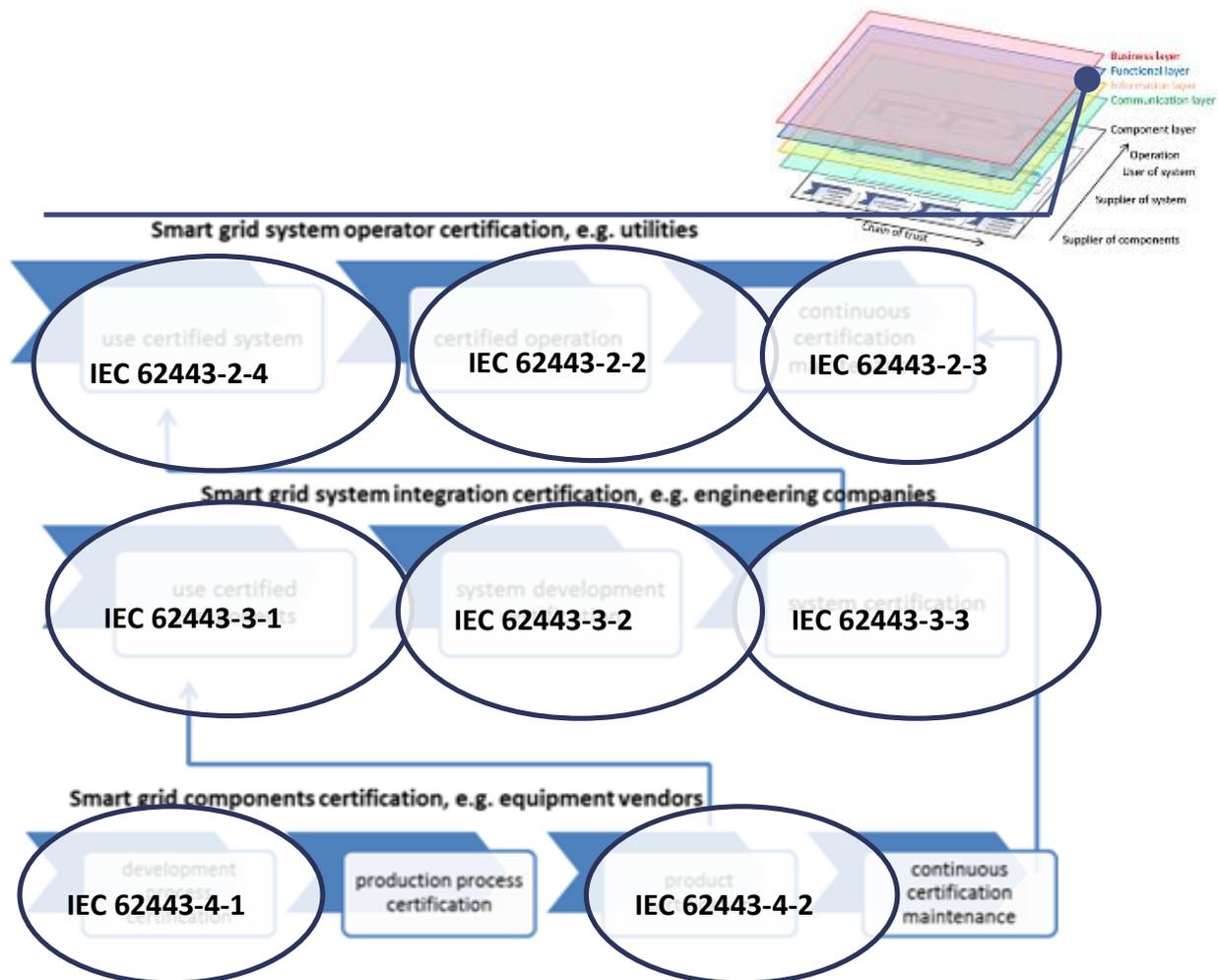


Figure 10 - Functional layer

4.4.3 Information layer

The information layer describes the information that is being used and exchanged between functions, services and components. It contains information objects and the underlying canonical data models. These information objects and canonical data models represent the common semantics for functions and services in order to allow an interoperable information exchange via communication means.

On the information layer there is nothing available for the certification of security. Such certification would have to focus on securing the information exchange at the technical level. This encompasses

such aspects as configuration, data model and database encryption, but it could also address key generation, installation, distribution and daily handling of sensitive data. Data encryption in devices on information level is not very common in embedded system, unless it is a smart meter device (where readings and keys have to be stored secure). On computer systems it is possible, but no certification scheme is available.

4.4.4 Communication layer

The communication layer seeks to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models.

There are standards available for secure communication, such as IEC62351 and the DLMS/IEC 62056. These standards recommend the implementation of communication security measures such as encryption and authentication. But no certification schemes are available yet to formally test the security of device communication. Validation can be done for example in part by penetration testing, or more in depth by validating the communication security requirements. The validation of communication security requirements does not prove that all security requirements have been implemented, but only provides proof that the communication interface comply with the security requirements defined in the communication standards.

4.4.5 Component layer

The emphasis of the component layer is the physical distribution of all participating components in the smart grid context. This includes system actors, applications, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches, servers) and any kind of computers.

Component layer security focusses on security of the components used in the smart grid. It addresses the security of the individual components, focussed on hardware, software, and the functions the devices should support. Although most standards listed here will also take into account the higher level requirements, they have been listed here, as they are applied and validated from a single device/product and/or system perspective. The technical validation of communication between systems, secure information handling and secure system management is out of scope.

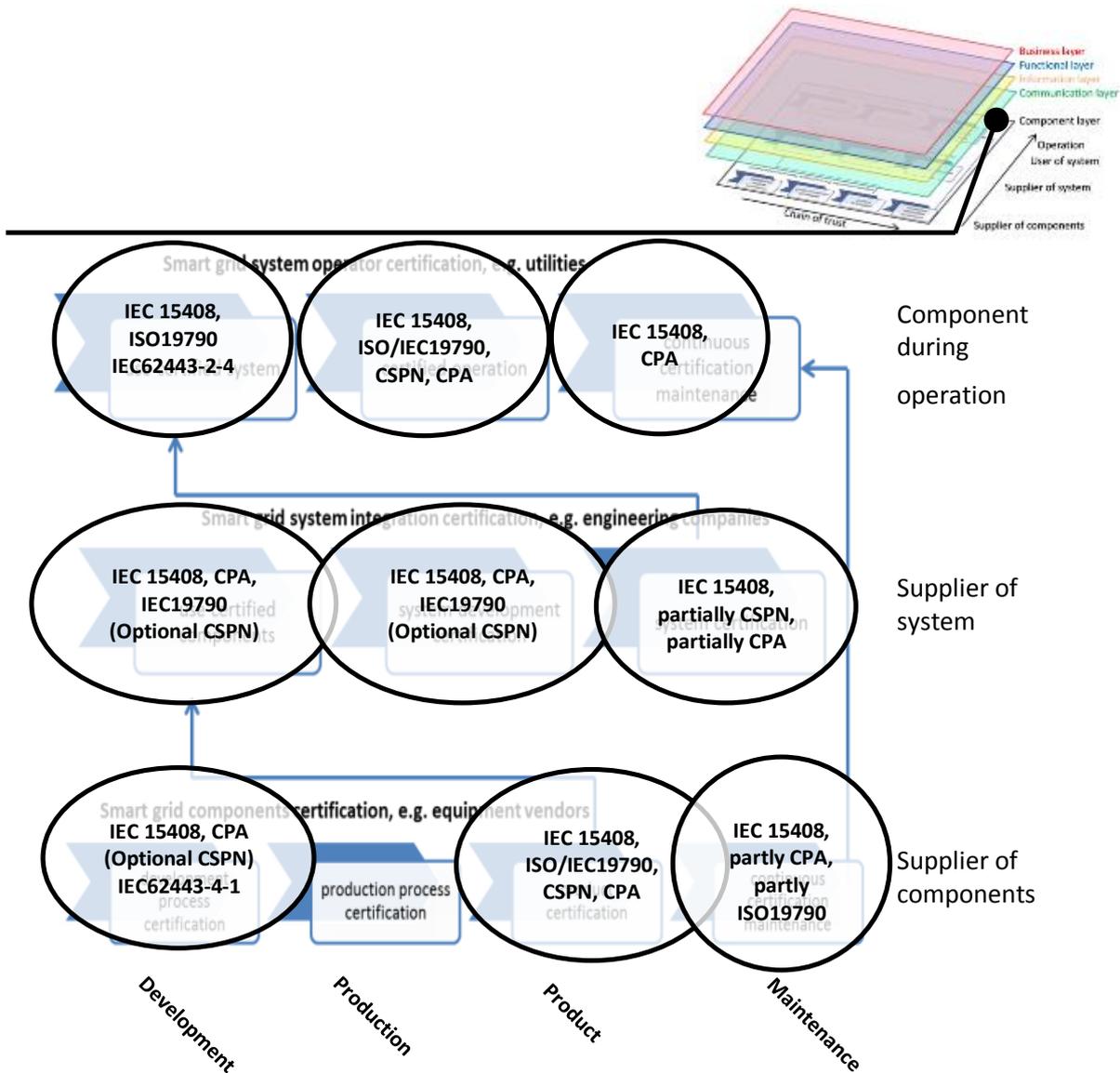


Figure 11 - Component layer

There is currently not one certification scheme that can cover all aspects of the smart grid. And there is also no combination of schemes that can be used to cover everything, as the communication and information layers do not have certification schemes that formally focus on these aspects.

But this does not need to be a major issue, as the practical implementations of the smart grid also do not cover every aspect of the SG-AM model. Additionally, several schemes mentioned can actually cover the parts described, if they are amended in line with profiles or standards and requirements in force.

Another important observation is that some standards like parts of IEC 62443 are not published yet, so they cannot serve as a basis for certification. Also there are currently no interoperability tests or certification schemes available for secure smart grid communication standards such as IEC 62351.

5 Gaps and Challenges

In respect to the needs described in chapter 2.3, the currently available and applied standards and schemes in the EU described in chapter 3, and the observations this report outlines the following gaps and challenges:

5.1 Gaps and challenges related to the needs

1. There is currently no established model for a smart grid **chain** of trust in the EU. It will be a challenge to create **consensus** about a chain of trust model. Although the concept is known, it has not been specifically adopted by any Member State in the context of smart grid certification. A chain of trust seems not to be explicitly mentioned in any complete certification approach. Only partial chains for the smart grid are supported for shared risk mitigation. It will be a **challenge to ensure** that **responsibility** of risk mitigation is properly assigned to the responsible party, as the interconnected nature of the grid makes it sometimes difficult to identify the accountable party in relation with a specific action.
2. A common **reference model** like SG-AM for smart grid security the is in line with SOG-IS is only available for components and operational parts; this however is not harmonized within nor adopted by all Member States. There is **no scheme** for the complete EU smart grid. Due to the large number and fragmented nature of the smart grid stakeholders, it will be a challenge to create consensus regarding a common reference model.
3. There is no common baseline **set of security requirements** that can be recognized by all participating EU Member States. Only three Member States⁴⁵ have defined their own protection profiles. These requirements are different per country, they do not focus on the whole grid but on specific parts of it (i.e. smart meters), based on different standards and adopted by technical committees (TCs). It will be **difficult** to create a common baseline, as multiple Member States adopted widely different approaches, and have different requirements and levels of security related to smart grids.
4. At European level **equivalent security and risk levels** are provided by the M/490 SG-IS framework but this is not formally recognized as an EU wide standard level for smart grid security. Recognizing the **M/490** SG-IS framework should be feasible, as it has been regarded by several Member States as a good reference model.
5. There are certification schemes for components and operation, but there is none for systems certification in Europe. There is **no scheme** that includes all aspects and enables a pan European approach. It will be a challenge to create a single scheme that includes all aspects of smart grid certification, as there are gaps and overlaps in the schemes that apply to a specific topic (please see chapter 4.2 for a detailed analysis).
6. Depending on the scheme and type of **testing**, procedures and methodologies are available, but detailed procedures are **fragmented** and not readily available for all smart grid aspects. Some certification schemes can overcome this by defining the test cases on a per-case basis.
7. Some schemes facilitate **public and private interaction** by including Technical Committee subgroups that could be useful on an EU level, but only for product certification. There is **no EU body** to facilitate public-private interaction. It will be a challenge to find an existing group of experts that can form a technical committee and having enough commitment to produce a workable scheme.

⁴⁵ Germany, the Netherlands and UK, see section 3.5

8. There is not a single scheme that can provide EU guidance for implementation, and supporting national legislation. There are some schemes that have been **mandated** by certain Member States that could also be applied at an EU level. There is no EU body to provide guidance for a scheme implementation and keeping the scheme up to date. It will be a challenge to **raise the maturity level** of all the Member States, as the amount of effort that is put in smart grid security differs per Member State (please see section 3.4 for the detailed analysis).
9. There is no **alignment** with smart grid definitions such as M/490 and only guidance for proper security measures on a national level that differ per Member State. As there is currently no harmonization, it will take **considerable effort** to create a harmonized approach that has consensus, but still complies with the desired scheme. Such an approach is necessary to facilitate the growth to a scheme that is geared towards service EU Member States' needs.
10. There are barriers and silos created by fragmented markets. There is no **harmonized** approach causing higher costs for certification per Member State. There are similarities among countries that can be used to create consensus, and a combination of schemes could be acceptable on an EU level, assisting in a lower cost. It will be a challenge to **keep cost to a minimum** while still providing security, as security is a topic that penetrates all aspects of a system, and therefore has to be widely implemented without directly providing a clear justification of the necessary cost and effort.
11. Some schemes include a **maintenance** scheme, but no harmonized approach or EU interface is available for all aspects of the smart grid. Additionally, there could be gaps with respect to life cycle coverage when they are analysed in more detail. It will be a challenge to create a **harmonized** maintenance and life cycle scheme. The available schemes do include one, but they do not relate to one another.

5.2 Gaps and challenges related to the desired properties

The analysis also includes the gaps regarding the additional properties of the desired scheme, as outlined hereunder:

Operational in a reasonable time

There are various scheme components available to support a single pan EU framework that can be rendered operational within a reasonable time frame. The organisation to maintain such a framework and harmonise the schemes related to smart grid security needs to be further analysed and appointed. Additionally, some of the standards such as IEC 62443 are still largely in draft stage and therefore in the current state they are not necessarily usable for certification. To become operational will be challenging in terms of consensus building and in creating all the background information to make the entire stakeholder group understand what and how to follow. Additionally, it will be difficult to get all standards published that are relevant, but currently still in draft such as IEC62443.

Recommendations based on accepted good practices

There are plenty of recommendations, but there needs to be a selected subset of them that is coherent and will be advertised as a single package for smart grid security in the EU. There are multiple standards that cover the same topics, but they sometimes address them on different abstraction level. It will be a challenge to create one set of recommendations with the right level of abstraction that does not overlap.

Easy to be adopted by the Member States

As the schemes adopted by different Member States vary, a gap lies in the utilisation of one harmonised scheme to make it easy to adopt. As several Member States have already taken steps in utilizing a specific scheme, it will be a challenge to create consensus regarding the adoption of one single approach, if that means stopping the national approach, and redoing certain activities.

Take into account new and existing technologies

Standards development is progressing slower than the evolution of security challenges. Therefore it is necessary to keep the level of a standard high to maintain its relevance in time. Technical subcommittees are then able to fill in the currently relevant security details by means of specifications. A good example of this approach is seen with the protection profile used in Common Criteria; Annex B.1 Common Criteria (CC). However, in the current situation the standards and schemes such as common criteria are present, but the smart grid specific protection profiles (with the exception of the smart gateway profile defined by BSI) and security use cases addressing the chain of trust are not available. It will be a challenge and a constant effort to create an environment where the baseline of security requirements grows with the technological advancements.

Self-certification tools

No pre-certification self-assessment tools have been identified during this analysis. It will be a challenge to provide self-certification tools because it is difficult to assess beforehand what smart grid use cases will be implemented, and to what level of detail a toolbox can assist in the implementation of the use case.

In line with the standardization efforts

The identified certification approaches are aligned with existing standards, used in the Member States, but there is currently no EU initiative for accomplishing this alignment for the whole smart grid supply chain. As already mentioned in chapter 4, the smart grid chain of trust involves several standards for the different smart grid layers. Alignment with several standards might be a challenge because of possible overlaps amongst standards and of different approaches in meeting the specified security requirements.

Not a single certifying authority

A single certifying authority should not be a problem while using ISO/IEC organizational frameworks including IAF, ILAC (please see "Annex E: Description of accreditation and certification" for an explanation) and national accreditation bodies. Not having a single scheme framework has advantages, but a growing number of certification bodies will also cause more administrative overhead and less control over the quality of the certification bodies and the evaluations they perform. It will require periodic audits that will have to be paid by one or more of the stakeholders.

Central certification storage

A centralized storage or public site for accessing smart grid certificates is not available. In the case of Common Criteria, it is maintained by the scheme itself. In the case of an EU based approach, it should logically be maintained by the EU smart grid security framework owner. Central storage needs to be maintained and updated to be useful. This cost money that will have to be paid in some form or another.

Partial certification

There are approaches that result in partial certification, by allowing the choice of what requirements will be complied to. This however reduces the amount of trust in the scheme in those particular cases (e.g. common criteria allows for the certification of a specific product configuration to a subset of requirements).⁴⁶ It will be a challenge to avoid trust issues regarding partial certification such as it

⁴⁶ <http://redmondmag.com/Articles/2003/03/01/Windows-and-Common-Criteria.aspx>

being perceived as a paper exercise. For example, the different levels below Common Criteria EAL4 are more paper exercises than real security tests.

This report also identifies additional challenges which can be found in “Annex I: Additional identified challenges”.

To summarise, there are numerous gaps and challenges that have been identified during the desktop exercise performed. Probably the most important one is that there is no single approach that covers all aspects of smart grid security certification. And even a combination of all schemes could leave gaps if they are not carefully combined. Additionally there are varying approaches and requirements in each Member State, and no coordination or harmonisation at European level.

6 Recommendations

This chapter provides an overview of all the recommendations based on the standard analysis, the current situation in the EU Member States, the desired situation and the gaps and challenges. The smart grid security certification recommendations refer to most of the challenges described above.

Recommendation 1: Appoint a EU steering committee⁴⁷ to coordinate smart grid certification activities

The European Commission should invite relevant stakeholders from both the public and private sector and mandate a EU steering committee with the aim to coordinate the EU smart grid certification activities with the following tasks:

- Providing oversight of smart grid security certification, security requirements definition, and coordination with national schemes.
- Enhancing the transparency and the trust of the smart grid certification activities by disseminating information and good practices on smart grid certification and providing centralised storage and publication of smart grid certificates together with the national schemes.
- Providing guidance and advice to interested parties on implementation of national schemes.
- Keeping the smart grid certification apparatus up to date regarding the latest threats, by using feedback from both the public and the private sector and lessons learned during the certification process.

Owner: The EU Commission should take action to request the formation of this steering committee.

Recommendation 2: Provide guidance and a reference model to implement a chain of trust

The EU steering committee should promote the concept of a chain of trust, similar to that described in chapter 4.2.1 that provides transparency and increases trust in the supply chain of the smart grid. A national use-case approach that is aligned with the SG-AM common reference model can be used as the basis for this activity. It should also have a set of common high level requirements that are recognized by all participating EU Member States. This common set of requirements can be amended by more detailed national requirements that address the specific use case details for a Member State on top of the commonly agreed ones. (Using SG-IS framework described in chapter 4.2.1)

Owner: The EU steering committee should provide guidance on how to implement smart grid security certification and the chain of trust.

Recommendation 3: Use of the currently available standards and schemes, and accommodating, better coordinating and harmonising national approaches

It is recommended that any approach to better harmonised security certification practices should be easy to implement by combining currently available standards described in section 3.1. This will facilitate the adoption by Member States and leverage the existing standardization efforts. A mapping exercise might take place in order to map and position different standards. This activity might take into account the properties described in section 3.2 together with the smart grid chain of trust.

Owner: The EU steering committee should perform a mapping exercise amongst available standards and schemes used in the EU.

⁴⁷ A voluntary committee is recommended.

Recommendation 3a: The steering committee should advise the Member States on how to map their preferred standard/scheme to the SG-AM

Chapter 4.4 provides a mapping of security certification schemes, related to the chain of trust model, to the SG-AM.

Owner: The EU steering committee should undertake to provide guidance and advice to Member States on how to implement the smart grid security certification framework.

Recommendation 4: Promote international recognition of schemes

Existing recognition agreements like SOG-IS (see section 3.4.6) should be utilised to create international requirements, and an international framework for certification.

Owner: The EU steering committee should ensure that certification schemes used, can operate at international level.

Recommendation 4a: Align with European accreditation bodies

Each Member State should use the European accreditation bodies to recognise its national scheme according to the EU reference model and use agreements like SOG-IS MRA for recognition of security certification bodies. This will ensure there is not a single certifying authority, and the process remains impartial (see annexes E and H).

Owner: The Member States should use certification schemes that are recognised by European accreditation bodies. This should also be a requirement of the framework.

Recommendation 5: Promote validation that is commensurate with the risk appetite involved in each use case.

Conformity testing, functional testing and Interoperability testing can be used to provide assurance that specific security requirements are met. Depending on the potential criticality of the security risk, in case of non conformance with requirements, it can be decided to perform first, second or third party assessments. However, in practice, only third party certification is seen as trustworthy for most cyber security schemes and is therefore recommended. Controls should also take into account the size of the certified entity and its capability to carry out background checks; it should also be in line with the risk assessment results.

Owner: The EU steering committee should promote a risk based approach to ensure the certification effort is in line with the risk appetite involved in the in scope use case.

Recommendation 5a: Ensure proper security levels for use cases

The Member States should make sure that the level of security is explicit for each certificate. The matching of security certificate levels to a use case should be facilitated by the EU steering committee.

Owner: The Member States should perform a risk assessment to ensure that national use case risk levels are clear, and the technical committees should match the proper assessment levels to each risk level.

Recommendation 6: Facilitate flexibility to update profiles so they can cope with the fast moving security landscape

In principle, technical committees should develop national profiles covering all possible smart grid use cases. The profiles can then be updated more frequently than the schemes or standards. Any activity towards harmonisation should provide enough flexibility for the security requirements in the profiles to evolve over time and be able to cope with a changing security and threat landscape. Furthermore,

updates in schemes and profiles should be announced so that they can be incorporated in the other national profiles. This way the maturity⁴⁸ of all national schemes can evolve over time.

Owner: The EU working group should ensure the maintenance of the profiles so they keep up to date with current technology developments and announce updates to the Member States.

Recommendation 7: Use national profiles as detailed specifications of international standards to cover the specific national use cases and nationally supported test and certification methods

The national profiles should reflect the national smart grid use cases' risk. The profile should refer to standards for details, amend them or expand on them to provide the flexibility to incorporate national requirements in an international base. The profile should contain test procedures for the national specific requirements, and provide required testing depth for the national use cases aligned with the international SG-IS framework risk levels.

Owner: The Member States wanting to implement smart grid security certification will have to create national profiles containing the details for their national use cases.

Recommendation 8: Use technical committees in collaboration with the European energy associations to create European profiles

The European Commission should support the definition of European wide security requirements. To this direction, European Commission should invite the private sector for cutting edge technology specific requirements and guidance in the form of technical committees, to amend slow moving standards with detailed European profiles. The profiles should be created by Technical Communities' subgroups with EU wide scope and in collaboration with smart grid relevant associations (like ESMIG and EURELECTRIC), but they can be based on the published national initiatives (like the smart gateway profile and the CPA⁴⁹ security characteristic).

Owner: The European Commission will have to support expert groups to set up technical committees to create profiles for the technical details for the national use cases, where other national schemes or national endorsed international standards can be used as input if needed.

Recommendation 9: Provide official third party certification and self-assessment tools for pre-assessment

The EU steering committee should encourage operational communities to provide tools that will help the adoption of the framework, and will make it attractive for industry to implement. Additionally, the national technical committees should assist the industry with pre-assessment tools to facilitate national compliance.

Owner: The EU working group should encourage the provision of tools in respect to the framework, while the national technical committees should provide pre-assessment tools for specific schemes.

Recommendation 10: Promote compliance and harmonization as economic advantage and a cost reduction measure

The European Commission and the Member States should promote commercial advantages for the private sector (e.g. ease of conformance assessment; lower insurance premiums, brand recognition) to endorse conformity assessment practices. As already demonstrated, lowering the cost is one of the

⁴⁸ In this particular context, maturity reflects the ability of a certification scheme to contain security objectives which meet the latest cyber security threats.

⁴⁹ Commercial Product Assurance, see section 3.4.2



most outstanding needs of the users. Harmonisation is considered as a major contributor to lowering the cost of certification together with the shared responsibility and risk based approach.

Owner: The European Commission and the Member States should promote the advantages of better harmonised and coordinated smart grid certification practices.

7 Conclusions

Below is a visualised summary of the key recommendations presented. The figure provides the context of where the smart grid certificate applies, based on a use case. The certificate needs to indicate what component, or components are being certificated, and what other certificates are used to obtain a chain of trust. The interpretation of the figure is provided with an example of an asset owner who wants to provide a smart grid device (e.g. meter) according to the harmonised security certification practices presented in this report.

Each device, will, at least, have to comply with the national use case for the Member State it intends to supply the device to. This does not mean it cannot comply to other Member States' uses cases, but for certification for a specific Member State, it will need to focus on that specific use case. The national specific use case can be described by the SG-AM model. The SG-AM model can then be used as a basis to create the chain of trust model (As described in section 4.2.1 - *Certification and the chain of trust*).

This chain of trust model can then be used to identify the needed national requirements profile and national certification scheme to create the chain of trust for this use case, and will indicate the levels of security that the asset owner will have to provide aligned with the risk involved as indicated by the SG-IS framework risk assessment as described in section 4.2.1.

The resulting national scheme will have to be submitted to the EU steering committee for administration by the technical committee that created the scheme. The national scheme will normally be created by a national technical committee consisting of stakeholders like the relevant member state authority(ies), solution providers, user associations and national certification bodies. They will have to deploy a SG-IS framework aligned methodology on the national use-case, and can get advice by the overseeing EU steering committee for correct implementation. The developed national scheme could for example, indicate the need for a certificate for secure development and production for the creation of a chain of trust on the component level. Depending on if the manufacturer already has this certificate for the same level or higher than indicated by the risk assessment, the available certificates can be used as proof for the chain of trust. When all certificates are obtained, they can be delivered to the EU steering committee for review and publication.

After publication, it is possible to easily assess for any other use case, if the level of security of the certified meter is sufficient for the usage in the use-case at hand. Provided the evaluated national profile matches the profile requirements of the use-case. Over time, these national profiles should move toward international profiles to minimize re-certification efforts due to additional requirements. Additionally, European technical communities could provide international EU based profiles that could be the common denominator of the national ones so as to ensure: a) the participation of the Member State; and b) flexibility of the Member States to define extra national requirements on top of the European ones.

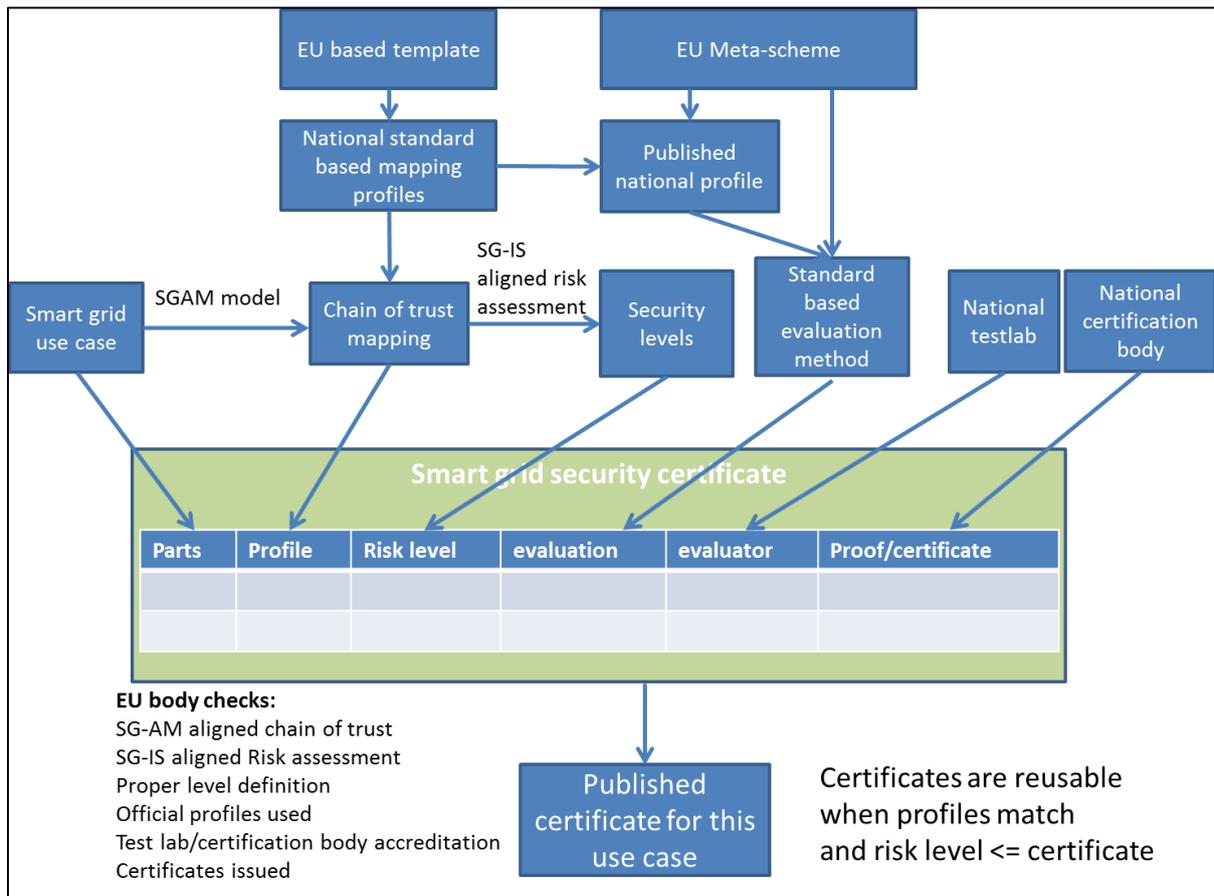


Figure 12 - Smart grid certification process

The key component towards more harmonised and better collaborated certification practices is a steering committee that is recognised by the EU which provides a focus point for smart grid security certification related activities. This body will need to provide the guidance and general approach on smart grid certification. This approach should be aligned with the SG-AM model, the SG-IS framework and the currently available initiatives and certification schemes. The body will also provide a central point for the publication of smart grid security certificates.

Furthermore, it will assist the Member States in creating their national mapping according to the EU smart grid security certification guidelines, and will ensure that national use cases and schemes are kept up-to-date, and certificates are published. Finally, it will ensure that the national approaches are mostly based on EU wide profiles, or at least harmonised, as much as possible and common approaches can eventually migrate from a more national approach to a more common set of EU requirements that can be endorsed by all Member States. This way the desired situation can be created where there is a common EU baseline, while national requirements that cannot be harmonised are still addressed.

8 References

- http://www.iso.org/iso/casco_building-trust.pdf
- ITU-T Z.450 - Quality aspects of protocol-related Recommendations - <http://www.itu.int/en/ITU-T/publications/Pages/structure.aspx>
- http://www.isasecure.org/PDFs/Articles-and-Technical-Paper-Folder/ISASecure_AssetOwnerViewpoint_Oct2013_v05.aspx
- SM-CG_Sec0073_DC_PSreport.pdf
- <http://www.lexology.com/library/detail.aspx?g=1f872876-3d23-44e7-a8f1-92a9be8d080b>
- <http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=AF#standardpick 27>
- MUTUAL RECOGNITION AGREEMENTS THEIR ROLE TODAY AND TOMORROW - a presentation on the role of mutual recognition agreements made at the Workshop on Standardization and Conformity Assessment Matters in the Transition Economies
- Source: <http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-204>
- <https://www.isa.org/pdfs/autowest/phinneydone/>
- The IECCE CB Scheme, IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE), available at <http://www.iecee.org/>

8.1 Related ENISA papers

- <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide>.
- <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components/workshop-minutes>.
- http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations/at_download/fullReport.
- Appropriate security measures for Smart Grids, ENISA 2012.
- Smart Grid Threat Landscape, ENISA 2013.
- Smart Grid Security Recommendations, ENISA 2011
- Protecting Industrial Control Systems - Recommendations for Europe and Member States, ENISA 2011.

8.2 Legislation

- M/490 mandate - http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf
- European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final) - http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Annex A: Definitions

In order to avoid confusion, a number of terms described in the table which are used in this document, they have been based on the IAF website:

Term	Explanation
Accreditation Body	An accreditation body is an organisation which evaluates the evaluators. To become a certification body, the organisation needs to be certified by an accreditation body.
Certification	Certification refers to the confirmation of certain characteristics of an object, person, or organization. This confirmation is often, but not always, provided by some form of external review, education, assessment, or audit.
Certification body	A certification body is an organisation which is accredited by an accreditation body. The organisation has demonstrated their competence, impartiality and performance capabilities. When applicable, their test labs and calibration laboratories were tested against international recognised standards.
Common criteria	The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification.
Declaration of conformity	A signed declaration to indicate that the product meets the requirements of the directive(s) which apply to it. For the declaration to be truly meaningful the signatory should also have the authority to commit the resources required to ensure that the conformity assessment process is properly completed.
First-party certification	In first-party certification, an individual or organization providing the goods or services offers assurances that it meets certain claims
Notified Body	A Notified Body, in the European Union, is an organization that has been accredited by a Member State to assess whether a product meets certain preordained standards.
Second-party certification	In second-party certification, an association to which the individual or organization belongs to provides the assurance
Smart grid environment	The whole environment in which smart grid components are implemented, however this can be a hybrid system in which legacy SCADA systems are part of
Smart energy system	A specific network, dedicated developed as a smart energy system. Old fashioned legacy system are not part of a smart energy system
Third-party certification	Third-party certification involves an independent assessment declaring that specified requirements pertaining to a product, person, process or management system have been met
Technical committee	A group responsible for development and revision of any document or documents emanating from a Technical Committee project.

Annex B: Schemes applicable to the smart grid domain

B.1 Common Criteria (CC)

Scope

Common Criteria is an industry-independent / product independent scheme. At present, certified products belong to a wide array of categories going from access control systems to operating systems and biometric systems and devices. Common Criteria offer pre-defined evaluation assurance levels (EAL), corresponding to increasing assurance efforts and vulnerability testing. A certification roughly consists of two different activities:

- Defining and assessing a consistent set of security requirements against a given security problem
- Assessing that a product is compliant with these security requirements.

These two activities are defined in ISO/IEC 15408 (also called Common Criteria for Information Technology Security Evaluation) and the associated Common Criteria Evaluation Methodology (CEM).

The Common Criteria allow the creation of a Protection Profile (PP) which is a set of security requirements for a type of product which may support many different implementations. The security requirements are derived from a set of security objectives that cover the security problem definition consisting of threats, assumptions and policies.

Common Criteria is used as the basis for a Government driven certification scheme and typically evaluations are conducted for the use in Federal Government agencies and critical infrastructure.

The Participants of Common Criteria share the following objectives:

- To ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles
- To ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;
- To improve the availability of evaluated, security-enhanced IT products and protection profiles;
- To eliminate the burden of duplicating evaluations of IT products and protection profiles;
- To continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and protection profiles.

Organization

The scheme is maintained under an international arrangement and endorsed by a group of national authorities (Certification Bodies). A Certification body (called CB hereafter) is generally a governmental agency or bureau of the national defence ministry.

Any Common Criteria evaluation relies on competent and independent licensed laboratories. These Evaluators (also called laboratories or ITSEF: Information Security Evaluation Facility) are accredited by a national standardization entity, and licensed or otherwise approved by the national Certification Body.

- In Canada, the Standards Council of Canada (SCC) under Program for the Accreditation of Laboratories (PALCAN) accredits Common Criteria Evaluation Facilities (CCEF)
- In France, the Comité français d'accréditation (COFRAC) accredits Common Criteria evaluation facilities, commonly called Centre d'évaluation de la sécurité des technologies de l'information (CESTI). Evaluations are done according to norms and standards specified by the

Agence nationale de la sécurité des systèmes d'information (ANSSI). ANSSI is also performing the licencing of the CESTI to attest that they have the appropriate security skills.

- In the UK the United Kingdom Accreditation Service (UKAS) accredits Commercial Evaluation Facilities (CLEF)
- In the US, the National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) accredits Common Criteria Testing Laboratories (CCTL)
- In Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI)
- In Spain, the National Cryptologic Center (CCN) accredits Common Criteria Testing Laboratories operating in the Spanish Scheme. Protection file for smart meter Gateways
- The German Ministry of Economy (BMWi) has mandated the Federal Agency for Security in Information technology (BSI) to develop a protection file for smart meter Gateways. The protection profile is based on Common Criteria. The use of certified Gateways is mandated for all smart meters.
- The German protection profile creates security on a very high level (CC level EAL 4+). The problem using this protection profile is that accreditation is not internationally accepted and the CC Level is higher than other countries accept.
- Norway and Sweden accepted Common Criteria as recognised standard for certification.

Evaluation methodology

The Common Criteria consists of the following catalogues:

- CC-Part 1: presents the conceptual framework of the methodology and is intended to developers as well as evaluators.
- CC-Part 2: describes a comprehensive series of standardized security (functional) requirements
- CC-Part 3: lists a comprehensive series of standardized security assurance requirements, which describe how a product should be evaluated.
- CEM: which defines the minimum actions to be performed by an evaluator in order to conduct a CC evaluation

B.2 CPA

Scope

CPA1 (Commercial Product Assurance) is a national GB scheme intended for commercial security products. CPA is defined and maintained by CESC (Communications Electronic Security Group – the Certification Body), which directly accredits evaluation laboratories (CPA Test Labs). The scheme aims at demonstrating compliance to national requirements, while rationalising legacy national schemes and maintaining the value of previously issued certificates.

CPA covers only specified types of products/features of products, while Common Criteria is industry / product independent. Examples of products covered by CPA are data sanitation, VPN's, firewalls ... Other types of products are in progress, such as smartphones or hardware security modules.

CPA offers one assurance level: Foundation Grade. This grade is intended for COTS (Commercial Off-The-Shelf) products used to process information classified as official in the new Government Classification Policy.

The two other tiers of this classification policy (secret and top-secret) require bespoke equipment to be evaluated under the CAPS (CESG Assisted Products Service) scheme. CAPS evaluation is performed by CESC itself, instead of commercial laboratories such as in CPA.

Organization

As mentioned above, CESG is GB Certification Body. It accredits evaluation laboratories and maintains CPA. Evaluation laboratories are called CPA Test Labs. Such laboratories perform evaluation of products for foundation grade certifications only. Evaluation laboratories mainly use evidence created by the developer, but can be led to create specific tests in order to check requirements left untested by the developer. Furthermore, cryptographic evaluation cannot be performed by the developer; it must be performed by an independent entity, if not by the evaluation laboratory.

Evaluation methodology

The evaluation methodology relies mainly on Security Characteristics (SCs) and the CPA Build standard.

The Security Characteristics define the expected security features of the product; they are focused on functions and are product specific (e.g. specific for data sanitation, VPN's, firewalls, etc.). Security Characteristics play a similar role to the Protection Profiles in CC. In the beginning of an evaluation, the evaluation laboratory refines the applicable Security Characteristics into Tailored Security Characteristics. Tailored Security Characteristics play a similar role as Security Targets in CC.

The CPA Build Standard defines the assurance requirements for product development and breaks into twelve high-level requirements addressing four themes:

- Configuration Management
- Flaw remediation
- Testing
- Developer security measures

Such requirements are somewhat similar to CC components listed in CC-Part3.

B.3 ISO/IEC 27001

ISO/IEC 27001 specifies the normative requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) within the context of the organization. ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. ISO 27001 provides a framework for certification. ISO/IEC 27001 is not especially focussed on smart grid, however an (energy) organisation can be certified to be compliant to this international standard.

ISO/IEC 27002 provides an outline or good practice guide for cybersecurity management. It includes guidelines for an organisation to obtain certification to the ISO 27001 standard. Once obtained, the certification lasts three years. Intermediate audits may be carried out during those three years, depending on the auditing organisation.

System operators in Germany and the UK have to be ISO/IEC 27001 compliant.

B.4 IASME

IASME is a UK-based standard for information assurance at small-to-medium enterprises (SMEs). It provides criteria and certification for small-to-medium business cyber security readiness. It also allows small to medium business to provide potential and existing customers and clients with an accredited measurement of the cyber security posture of the enterprise and its protection of personal/business data.

IASME was established to enable businesses with capitalization of 1.2 billion pounds or less (1.5 billion Euros; 2 billion US dollars) to achieve an accreditation similar to ISO 27001 but with reduced

complexity, cost, and administrative overhead (specifically focused on SME in recognition that it is difficult for small cap businesses to achieve and maintain ISO 27001).

The cost of the certification is progressively graduated based upon the employee population of the SME (e.g., 10 & fewer, 11 to 25, 26 - 100, 101 - 250 employees); the certification can be based upon a self-assessment with an IASME questionnaire or by a third-party professional assessor. Some insurance companies reduce premiums for cyber security related coverage based upon the IASME certification.

B.5 ISO 9001

ISO 9000 is a series of standards, developed and published by the International Organization for Standardization (ISO), that define, establish, and maintain a quality assurance system for manufacturing and service industries. The standards are available through national standards bodies. ISO 9000 deals with the fundamentals of quality management systems, including the eight management principles upon which the family of standards is based. ISO 9001 deals with the requirements that organizations wishing to meet the standard must fulfil.

ISO9001 provides an auditing possibility, but nothing else, as it is mainly about properly documenting what actions are performed.

Third-party certification bodies provide independent confirmation that organizations meet the requirements of ISO 9001. Over a million organizations worldwide are independently certified, making ISO 9001 one of the most widely used management tools in the world today.

B.6 IEC62443

ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

These documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards.

ISA/IEC-62443 is a set of standards and technical reports defining functional requirements and guidelines for implementing electronically secure ICS implementations. ISA/IEC 62334 focuses on all ecosystem players and consists out of 13 distinct parts (standards) organized in four categories: (i) General, (ii) Policies and Procedures, (iii) System, and (iv) Component.

1. The first (top) category includes common or foundational information such as concepts, models and terminology. Also included are work products that describe security metrics and security life cycles for IACS.
2. The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program.
3. The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model.

- The fourth category includes work products that describe the specific product development and technical requirements of control system products. This is primarily intended for control product vendors, but can be used by integrator and asset owners for to assist in the procurement of secure products.

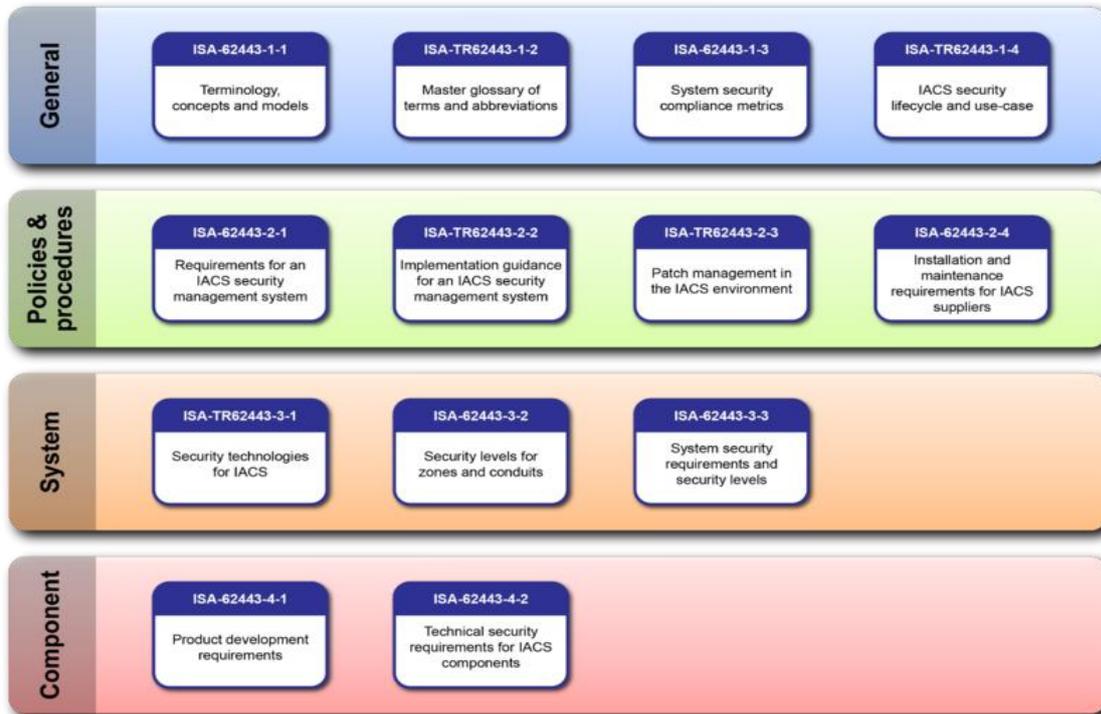


Figure 13 - IEC 62443 overview

Two parts are currently published and belong to the System category: 3-1 “Security technologies for IACS” and 3-3 “System security requirements and security levels” defining the Security Levels (SL) 1 to 4 in an ICS environment.

Two parts are published under review: 2-1 “Requirements for an IACS security management system” is based on ISO/IEC 27001(2) and belongs to the Policies and Procedures category. 1-1 defines the “Terminology, concepts and models”.

Seven parts are under development and two parts are planned.

B.7 ISO/IEC 19790

Scope

These two standards are the ISO counterpart of the US NIST FIPS 140-2, Security requirements for cryptographic modules and the derived test requirements. As such, ISO/IEC 19790 and ISO/IEC 24759 are applicable to validate whether the cryptographic core of any security product is properly implementing an approved suite of cryptographic protocols, modes of operation and key sizes, while protecting this implementation and the critical security parameters, such as keys, in accordance to the design and specification requirements laid out in the standards. There are four levels of security defined, and ISO/IEC 19790 contemplates a variety of possible implementations, both software and hardware.

Organization

Compliance to ISO/IEC 19790 is an open matter, in accordance with the existing European regulations dealing with product compliance. Since this or an equivalent harmonised standards not referred in any European Directive, it is not subject to the usual requirements for Certification Bodies to operate under Notified Bodies, but Certification Bodies for ISO/IEC 19790 are simply subject to accreditation under the applicable national accreditation entity.

The European co-operation for Accreditation (EA), and more specifically, the EA Multilateral Agreement (EA MLA) ensure cross-European recognition of ISO/IEC 19790 product compliance certificates.

Evaluation methodology

ISO/IEC 19790 and ISO/IEC 24759 are conformity testing standards, so products are tested for compliance against the applicable and very specific requirements, leaving out much of the subjectivity required for security evaluation. The requirements are set in ISO/IEC 19790, and the derived tests are specified in ISO/IEC 24759.

The conformity testing of the cryptographic protocols demand the existence of a reference implementation, and a standardized protocol to verify the correctness of the algorithm implementation, that allows a quick verification process. The requirements that apply to the cryptographic module need to be re-instantiated by the tester for each product.

The whole process is usually faster and cheaper than an equivalent security evaluation.

B.8 CSPN

Scope

The CSPN is a French scheme defined by ANSSI that aims at providing a first-level security certification for IT security products. Its scope is similar to Common Criteria, with the following specificities:

- The assurance process is simplified
- The evaluation is focused on vulnerability analysis
- The actors are committed to a given evaluation duration and cost

IT products can currently apply to CSPN if they belong to a specific list of domains (e.g. data deletion, firewalls, secure communication, etc.). This list is regularly updated to address new needs.

It should be noted that standard CSPN excludes products too complex to be evaluated in an expected duration and cost and products including non-standard cryptography.

Organization and evaluation methodology

The process is similar to the Common Criteria process. Instead of applying CC security and assurance requirements (see CC description) the developer uses guidelines described in CSPN. CSPN also has common features with CPA, especially the domain-specific approach.

Annex C: Standards and certification schemes

The following articles, standards, schemes, services and organisations have been reviewed in the research related to European smart grid security certification schemes:

Articles and investigations

- ENISA: Protecting industrial control systems, Annex III
- ENISA Appropriate security measures for Smart Grids Final
- Security_Certification-A_critical_review_2010-10-06-ICSJWG
- ahmadi-paper_gil Lpdf - The Need for Security Testing and Conformance Standards in the smart grid
- The Escorts and Viking projects
- <http://www.isacahouston.org/documents/RedTigerSecurity-NERCCIPandotherframeworks.pdf>
- CRISALIS - Critical Infrastructure Security Analysis

Security and/or smart grid standards and schemes

- M/490-SG-IS
- WIB M2784 PCS Vendor Security v2NISTIR 7628
- NIST 800-53
- NIST 800-115
- ISA/IEC62443
- IEC61850
- IEC60870-5
- IEC62351
- Common Criteria/IEC 15408 framework
- CESG CPA framework
- NERC-CIP
- ISO27001/2/5/9
- DIN SPEC 27009 (2012-04)
- US-SCADA Test bed specification from DHS-INL Idaho

Smart grid security services

- Wurldtech Achilles certification
- ISCI ISASecure EDSA Certification
- Exida's Integrity Certification

Current stocktaking lists the following additional sources and initiatives eligible for investigation:

- www.syssec-project.eu
- ENCS Topsectoren project
- BSI group (German)
- Sans institute
- Digital bond
- EPRI organisation
- CPNI (UK) best practices
- SERTIT, CSEC, UL, Infineon, ERNCIP, NEI
- CEN,/CENELEC/ETSI
- Smart Grid Coordination Group, WG Smart Grid Information Security
- Smart Grid task Force Expert Group 2 Smart Meters coordination Group

- SG-TF EG2, intermediate results of JRC study on privacy seals
- CRISALIS,
- ENCS,
- ESMIG,
- NERC-CIP/NIST,
- Smart meter DLMS,
- Dutch/Belgium IEC60870-5-104 User Group,
- Utility Communications Architecture (UCA) International User Group for IEC61850
- USEF (Universal Smart Energy Framework) - Smart Energy Collective

Based on the provided model of what needs to be certified (the SG-AM and chain of trust model described in section “4.2.1 Certification and the chain of trust”) a desktop study has been performed to create an inventory of available schemes that are applicable to the smart grid domain. From a list of initiatives, best practices, standards and schemes, only the items that were in line with the needs described in chapter 2 have been selected. The selection criteria included answering the following questions;

1. It is a scheme that is actually applicable to smart grid devices? (meaning that standards regarding general IT, or person certification are out of scope)
2. It is scheme that applies to cyber security? (meaning that safety and physical security is out of scope)
3. It is a scheme that can support certification, audits and/or legislation? (meaning that best practices and informative standards were excluded, as they are too vague)
4. Is the scheme is applicable in the EU? (meaning that schemes not used in EU were excluded)
5. Is the scheme supported by public and private bodies (meaning biased or vendor based schemes were excluded)
6. Is the scheme superseded or incorporated by another applicable scheme?

The following schemes have therefore been excluded;

	Standard / scheme	Exclusion Reason
1.	Borg	Not applicable for smart grid
2.	TC57 IEC61850/IEC60870/DLMS	Not cyber security
3.	ISA99	Superseded by IEC62443
4.	Exida's Integrity Certification	Commercial private program, no public endorsement
5.	Wurldtech Achilles	Commercial private program, no public endorsement
6.	Security Rating Guide	Not applicable for smart grid, only general IT
7.	NERC-CIP	US based
8.	WIB M2784 PCS Vendor Security	Incorporated by IEC62443
9.	FIPS PUB 140-2	US based
10.	IEC 61508 CASS certification scheme	IEC 61511 process safety
11.	SERTIT	Not applicable for smart grid, only general IT

12.	ISO/IEC-27002 – ISO/IEC TR 27019, NISTIR-7628, RFC 2196, NIST 800-53 rev3, NIST 800-115	Informative only
13.	NIST Special Publication 800-37	Informative only
14.	Certified Cloud Service - TÜV Rheinland	Not applicable for smart grid, only general IT
15.	Open Certification Framework - OCF	Not applicable for smart grid, only general IT
16.	EuroCloud Star Audit	Not applicable for smart grid, only general IT
17.	Supplier Information Assurance Assessment Framework and Guidance	Not applicable for smart grid, only general IT
18.	IEC62351	No scheme available
19.	IsaSecure EDSA	No EU based stakeholders within smart grid

Table 1 - excluded standards and schemes

What is left is a list of available schemes that are applicable to the smart grid domain:

- ISO/IEC 15408 Common Criteria (C.C.)
- CPA
- ISO/IEC 27001
- IASME
- ISO 9001
- IEC62443
- ISO/IEC 19790
- CSPN

Annex D: Scheme mapping

There is no uniform method available for mapping certification schemes. There is a standard called ISO 17067 (*Annex F: ISO/IEC 17067 - fundamentals of product certification and guidelines for product certification schemes*) that provides properties for product certification schemes. But this is not a good base for a mapping exercise, as it does not address the differentiating properties like practical implementation, and market reception of a scheme. Therefore a different method has been used to map the schemes. The method used is based on a textual analysis of the information publicly available for each scheme, amended by the practical knowledge of the authors' team about the schemes. Additionally, the ENISA research for cloud computing certification has performed similar research regarding cloud computing schemes⁵⁰, and SM-CG has provided a document comparing some of the schemes found⁵¹ that has been used for input as well.

To be able to compare the different schemes, an analysis has been made regarding the available schemes by comparing the following properties:

D.1.1 Administrative details

Name:

Type:

Group/initiative/organisation: Group, initiative or organisation responsible for the creation of the standard, guideline (e.g. ANSI/ISA), or regulatory document.

Related documents: Other identified standards, guidelines, or regulatory documents, not necessarily related to cyber security, which have a strong relationship with the document being described.

D.1.2 Geographic relevance

Geographic relevance: Worldwide, European, Subgroup of European Member States, and National.

D.1.3 Current maintenance and activity of the program working group

Status: draft/final, version 1,2,3?

Publication date: how actual is it, is it ongoing?

D.1.4 Program scope definition

Description:

Target audience: Specifies which, among the stakeholder types identified in this study

Addressed industry: All, Generic (ICS in general), SCADA, automation, chemistry, electricity distribution/transportation, nuclear generation, water, railway transportation, oil and gas distribution, etc.

Technical relevance of the methodology

- The certification bodies facilitate coordination with technical communities to ensure technical relevance.
- The methodology covers generic security functionalities like: "Security audit, logs, events & alarms", "Role based access and account management", "Cryptography and key management", etc.
- The methodology or recognition agreement defines an assurance continuity process after product updates.
- The methodology supports multiple security/assurance levels.

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

⁵⁰ <https://resilience.enisa.europa.eu/cloud-computing-certification>

⁵¹ SMCG Smart Meters Co-ordination Group 2 Privacy and Security approach - part II; Annual report 2013

security function testing, test of the user guidance, testing of protection against misuse, regression testing (re-testing after product changes), etc.

- 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.

The heaviness of the program

- Resources needed,
- Certification delay

Maintenance scheme definition for the program

- Committing to flaw remediation obligations, delays and information provision to end-users:
- The certification scheme requires a procedure for providing information to end-users on identified flaws and security incidents. Furthermore, it requires that timely action is taken for flaw remediation.

D.1.5 National and international accreditation body recognition

Recognition by accreditation bodies (ISO, IEC, other?) National and international;

- Necessary steps to instate a certification body (national and/or European)
- Ability to be used to generate consensus between parties

Definition of CB accreditation criteria

- The recognition agreement organization defines requirements for accreditation of individual Certification Bodies.
- The recognition agreement organization defines criteria for periodic assessment of Certification Bodies’ continued compliance to accreditation requirements.

D.1.6 Ability to evolve to a European certification scheme, from the current situation

Ability to customize and adoption of the program for other applications. The certification scheme applies to a wider product scope, and is able to grow. Has it been done? What needs to be changed, are there issues identified?

D.1.7 Program stakeholder trust

Public private participation

Information provision to stakeholders

- The recognition agreement organization publishes certificates and provides information on accredited certification bodies.

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 performance, functional and physical attributes with its requirements. An example of such a requirement is “All constituent components that are used to create the finished product must be uniquely identified.”
- The certification scheme requires that third-party tools and components are properly managed. For example through procedures for acquisition, reception and testing, installation, patching, etc. of third-party tools.
- The certification scheme requires that developers are properly trained on security related subjects.
- The certification scheme demands that sufficient user guidance is being provided to actors responsible for operation / administration / maintenance of the system.
- The certification scheme requires a flaw remediation procedure tracking (amongst others) product flaws, their effects, corrective measures, etc.

- The certification scheme requires a documented lifecycle model (formalization of product specification design documentation, requirements traceability, etc.) providing for the necessary quality control over the development and maintenance of the product.

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 ...)
- The certification scheme required that user guidance is provided to secure the product during operation/administration/maintenance.

D.1.8 Market drivers for the program

Economics: The scheme includes measures to limit the cost and/or workload and/or duration of evaluation

D.2 List of schemes

This list of properties to be used for comparison has been based on the knowledge DNV GL has regarding the properties of schemes, and has been amended by the existing work from ESMIG.

- ISO 9001
- ISO/IEC 27001
- IASME
- IEC62443
- ISO/IEC 15408 Common Criteria (C.C.)
- CPA
- CSPN
- ISO/IEC 19790

Administrative details	Name: ISO 9001 Type: quality management system certification Group/initiative/organisation: ISO Related documents: ISO 9000 series
Geographic relevance	global
Current maintenance and activity of the program working group	Initial development: 1987 Last publication: version 2008 Active working group: yes
Program scope definition <ul style="list-style-type: none"> • Description • Target audience • Addressed Industry • Technical relevance of the methodology • Product testing • The heaviness of the program • Maintenance scheme definition for the program 	Description: "ISO 9000 is a series of standards, developed and published by the International Organization for Standardization (ISO), that define, establish, and maintain an effective quality assurance system for manufacturing and service industries. The standards are available through national standards bodies. ISO 9000 deals with the fundamentals of quality management systems, including the eight management principles upon which the family of standards is based. ISO 9001 deals with the requirements that organizations wishing to meet the standard must fulfil. Target audience: companies in general Addressed Industry: companies in need of quality management Technical relevance of the methodology: it is a general methodology that requires policies and procedures have to be

	<p>documented, and can serve as a way to enforce structure regarding more detailed certification schemes.</p> <p>Product testing: Not applicable</p> <p>The heaviness of the program: it requires documentation and training. One year for implementation is not uncommon. It can be too costly for small companies</p> <p>Maintenance scheme definition for the program: external audits and re-certification efforts should be performed</p>
<p>National and international accreditation body recognition</p> <ul style="list-style-type: none"> • Recognition by accreditation bodies (ISO, IEC, other?) National and international; • Definition of CB accreditation criteria 	<p>Recognition by accreditation bodies:</p> <p>accreditation by IAF members, recognised by EU and industry in general</p> <p>Definition of CB accreditation criteria: yes</p>
<p>Ability to evolve to a European certification scheme, from the current situation</p>	<p>Due to the general nature, it will probably not be possible to adopt this standard explicitly for smart grid purposes, but can still be used as a general means for QA regarding a company involved with smart grids</p>
<p>Program stakeholder trust</p> <ul style="list-style-type: none"> • Public private participation, • Information provision to stakeholders • Use of proven methods and maintaining skills • Defining security measures for the premises of developers / OAM actors 	<p>Third-party certification bodies provide independent confirmation that organizations meet the requirements of ISO 9001. Over a million organizations worldwide are independently certified, making ISO 9001 one of the most widely used management tools in the world today. Despite widespread use, the ISO certification process has been criticized as being wasteful and not being useful for all organizations.</p> <p>Specific security related details to enhance stakeholder trust are not applicable to ISO9001 as it is too general.</p>
<p>Market drivers for the program</p>	<p>As it describes the fundamentals of quality management, it has been especially been endorsed for supply chain and cross industry recognition of upholding a certain degree of quality.</p>

<p>Administrative details</p>	<p>Name: ISO/IEC 27001</p> <p>Type: Information security management certification</p> <p>Group/initiative/organisation: IEC/ISO</p> <p>Related documents: IEC/ISO 27000 series</p>
<p>Geographic relevance</p>	<p>global</p>
<p>Current maintenance and activity of the program working group</p>	<p>Initial development: 1995</p> <p>Last publication: version 2013</p> <p>Active working group: yes</p>
<p>Program scope definition</p> <ul style="list-style-type: none"> • Description • Target audience • Addressed Industry • Technical relevance of the methodology • Product testing • The heaviness of the program • Maintenance scheme definition for the program 	<p>Description: ISO/IEC 27001:2005 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.</p> <p>Target audience: risk management, security officer</p> <p>Addressed Industry: companies with IT systems</p>

	<p>Technical relevance of the methodology: it is mainly an audit and inspection effort regarding defined policies and correctly executed procedures.</p> <p>Product testing: not applicable</p> <p>The heaviness of the program: ISO27001 compliance is an effort that takes around one year, and will require the resources available in large companies, but will be difficult to achieve in small to mid-sized companies.</p> <p>Maintenance scheme definition for the program: An ISO27001 certification is subject to updates, audits and re-certification.</p>
<p>National and international accreditation body recognition</p> <ul style="list-style-type: none"> • Recognition by accreditation bodies (ISO, IEC, other?) National and international; • Definition of CB accreditation criteria 	<p>Recognition by accreditation bodies:</p> <p>Accreditation by IAF members, recognised by EU and industry in general.</p> <p>Definition of CB accreditation criteria: yes</p>
<p>Ability to evolve to a European certification scheme, from the current situation</p>	<p>The standard in itself is general enough to apply to any company in need for information security management, but there have been specifications issued for process control systems</p>
<p>Program stakeholder trust</p> <ul style="list-style-type: none"> • Public private participation • Information provision to stakeholders • Use of proven methods and maintaining skills • Defining security measures for the premises of developers / OAM actors 	<p>Public private participation:</p> <p>Information provision to stakeholders: Certificates are published on the ISO website.</p> <p>Use of proven methods and maintaining skills: skilled personnel like ISO27000 lead auditors are needed to grant certification. ISO 27002 provides implementation guidance of controls. ISO27000 requires a documented lifecycle model regarding the security management.</p> <p>Defining security measures for the premises of developers / OAM actors: ISO 27001 defines security measures for premises of developers / OAM actors.</p>
<p>Market drivers for the program</p>	<p>Corporate governance, supply chain pressure, and it is generally being recognised as the main standard for managing information security. Source: http://bhconsulting.ie/securitywatch/?p=953</p>

<p>Administrative details</p>	<p>Name: IASME Type: ISO27001 for small and mid-size companies Group/initiative/organisation: IASME Consortium Limited Related documents: IEC/ISO 27000 series</p>
<p>Geographic relevance</p>	<p>UK</p>
<p>Current maintenance and activity of the program working group</p>	<p>Initial development: 2010 Last publication: 2011 Active working group: yes</p>
<p>Program scope definition</p> <ul style="list-style-type: none"> • Description • Target audience • Addressed Industry 	<p>Description: IASME is a UK-based standard for information assurance at small-to-medium enterprises (SMEs).It provides criteria and certification for small-to-medium business cyber security readiness. It also allows small to medium business to</p>

<ul style="list-style-type: none"> • Technical relevance of the methodology • Product testing • The heaviness of the program • Maintenance scheme definition for the program 	<p>provide potential and existing customers and clients with an accredited measurement of the cyber security posture of the enterprise and its protection of personal/business data.</p> <p>Target audience: risk management, security officer</p> <p>Addressed Industry: small to mid-sized companies with IT systems(e.g., 10 & fewer, 11 to 25, 26 - 100, 101 - 250 employees)</p> <p>Technical relevance of the methodology: it is mainly an audit and inspection effort regarding defined policies and correctly executed procedures.</p> <p>Product testing: not applicable</p> <p>The heaviness of the program: IASME compliance is a self-assessment effort that will require the resources depending on the size of the company.</p> <p>Maintenance scheme definition for the program: present</p>
<p>National and international accreditation body recognition</p> <ul style="list-style-type: none"> • Recognition by accreditation bodies (ISO, IEC, other?) National and international; • Definition of CB accreditation criteria 	<p>Recognition by accreditation bodies:</p> <p>UK accreditation, UK recognition</p> <p>Definition of CB accreditation criteria: not found</p>
<p>Ability to evolve to a European certification scheme, from the current situation</p>	<p>Similar to ISO27001, however not widely recognised outside of UK.</p>
<p>Program stakeholder trust</p> <ul style="list-style-type: none"> • Public private participation, • Information provision to stakeholders • Use of proven methods and maintaining skills • Defining security measures for the premises of developers / OAM actors 	<p>Public private participation:</p> <p>The certification can be based upon a self-assessment with an IASME questionnaire or by a third-party professional assessor.</p> <p>Information provision to stakeholders:</p> <p>Publication of certificate is done by CESG</p> <p>Use of proven methods and maintaining skills:</p> <p>Defining security measures for the premises of developers / OAM actors: Same measures defined as ISO27001</p>
<p>Market drivers for the program</p>	<p>The cost of the certification is progressively graduated based upon the employee population of the SME. As it is targeted at small to medium companies, the main driver was to provide an affordable scheme for the UK market. Some insurance companies reduce premiums for cyber security related coverage based upon the IASME certification."</p>

<p>Administrative details</p>	<p>Name: IEC 62443 Type: Security for Industrial Automation and Control Systems Group/initiative/organisation: IEC/ISA Related documents:ISA.99</p>
<p>Geographic relevance</p> <p>Current maintenance and activity of the program working group</p>	<p>global</p> <p>Initial development: 2007 Last publication: Part final, part draft, target date 2016 Active working group: yes</p>

<p>Program scope definition</p> <ul style="list-style-type: none"> • Description • Target audience • Addressed Industry • Technical relevance of the methodology • Product testing • The heaviness of the program • Maintenance scheme definition for the program 	<p>Description: The ISA99/IEC 62443 standard is the worldwide standard for security of the Industrial Control Systems in the Operational Technology (OT) domain of organizations. The standard was created by the International Society of Automation (www.isa.org), a leading worldwide non-profit organization. The standard offers organizations handles to improve the digital security and safety of their process and SCADA environments. Implementation of the standard brings your organization to a higher level for security of the OT domain, the process or production environments. The ISA99/IEC 62443 standard is derived from the ISO/IEC 27000 series standard and adapted with the focus on Industrial Control Systems environments.</p> <p>Target audience: vendors, governance, system integrators, operators</p> <p>Addressed Industry: Industrial Automation and Control Systems</p> <p>Technical relevance of the methodology: it focusses on all aspects of industrial control systems from a functional perspective. It addresses the different actors in the chain of trust.</p> <p>Product testing: There are requirements for product testing, but no official certification scheme yet that is usable in Europe.</p> <p>The heaviness of the program: As the program does not have an official certification scheme for all parts, it is difficult to assess. But the ISASecure testing seems to provide 3 levels, and will probably take several months to complete.</p> <p>Maintenance scheme definition for the program: present</p>
<p>National and international accreditation body recognition</p> <ul style="list-style-type: none"> • Recognition by accreditation bodies (ISO, IEC, other?) National and international; • Definition of CB accreditation criteria 	<p>The IEC/ISA standardisation bodies are recognised, but the only existing certification service called ISASecure is only available at certification bodies in the US and Japan, and recognised by ANSI (American National Standards Institute).</p>
<p>Ability to evolve to a European certification scheme, from the current situation</p>	<p>A big portion of the standards are still in draft. But it seems there are promising developments going on related to certification schemes that would fit into a European approach</p>
<p>Program stakeholder trust</p> <ul style="list-style-type: none"> • Public private participation, • Information provision to stakeholders • Use of proven methods and maintaining skills • Defining security measures for the premises of developers / OAM actors 	<p>Public private participation: The standard is being developed by working groups that include suppliers, operators and public bodies.</p> <p>Information provision to stakeholders: As the ISA.99 and IEC62443 standard are maintained by different working groups (IEC TC65 and ISA) and the certification is done by a third (ISASecure) information is fragmented.</p> <p>Use of proven methods and maintaining skills: There is a certification for persons regarding IEC 62443 called "Cybersecurity Fundamentals Specialist Certificate"</p> <p>Defining security measures for the premises of developers / OAM actors: IEC62443-2-4 and IEC62443-4-1 define requirements about this</p>
<p>Market drivers for the program</p>	<p>Endorsed by manufacturers, IEC62443-2-4 (as the WIB_M2784_PCS_vendorsecurity) initially created by Shell for</p>

	a specific need to mandate vendor equipment was meeting certain cyber security requirements.
--	----------------------------------------------------------------------------------------------

Administrative details	Name: ISO/IEC 15408 Common Criteria (C.C.) Type: component security certification scheme Group/initiative/organisation: ISO/IEC, CCRA Related documents: CCDB-200X
Geographic relevance	global
Current maintenance and activity of the program working group	Initial development: 1990 Last publication: 2009 Active working group: yes
Program scope definition <ul style="list-style-type: none"> • Description • Target audience • Addressed Industry • Technical relevance of the methodology • Product testing • The heaviness of the program • Maintenance scheme definition for the program 	<p>Description: The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1 revision 4.[1]</p> <p>Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.</p> <p>Target audience: vendors of IT equipment</p> <p>Addressed Industry: users of IT products</p> <p>Technical relevance of the methodology: The certification bodies facilitate coordination with technical communities to ensure technical relevance. The methodology partially covers generic security functionalities like: “Security audit, logs, events & alarms”, “Role based access and account management”, “Cryptography and key management”, etc. The methodology or recognition agreement defines an assurance continuity process after product updates. The methodology supports multiple security/assurance levels.</p> <p>Product testing: The standard contains detailed requirements and procedures for functional and vulnerability testing depending on security level.</p> <p>The heaviness of the program: Certification can cost several months up to multiple years depending on complexity and security level. Low security levels can be only a check of documentation, while higher levels can require deep hardware and software evaluations</p> <p>Maintenance scheme definition for the program: Fully covered depending on security level</p>
National and international accreditation body recognition <ul style="list-style-type: none"> • Recognition by accreditation bodies (ISO, IEC, other?) National and international; 	accreditation by IAF members, recognised by EU and industry in general

<ul style="list-style-type: none"> • Definition of CB accreditation criteria 	<p>Recognition by accreditation bodies: Inter-national (17 authorizing members and 9 consuming members). Mutual recognition agreements between EU Member States.</p> <p>Definition of CB accreditation criteria: Fully covered</p>
Ability to evolve to a European certification scheme, from the current situation	The scheme is highly customizable for other technical fields where there is a need to certify a product for security. This has already been demonstrated, and is endorsed by Germany for the smart meter
<p>Program stakeholder trust</p> <ul style="list-style-type: none"> • Public private participation, • Information provision to stakeholders • Use of proven methods and maintaining skills • Defining security measures for the premises of developers / OAM actors 	<p>Public private participation: EA, SOGIS</p> <p>Information provision to stakeholders: Yes, through common criteria and SOG-IS web portals</p> <p>Use of proven methods and maintaining skills: Fully covered depending on security level</p> <p>Defining security measures for the premises of developers / OAM actors: fully covered depending on security level</p>
Market drivers for the program	Common Criteria is used as the basis for a Government driven certification scheme and typically evaluations are conducted for the use of Federal Government agencies and critical infrastructure." The scheme originated from smart-card users and producers, but has since been adopted for a broad range of products. Technical committee's provide input for specific protection profiles and standard improvement

Administrative details	<p>Name: CPA</p> <p>Type: component security certification scheme</p> <p>Group/initiative/organisation: CESC</p> <p>Related documents: http://www.cesg.gov.uk</p>
Geographic relevance	UK
Current maintenance and activity of the program working group	<p>Initial development: undisclosed</p> <p>Last publication: 2011</p> <p>Active working group: yes</p>
<p>Program scope definition</p> <ul style="list-style-type: none"> • Description • Target audience • Addressed Industry • Technical relevance of the methodology • Product testing • The heaviness of the program • Maintenance scheme definition for the program 	<p>Description: The Commercial Product Assurance (CPA) scheme evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry.</p> <p>CPA consolidates previous CESC schemes to provide simplified, certificate-based assurance of security products for use in lower threat environments.</p> <p>Target audience: Suppliers to UK government</p> <p>Addressed Industry: IT industry</p> <p>Technical relevance of the methodology: The certification bodies facilitate coordination with technical communities to ensure technical relevance.</p> <p>Product testing: The standard contains detailed requirements and procedures for functional and partly vulnerability testing</p> <p>The heaviness of the program: CPA is designed to be less intensive than common criteria while achieving similar results</p>

	Maintenance scheme definition for the program: present, except for a documented lifecycle model
National and international accreditation body recognition <ul style="list-style-type: none"> • Recognition by accreditation bodies (ISO, IEC, other?) National and international; • Definition of CB accreditation criteria 	Recognition by accreditation bodies: Only CESG in UK Definition of CB accreditation criteria: accreditation by UK accreditation council, recognised by UK government
Ability to evolve to a European certification scheme, from the current situation	similar to common criteria, however not so widely recognised outside of UK
Program stakeholder trust <ul style="list-style-type: none"> • Public private participation, • Information provision to stakeholders • Use of proven methods and maintaining skills • Defining security measures for the premises of developers / OAM actors 	Public private participation: Unknown Information provision to stakeholders: Available on CESG website Use of proven methods and maintaining skills: Partly covered Defining security measures for the premises of developers / OAM actors: Fully covered
Market drivers for the program	The British government and CESA are the main drivers behind CPA, and the scheme is intended to solve certain shortcomings and disadvantages of common criteria for the UK market.

Administrative details	Name: CSPN Type: component security certification scheme Group/initiative/organisation: ANSSI Related documents: http://www.ssi.gouv.fr/
Geographic relevance	France
Current maintenance and activity of the program working group	Initial development: 2008 Last publication: 2012 Active working group: yes
Program scope definition <ul style="list-style-type: none"> • Description • Target audience • Addressed Industry • Technical relevance of the methodology • Product testing • The heaviness of the program • Maintenance scheme definition for the program 	Description: First level security certification for information technologies (CSPN) relies on criteria, methodologies and a process created by ANSSI. The main goal of CSPN is to offer a security evaluation of a product within certain time and workload constraints that may lead to certification Target audience: Vendors of IT products Addressed Industry: IT industry Technical relevance of the methodology: The certification bodies optionally facilitate coordination with technical communities to ensure technical relevance. The methodology defines an assurance continuity process after product updates. Product testing: The standard contains detailed requirements and procedures for functional and partly vulnerability testing The heaviness of the program: A CSPN evaluation contains a fixed timeframe for the evaluation of the product. Maintenance scheme definition for the program: Yes
National and international accreditation body recognition	Recognition by accreditation bodies:

<ul style="list-style-type: none"> • Recognition by accreditation bodies (ISO, IEC, other?) National and international; • Definition of CB accreditation criteria 	<p>Only ANSSI in France</p> <p>Definition of CB accreditation criteria:</p> <p>Not available</p>
<p>Ability to evolve to a European certification scheme, from the current situation</p>	<p>Not found</p>
<p>Program stakeholder trust</p> <ul style="list-style-type: none"> • Public private participation, • Information provision to stakeholders • Use of proven methods and maintaining skills • Defining security measures for the premises of developers / OAM actors 	<p>Public private participation: unknown</p> <p>Information provision to stakeholders: Not found</p> <p>Use of proven methods and maintaining skills: optional</p> <p>Defining security measures for the premises of developers / OAM actors: optional</p>
<p>Market drivers for the program</p>	<p>Compliance with French market demand. Fixed assessment time should reduce cost of certification.</p>

<p>Administrative details</p>	<p>Name: ISO/IEC 19790</p> <p>Type: certification for cryptographic modules</p> <p>Group/initiative/organisation: IEC/ISO</p> <p>Related documents: FIPS140-2</p>
<p>Geographic relevance</p>	<p>global</p>
<p>Current maintenance and activity of the program working group</p>	<p>Initial development: 2001</p> <p>Last publication: 2012</p> <p>Active working group: yes</p>
<p>Program scope definition</p> <ul style="list-style-type: none"> • Description • Target audience • Addressed Industry • Technical relevance of the methodology • Product testing • The heaviness of the program • Maintenance scheme definition for the program 	<p>Description: SO/IEC 19790:2012 specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems. ISO/IEC 19790:2012 defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location). ISO/IEC 19790:2012 specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level. The requirements are set in ISO/IEC 19790, and the derived tests are specified in ISO/IEC 24759.</p> <p>Target audience: all users of cryptography modules</p> <p>Addressed Industry: providers of cryptographic modules</p> <p>Technical relevance of the methodology: The certification bodies optionally facilitate coordination with technical communities to ensure technical relevance. The methodology partially covers generic security functionalities like: "Security audit, logs, events & alarms", "Role based access and account management", "Cryptography and key management", etc. The methodology supports multiple security/assurance levels.</p> <p>Product testing: The standard contains detailed requirements and procedures for only functional testing</p>

	<p>The heaviness of the program: Good for top secret governmental grade. Evaluation timespan of half a year to a year</p> <p>Maintenance scheme definition for the program: Not found, only documented lifecycle model, with depth depending on security level</p>
<p>National and international accreditation body recognition</p> <ul style="list-style-type: none"> • Recognition by accreditation bodies (ISO, IEC, other?) National and international; • Definition of CB accreditation criteria 	<p>Recognition by accreditation bodies: Full Europe (35 full members and 13 associate members). Accreditation by IAF members, recognised by global countries and industry in general.</p> <p>Definition of CB accreditation criteria: covered, but no periodic assessment criteria</p>
<p>Ability to evolve to a European certification scheme, from the current situation</p>	<p>It is being recognised in Europe, and could be part of a European scheme, but too specific for a single purpose to be relevant in this context</p>
<p>Program stakeholder trust</p> <ul style="list-style-type: none"> • Public private participation, • Information provision to stakeholders • Use of proven methods and maintaining skills • Defining security measures for the premises of developers / OAM actors 	<p>Public private participation: Inclusion of public accreditation bodies and involvement of US government with development of FIPS140-2</p> <p>Information provision to stakeholders: Partially covered (only accredited labs)</p> <p>Use of proven methods and maintaining skills: Partly covered</p> <p>Defining security measures for the premises of developers / OAM actors: Not covered, only user guidance to secure the product during operation/administration/maintenance.</p>
<p>Market drivers for the program</p>	<p>the US government was the main driver behind the creation of this certification scheme to facilitate the selection of approved products in high security environments, it is an adaption of FIPS140-2 to be used by the international community</p>

Annex E: Description of accreditation and certification

Accreditation is the independent evaluation of conformity assessment bodies against recognised standards to ensure their impartiality and competence. Through the application of national and international standards, government, procurers and consumers can have confidence in the calibration and test results, inspection reports and certifications provided.

Accreditation bodies are established in many countries with the primary purpose of ensuring that conformity assessment bodies are subject to oversight by an authoritative body.

Accreditation bodies, which have been evaluated by peers as competent, sign arrangements that enhance the acceptance of products and services across national borders, thereby creating a framework to support international trade through the removal of technical barriers.

Different countries may use different security standards, best practices and frameworks regarding Cyber Security. This section provides an overview of the accreditation and certification approach used in the European Union.

E.1 Existing accreditation bodies

Although this report focusses on the European Union and common practices used in the EU, DNV GL took international (worldwide) accepted certification approaches in account.

E.1.1 International recognised accreditation Fora

On the uppermost top level of the certification approach you will find the international (world-wide) organised accreditation fora. The national bodies are all committed to one or more international forum.

The three most important international accreditation fora are:

1. International Accreditation Forum (IAF, Quebec, Canada)
2. International Laboratory Accreditation Cooperation (ILAC, Rhodes, Australia)
3. European co-operation for Accreditation (EA, Paris, France)

1: IAF Accreditation arrangements are managed by the International Accreditation Forum (IAF), in the fields of management systems, products, services, personnel and other similar programmes of conformity assessment, and the International Laboratory Accreditation Cooperation (ILAC), in the field of laboratory and inspection accreditation.

2: The ILAC Arrangement is the culmination of 22 years of intensive work. The ILAC Arrangement provides significant technical underpinning to international trade. The key to the Arrangement is the global network of accredited testing and calibration laboratories and inspection bodies that are assessed and recognised as being competent by ILAC Arrangement signatory accreditation bodies. On 2 November 2000, ILAC's 36 full members, consisting of laboratory accreditation bodies from 28 economies worldwide, signed a mutual recognition arrangement (the ILAC Arrangement) in Washington DC, to promote the acceptance of technical test and calibration data for exported goods. The Arrangement came into effect on 31 January 2001 and was extended in October 2012 to include the accreditation of inspection bodies

3: EA exists to coordinate and lead the European accreditation infrastructure to allow the results of conformity assessment services in one Member State to be accepted by Regulators and the market place in another Member State without further examination, for the benefit of the European community and the global economy.

E.1.2 National accreditation bodies

To reach the level of certification body, the organisation should be evaluated by a national accreditation body. The mentioned accreditation bodies below are member of EA, ILAC and IAF.

Some examples of European accreditation bodies are:

1. United Kingdom Accreditation Services (UKAS, Feltham Middlesex, UK)
2. Raad voor Accreditatie (RvA, Utrecht, the Netherlands)
3. Deutsche Akkreditierungsstelle GmbH (DAkkS)

The full list of accreditation bodies that are recognized is publicly available at;

http://www.iaf.nu/articles/IAF_MEMBERS_SIGNATORIES/4

UKAS is licensed by the Department for Business Innovation & Skills (BIS) to use and confer the national accreditation symbols (formerly national accreditation marks) which symbolise Government recognition of the accreditation process. UKAS accreditation provides an assurance of the competence, impartiality and integrity of conformity assessment bodies.

With the law on the appointment of the national accreditation body, **RvA** is appointed as the Dutch national accreditation body and is entrusted with the operation of accreditation as a public authority activity.

Accreditation bodies such as UKAS and RvA are national entities responsible for national accreditation of a certification body. UKAS is member of the EA. RvA is member of EA, ILAC and IAF.

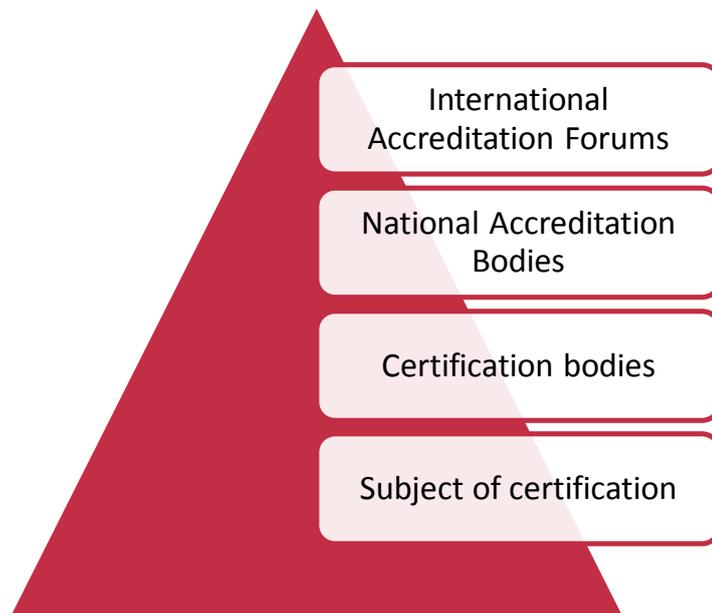


Figure 14 - Certification top down approach

E.2 Internationally recognized certification bodies

On a national level certification bodies are then accredited to issue certificates for certification schemes they are accredited for. Certification bodies are free to choose their way of working, within the context of the subject of study.

Certification bodies are, or were in the past, often governmental related organisations. In the EU there are some widely known organisations working in the field of testing and certifying.

- Bundesamt für Sicherheit in der Informationstechnik (BSI, Germany)
- TÜV (Germany)

- Communications-Electronics Security Group (CESG, UK)
- Brightside (London, UK)
- DNV GL (Høvik, Norway, DNV GL Energy, Arnhem, the Netherlands)

Figure 15 on the next page provides an overview of the accreditation and certification approach in the European Union.

The International Accreditation Forum (IAF) and International Laboratory Accreditation Cooperation (ILAC) oversee the accreditation bodies globally. Accreditation bodies such as UKAS and RvA are national entities responsible for national accreditation of a certification body. Certification bodies such as BSI, TuV and CESG are then accredited to issue certificates for certification schemes they are accredited for. Certification schemes such as common criteria are maintained by a scheme owner.

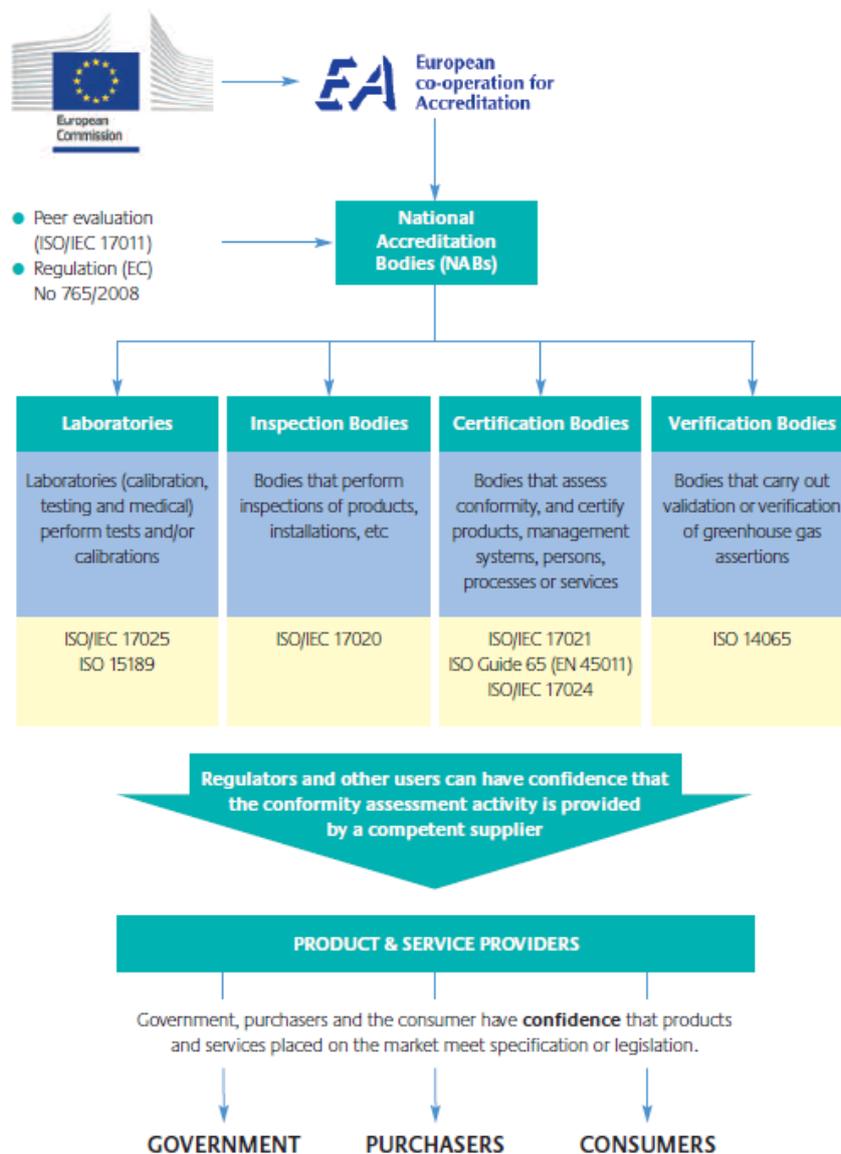


Figure 15 - Overview of hierarchy in accreditation and certification

E.2.1 Certification organisations

Accreditation bodies and certification bodies use international standards to fulfil their jobs. On one hand this is necessary to understand their way of working, on the other hand using international standards creates worldwide acceptance for a certificate. A certificate issued in the Netherlands for a German product will be accepted in France, the UK and even in Australia.

Figure 16 on the next page provides a description of how the international structure of accreditation and certification organisations is shaped for the IEC and ISO standards.

A test or assessment according to a scheme is executed by an independent test laboratory such as DNV GL, TuV or Brightside, in case of common criteria.

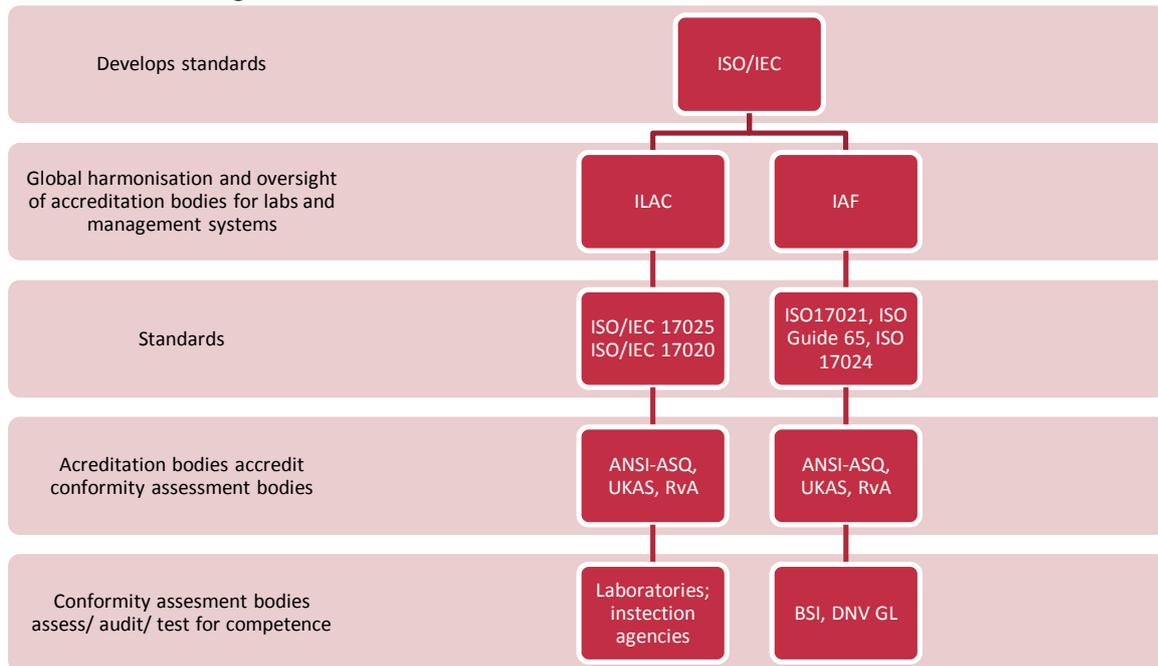


Figure 16 - Overview ISO/IEC certification organisation

Figure 17 describes an interaction diagram between different stakeholders during an evaluation. It should be noted that the evaluation facility evaluates the product, but the certification body issues the certificate, to ensure integrity of the parties involved.

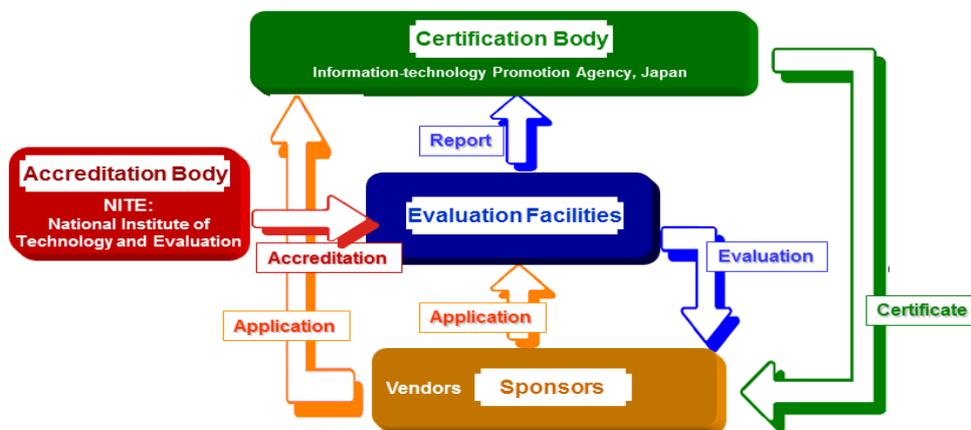


Figure 17 - Interaction between stakeholders. Source: Common Criteria, IPA, Japan

Annex F: ISO/IEC 17067 - fundamentals of product certification and guidelines for product certification schemes

F.1 Product scheme properties

Each scheme has certain properties that must be fulfilled in order to be seen as a scheme. ISO/IEC 17067 lists these as the following;

- **selection**, which includes planning and preparation activities in order to collect or produce all the information and input needed for the subsequent determination function;
- **determination**, which may include conformity assessment activities such as
 - testing
 - measuring
 - inspection
 - design appraisal
 - assessment of services and processes
- **auditing** — review, which means verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfilment of specified requirements (see ISO/IEC 17000:2004, clause 5.1);— decision on certification;

Depending on the scheme, decisions can be made regarding;

- **attestation**, which means issue of a statement of conformity, based on a decision following review, that fulfilment of specified requirements has been demonstrated (see ISO/IEC 17000:2004, clause 5.2);
 - Granting the right to use certificates or attestation of conformities
 - Using a certificate for a batch
 - Granting the right to use marks of conformity based on surveillance or for a batch
- **Surveillance** which means systematic iteration of conformity assessment
 - Testing or inspection of open market
 - Testing or inspection from factory samples
 - Assessment of the production, delivery of service or operation of the process
 - Management system audits combined with random tests or inspections

F.2 Content of a scheme

A product certification scheme should specify the following elements:

- a) the scope of the scheme, including the type of products covered;
- b) the requirements against which the products are evaluated, by reference to standards or other normative documents; where it is necessary to elaborate upon the requirements to remove ambiguity, the explanations should be formulated by competent people and should be made available to all interested parties; NOTE Further guidance on how to formulate specified requirements is provided in ISO/IEC 17007.
- c) the selection of the activities (see Table 2) appropriate to the purpose and the scope of the scheme; as a minimum, a certification scheme should include the functions and activities I, II, III, IV and V a);

- d) other requirements to be met by the client, e.g. the operation of a management system or process control activities to assure the demonstration of fulfilment of specified requirements is valid for the ongoing production of certified products;
- e) the requirements for certification bodies and other conformity assessment bodies involved in the certification process; these requirements should not be in contradiction to the requirements of the applicable standards for conformity assessment bodies;
- f) whether conformity assessment bodies involved in the scheme (e.g. testing laboratories, inspection bodies, product certification bodies, bodies auditing manufacturers' management systems) are to be accredited, participate in peer assessment or qualified in another manner; if the scheme is to require that conformity assessment bodies are accredited, the appropriate references should be specified, e.g. that the accreditation body is a member of a mutual recognition arrangement between accreditation bodies;
- g) the methods and procedures to be used by the conformity assessment bodies and other organizations involved in the certification process, so as to assure the integrity and consistency of the outcome of the conformity assessment process;
- h) the information to be supplied to the certification body by an applicant for certification;
- i) the content of the statement of conformity (e.g. certificate) which unambiguously identifies the product to which it applies;
- j) the conditions under which the client may use the statement of conformity or marks of conformity;
- k) where marks of conformity may be used, the ownership, use and control of the marks; the requirements of ISO/IEC 17030 should be applied;
- l) the resources required for the operation of the scheme, including impartiality and competence of the personnel (internal and external), the evaluation resources, and the use of subcontractors;
- m) how the results of the determination (evaluation) and surveillance stages are to be reported and used by the certification body and the scheme owner;
- n) the question of how non-conformities with the certification requirements, which include product requirements, are to be dealt with and resolved;
- o) surveillance procedures, where surveillance is part of the scheme;
- p) the criteria for access of conformity assessment bodies to the scheme and for the access of clients to the scheme;
- q) content, conditions and responsibility for publication of the directory of certified products by the certification body or the scheme owner;
- r) the need for, and content of, contracts, e.g. between scheme owner and certification body, scheme owner and clients, certification body and clients: the rights, responsibilities and liabilities of the various parties should be defined in contracts;
- s) general conditions for granting, maintaining, continuing, extending the scope of, reducing the scope of, suspending and withdrawing certification: this includes requirements for discontinuation of advertising and return of certification documents and any other action if the certification is suspended, withdrawn or terminated;
- t) the way in which the clients' complaints records are to be verified if such verification is part of the scheme;
- u) the way in which the clients make reference to the scheme in their publicity material;
- v) retention of records by scheme owner and certification bodies.

Conformity assessment functions and activities ^a within product certification schemes		Types of product certification schemes ^b							
		1a	1b	2	3	4	5	6	N ^{c,d}
I	Selection, including planning and preparation activities, specification of requirements, e.g. normative documents, and sampling, as applicable	x	x	x	x	x	x	x	x
II	Determination of characteristics, as applicable, by: a) testing b) inspection c) design appraisal d) assessment of services or processes e) other determination activities, e.g. verification	x	x	x	x	x	x	x	x
III	Review Examining the evidence of conformity obtained during the determination stage to establish whether the specified requirements have been met	x	x	x	x	x	x	x	x
IV	Decision on certification Granting, maintaining, extending, reducing, suspending, withdrawing certification	x	x	x	x	x	x	x	x
V	Attestation, licensing								
	a) issuing a certificate of conformity or other statement of conformity (attestation)	x	x	x	x	x	x	x	x
	b) granting the right to use certificates or other statements of conformity	x	x	x	x	x	x	x	
	c) issuing a certificate of conformity for a batch of products		x						
VI	d) granting the right to use marks of conformity (licensing) is based on surveillance (VI) or certification of a batch.		x	x	x	x	x	x	
	Surveillance, as applicable (see 5.3.4 to 5.3.8), by:								
	a) testing or inspection of samples from the open market			x		x	x		
	b) testing or inspection of samples from the factory				x	x	x		
	c) assessment of the production, the delivery of the service or the operation of the process				x	x	x	x	
	d) management system audits combined with random tests or inspections						x	x	
^a Where applicable, the activities can be coupled with initial audit and surveillance audit of the applicant's management system (an example is given in ISO/IEC Guide 53) or initial assessment of the production process. The order in which the assessments are performed may vary and will be defined within the scheme. ^b An often used and well-tried model for a product certification scheme is described in ISO/IEC Guide 28; it is a product certification scheme corresponding to scheme type 5. ^c A product certification scheme includes at least the activities I, II, III, IV and V a). ^d The symbol N has been added to show an undefined number of possible other schemes, which can be based on different activities.									

Table 2 – building a product certification scheme

F.3 Types of schemes

F.3.1 Scheme type 1a - One or more samples of the product are subjected to the determination activities

In this scheme, one or more samples of the product are subjected to the determination activities. A certificate of conformity or other statement of conformity (e.g. a letter) is issued for the product type, the characteristics of which are detailed in the certificate or a document referred to in the certificate. Subsequent production items are not covered by the certification body's attestation of conformity. The samples are representative of subsequent production items which could be referred to by the manufacturer as being manufactured in accordance with the certified type. The certification body may grant to the manufacturer the right to use the type certificate or other statement of conformity (e.g.

letter) as a basis for the manufacturer to declare that subsequent production items conform to the specified requirements.

F.3.2 Scheme type 1b - This scheme type involves the certification of a whole batch of products

This scheme type involves the certification of a whole batch of products, following selection and determination as specified in the scheme. The proportion to be tested, which can include testing of all the units in the batch (100% testing), would be based, for example, on the homogeneity of the items in the batch and the application of a sampling plan, where appropriate. If the outcome of the determination, review and decision is positive, all items in the batch may be described as certified and may have a mark of conformity affixed, if that is included in the scheme.

F.3.3 Scheme type 2 - Periodically taking samples of the product from the market

The surveillance part of this scheme involves periodically taking samples of the product from the market and subjecting them to determination activities to check that items produced subsequent to the initial attestation fulfil the specified requirements.

While this scheme may identify the impact of the distribution channel on conformity, the resources it requires can be extensive. Also, when significant nonconformities are found, effective corrective measures may be limited since the product has already been distributed to the market.

F.3.4 Scheme type 3 - This scheme involves periodically taking samples of the product from the point of production

The surveillance part of this scheme involves periodically taking samples of the product from the point of production and subjecting them to determination activities to check that items produced subsequent to the initial attestation fulfil the specified requirements. The surveillance includes periodic assessment of the production process. This scheme does not provide any indication of the impact the distribution channel plays on conformity. When serious nonconformities are found, the opportunity may exist to resolve them before widespread market distribution occurs.

F.3.5 Scheme type 4 - Periodically taking samples of the product from the point of production, or from the market, or from both

The surveillance part of this scheme allows for the choice between periodically taking samples of the product from the point of production, or from the market, or from both, and subjecting them to determination activities to check that items produced subsequent to the initial attestation fulfil the specified requirements. The surveillance includes periodic assessment of the production process.

This scheme can both indicate the impact of the distribution channel on conformity and provide a premarket mechanism to identify and resolve serious nonconformities. Significant duplication of effort may take place for those products whose conformity is not affected during the distribution process.

F.3.6 Scheme type 5 - Periodically taking samples of the product either from the point of production, or from the market, or from both

The surveillance part of this scheme allows for the choice between periodically taking samples of the product either from the point of production, or from the market, or from both, and subjecting them to determination activities to check that items produced subsequent to the initial attestation fulfil the specified requirements. The surveillance includes periodic assessment of the production process, or audit of the management system, or both. The extent to which the four surveillance activities are

conducted may be varied for a given situation, as defined in the scheme. If the surveillance includes audit of the management system, an initial audit of the management system will be needed.

F.3.7 Scheme type 6 - This scheme is mainly applicable to certification of services and processes

This scheme is mainly applicable to certification of services and processes. Although services are considered as being generally intangible, the determination activities are not limited to the evaluation of intangible elements (e.g. effectiveness of an organization's procedures, delays and responsiveness of the management). In some situations, the tangible elements of a service can support the evidence of conformity indicated by the assessment of processes, resources and controls involved. For example, inspection of the cleanliness of vehicles for the quality of public transportation. As far as processes are concerned, the situation is very similar. For example, the determination activities for welding processes can include testing and inspection of samples of the resultant welds, if applicable. For both services and processes, the surveillance part of this scheme should include periodic audits of the management system and periodic assessment of the service or process.

F.4 Scheme owner responsibilities

1. The scheme owner should be a legal entity.
NOTE: A governmental scheme owner is deemed to be a legal entity on the basis of its governmental status.
2. The scheme owner should be able to take on full responsibility for the objectives, the content and the integrity of the scheme.
3. The scheme owner should maintain the scheme and provide guidance when required.
4. The scheme owner should set up a structure for the operation and management of the scheme.
5. The scheme owner should document the content of the scheme.
6. The scheme owner should ensure that the scheme is developed by persons competent in both technical and conformity assessment aspects.
7. The scheme owner should make arrangements to protect the confidentiality of information provided by the parties involved in the scheme.
8. The scheme owner should evaluate and manage the risks/liabilities arising from its activities.
NOTE: evaluating risks does not imply risk assessments in accordance with ISO 31000.
9. The scheme owner should have adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its activities. Arrangements should be appropriate e.g. for the range of activities and schemes undertaken and in the geographic regions in which the scheme operates.
10. The scheme owner should have the financial stability and resources required for it to fulfil its role in the operation of the scheme.

Annex G: Conformity assessment and testing

Certification, conformity assessment and testing are commonly used interchangeably. To understand what certification is, and how it relates to terms such as conformity assessment and testing, this chapter explains their relation. For a more in depth view, ISO provides a comprehensive overview online: http://www.iso.org/iso/casco_building-trust.pdf.

ISO/IEC 17000 defines conformity assessment as a demonstration that specified requirements relating to a product, process, system, person, or body are fulfilled. A few points to note:

- In line with the terminology of ISO 9000, a service is regarded as a particular form of product
- The methods for demonstrating conformity include testing, inspection, suppliers' declarations of conformity and certification
- Specified requirements include those contained in suppliers' or purchasers' specifications, national, regional or international standards or governmental regulations
- Accreditation of conformity assessment bodies is included within the definition of conformity assessment
- The term *object of conformity assessment*, or sometimes just *object*, is used in the standard to refer to "product, process, system, person or body".

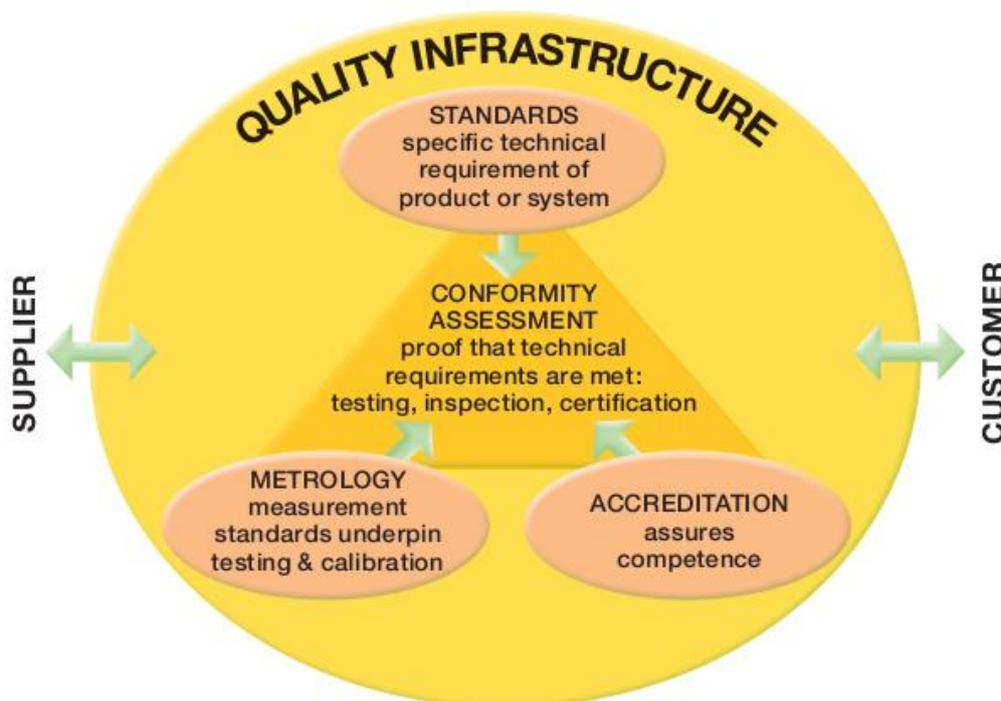


Figure 18 - Conformity assessment quality infrastructure

Conformity assessment is often characterized as part of a quality infrastructure. In addition to testing, inspection and certification, there are other activities which may fall under the umbrella of conformity assessment and there has been considerable international debate on whether activities such as accreditation, production of reference materials and conduct of proficiency testing are conformity assessment activities. Even within the realm of testing, there has been varying opinion on whether some forms of diagnostic testing, such as pathology services, fit the formal definition of conformity assessment. In practical terms, however, all of these various activities are part of the everyday world

of conformity assessment and are important elements in broader national or regional quality infrastructures. Some key components in the definition also have related activities, and subsets. For example, “certification” includes management systems, product and personnel certification. The concept of “testing” includes the related activities of calibration and measurement.⁵²

Too often “conformity assessment” is taken to mean certification and nothing else. In fact, conformity assessment can be undertaken by many people, including the supplier of a product or service, its purchaser and other parties which might have an interest such as insurance companies and regulatory authorities. It is convenient when talking about conformity assessment to refer to the parties as follows:

- First party (1st party) – the person or organization that provides the object which is being assessed
- Second party (2nd party) – a person or organization that has a user interest in the object
- Third party (3rd party) – a person or body that is independent of the person or organization that provides the object, and of user interests in the object.

In general, the conformity assessment techniques described in this chapter can be carried out by a 1st, 2nd or 3rd party. But a 1st party conformity assessment is perceived as less trustworthy than a 3rd party assessment. Therefore, in relation to the risk that nonconformity poses, a choice is made to what parties are allowed to perform the assessment. The SG-IS framework (described in chapter 4.2.1) can help to decide the risk for a specific scenario and associated assurance level.

G.1.1 Conformity assessment activities

The following items are the most common conformity assessment activities.

Inspection is the examination of a product design, product, process or installation and the determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements. Inspection is often conducted on consignments, for example import inspection, to ensure that the whole consignment is equivalent to the product sample tested.

Typical inspection institutions are import inspection agencies and general inspection agencies. These can be public or private agencies and normally compete in the market place.

Testing is the determination of a product’s characteristics against the requirements of the standard. Testing can vary from a non-destructive evaluation (e.g. X-ray, ultra sound, pressure testing, electrical, etc., after which the product is still fit for use) to a to-tally destructive analysis (e.g. chemical, mechanical, physical, microbiological, etc., or any combination of these), after which the product is no longer fit for use.

Typical testing institutions are test laboratories, pathology laboratories and environmental laboratories. These can be public or private laboratories and normally compete in the marketplace.

Certification by a certification body formally establishes, after evaluation, testing, inspection or assessment, that a product, service, organization or individual meets the requirements of a standard.

Typical certification institutions are product certification organizations and system certification organizations. These can be public or private organizations. Competition in the market place is the norm.

⁵² http://www.iso.org/iso/casco_building-trust.pdf

Accreditation provides independent attestation of the competence of an individual or an organization to offer specified conformity assessment services (e.g. testing, inspection or certification). The typical accreditation institution is the national accreditation organization. This is usually a public body with a defined monopoly. There are a few conflicts of interests that have to be considered when establishing a quality infrastructure:

- The accreditation function cannot be carried out by an organization that also provides conformity assessment, i.e. inspection, testing and certification
- The national standards body may also become the national accreditation body, but then it may not provide any conformity assessment services
- Although fundamental metrology and accreditation is not per se a conflict of interest (as defined by the BIPM (International Bureau of Weights and Measures), ILAC and the IAF) it is considered close to being one, and hence UNIDO encourages developing countries to avoid this combination. In particular, a body which accredits calibration laboratories cannot itself provide calibration services.

G.1.2 Conformity, interoperability and functional testing

There are different types of aspects that can be focussed on while testing. The most common are:

- **Conformity testing:** testing to assess the compliance of the test subject to standardised requirements.
- **Functional testing:** testing to assess the ability of the test subject to provide the advertised functionality that is required by the assessment. Functional testing can be part of conformity testing.
- **Interoperability testing:** testing to assess the ability of two or more systems to exchange information and to make mutual use of the information that has been exchanged.⁵³ Interoperability testing can be part of conformity testing.

In respect to smart grid cyber security, all three aspects play a role. Conformity testing needs to be performed to ensure that smart grids comply with requirements set by the EU and Member States. Functional security testing needs to be performed to support the implementation of cyber security in the grid, as conformity testing normally does not focus on the validation of security functions that the device can support. For example, the conformity security requirement is for a device to have access control, but the functional security requirements can be that access control should work in a specific manner. Regarding interoperability testing, it is an important aspect of conformity assessments of communication standards.

For example, an encryption mechanism needs to be interoperable between smart grid devices to be useful. If interoperability testing is skipped for an encrypted communication channel, the system can be conforming to all security requirements, and have been functionally tested, but can still not be able to use the encrypted channel because the devices are not interoperable.

Penetration testing

A more specific form of testing that is common in security tests is penetration testing. This type of testing revolves around the exploitation of possible design flaws and weaknesses to compromise the security of a device. Such tests do not focus on a specific test book, but rely more on the creativity of the tester, and the time there is available to perform a penetration test. Penetration testing can be

⁵³ ITU-T Z.450 - Quality aspects of protocol-related Recommendations - <http://www.itu.int/en/ITU-T/publications/Pages/structure.aspx>

incorporated as part of a functional test, by describing it as a negative test case for a functional requirement. For example, the validation by the following functional requirement can be tested by a penetration test; ‘the device under test shall not provide means to circumvent the access control mechanism’. Such a requirement can be validated by a negative test scenario, where the device will be subjected to a penetration test in an attempt to circumvent the access control mechanism.

Annex H: SOG-IS

The SOG-IS agreement was introduced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.

The agreement was updated in January 2010 and the full text can be downloaded in the section "Agreement" of the Web site. Participants in this Agreement are government organisations or government agencies from Member States of the European Union or EFTA (European Free Trade Association) countries, representing their Member State or country. As of June 2011, the national bodies participating in the agreement are:



Austria, Bundeskanzleramt



Finland, FICORA - Finnish Communications Regulatory Authority



France, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information



Germany, BSI - Bundesamt für Sicherheit in der Informationstechnik



Italy, OCSI - Organismo di Certificazione della Sicurezza Informatica



The Netherlands, NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations



Norway, SERTIT - Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security



Spain, CCN - Centro Criptológico Nacional, Organismo de Certificación de la Seguridad de las Tecnologías de la Información



Sweden, FMV - Försvarets Materielverk



United Kingdom, CESG - Communications-Electronics Security Group

Table 3: participating countries

The participants work together to:

- Coordinate the standardisation of Common Criteria protection profiles and certification policies between European Certification Bodies in order to have a common position in the fast growing international CCRA group
- Coordinate the development of protection profiles whenever the European commission launches a directive that should be implemented in national laws as far as IT-security is involved

The agreement provides for member nations to participate in two fundamental ways:

1. As certificate consuming participants and

2. As certificate producers

For certificate producing nations there are also two levels of recognition within the agreement:

1. Certificate recognition up to EAL4
2. Certificate recognition at higher levels for defined technical areas when schemes have been approved by the management committee for this level.

Certification is based on an evaluation conducted by an evaluation lab that:

- either has been accredited in its country of origin according to ISO 17025,
- or has been established under the laws, statutory instruments, or other official administrative procedures valid in the concerned country, and licenced by the certification body for Common Criteria and specific technologies like those covered by the technical domain SOG-IS MRA.

This process helps to assess whether the evaluation lab has the necessary skills to perform appropriate vulnerability analysis.

Proofs of competency between SOG-IS MRA members are called shadowing and voluntary periodic assessments (VPA) per technical domain. After an initial shadowing, VPAs take place on a regular basis for no longer than five years, and they are performed by two or more SOG-IS MRA members. Formally, the prerequisites for certification bodies to join the SOG-IS MRA are equivalent to the requirements laid down in 765/2008/EC. The VPA reliably demonstrates that a certification body permanently is able to retain its competency in processes, procedures and technologies, and therefore that its certificates remain up-to-date with the evolving cyber threat landscape.

Annex I: Additional identified challenges

Usage of immature standards

As the standard analysis showed (please see chapter 4.4.5), not all standards have been published, and it is not possible to base a certification framework on an unpublished standard. Also, any newly published standard suffers from mistakes that can cause confusion and unclarity regarding implementation and compliancy. We could imagine a mechanism like the “demonstrable conformance” in Common Criteria, which enables the national CBs to adapt a new protection profile whenever it included some mistakes.

In state legislation

It will be a challenge to instate legislation, as it requires the endorsement of multiple stakeholders. This could be solved by discussing with national bodies, if they could accept to bypass some verifications on their EAL4+ smart metering gateway, in case the gateway was certified by another CB on some specific security functions.

Balance of cost/effort and threat

It will be a challenge to balance the cost of certification against the threat, as they are not directly linked, and therefore a device that needs to be cheap, can also require the most stringent security requirements (such as is the case with the smart meter). Cost/benefit is especially bad for low threat certifications (because there is an incompressible set of assurance activities). As smart grid face very sophisticated threats, the balance may be relatively good, but this requires a thorough analysis in the future.

Avoid compliancy cultures

It will be a challenge to prevent the scenario that only obtaining the paper certificate counts (compliance) and no effort is put in actually securing the system. The scheme will have to safeguard against this by the enforcement of certain controls that reward a security based approach above a compliance based one.

Acceptance of a specific scheme

Any particular scheme could be met with resistance from a particular European Member State, if it already has a similar scheme in place, and is unwilling to discard the already developed and active scheme. However, well-thought certification schemes such as Common Criteria imply that vulnerability testing will be performed by independent labs.

Acceptance by stakeholders

A scheme will need to be accepted by the Member States, and international agreements need to be made to accept certificates from other countries, if such systems are not in place yet.

I.1 Challenges identified in ENISA stakeholder discussions

Based on previous stakeholder discussions, the following additional challenges were identified

- *Need for a specific risk assessment methodology*
- *Necessary to train and raise awareness among operators, manufacturers and consumers*
- *Security efforts should not only focus on smart meters but also on substation automation, micro grids, SCADA, telecommunication networks, etc.*
- *Security initiatives: duplicity of topics, lack of visibility, same experts in all initiatives.*

- *Security addressed more as an overlay than as part of the design phase*
- *Need for a coordinating entity on ICS-SCADA and smart grid cyber security and privacy initiatives*

1.2 Common pitfalls

Below are common pitfalls as listed by NIST⁵⁴ that apply to certification schemes, and are relevant for a smart grid security scheme:

1. Use of Certification as a Substitute for Improving Quality of the Product and the Manufacturing Process

As Deming⁵⁵ has pointed out, quality must be designed into the product and assured through an effective and efficient manufacturing process. Certification and other types of conformity assessment processes can provide information on whether the desired end result has been achieved. Since certification usually this occurs late in the manufacturing process, it does not improve the quality of the products.

2. Use of Inappropriate Product Standards

Standards, which cover all essential characteristics of the product necessary to ensure a given level of quality or safety, may not be available or may not be selected for use in a certification program. The introduction of new technology and new products may also be inhibited if there is no provision for handling products which fall outside the scope of the standard. Standards may also contain specifications that are unnecessary and not based on well documented research or information.

3. Lack of Adequate Test Methods

Test methods may not adequately measure all essential product characteristics included in the certification program in a cost-effective manner. In addition, sampling requirements may not be sufficient to ensure that the certified products adequately represent the entire production line.

4. Lack of Technical and Financial Competency on the Part of the Certifier

The certifier may lack the necessary technical competence and resources to properly use and maintain the test equipment and to conduct the certification process. The organization may not have developed adequate written documentation on the certification requirements and procedures or may not have kept adequate records on the results. In addition, the certifier might also have biases which compromise the integrity of the results.

5. Public Misperception Regarding Legal Responsibility for a Certified Product

Legal responsibility for the quality and/or safety of the product generally rests with the manufacturer, despite frequent public misperception that the third party certifier is responsible.

6. Lack of an Adequate Appeals System

Disagreements may occasionally arise among parties participating in a certification program. Some programs do not have an adequate and impartial appeals mechanism to handle disagreements that cannot otherwise be resolved.

⁵⁴ Source: <http://qsi.nist.gov/global/index.cfm/L1-5/L2-45/A-204>

⁵⁵ Deming circle; <http://en.wikipedia.org/wiki/PDCA>

7. Lack of Knowledge on the Part of Users of the Certification Scheme

Buyers who rely on a certification and who are not adequately informed as to the purpose, scope, and technical limitations of the resulting certification may be misled as to the meaning and degree of confidence that can be placed in the certification mark or certificate of conformity.

8. Lack of Adequate Surveillance and Enforcement

Without an adequate process to ensure that any misuse of the certification mark or certificate of conformity is dealt with efficiently and effectively, the mark's integrity may be compromised. Certification programs should take steps to ensure that certified products that are subsequently found not to conform are either recalled from the marketplace or have their marks or certificates of conformity removed.

9. Incompatibilities among National Certification Schemes

As noted above, national certification schemes for the same product or group of products can differ significantly in the standards used and product characteristics that are assessed, the sampling process and the test methods used, and other program aspects. Such differences have the potential to create barriers to trade.



TP-06-14-073-EN-N

ENISA

European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece



doi: 10.2824/36179



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu