Smart Grid Security Certification

Validation workshop, Heidelberg 30 September 2014

Workshop agenda

Session: "Smart Grid Component Certification"	
13:15-13:30	Keynote Speaker The German IT security certification scheme-Bernd Kowalski, BSI
13:30 – 14:15	-Short introduction to the ENISA report: - Focus on: - the comparison criteria - the challenges of Smart Grid Component Certification identified in the Report - Overview of the Challenges
14:15- 14:30	Coffee Break
14:30- 14:45	Keynote Speaker Results of a recent survey on smart meter certification, Willem Strabbing, ESMIG
14:45 - 15:30	Discussion & comments on the Recommendations presented in the ENISA report
15:30 – 15:45	Collection of Feedback and Identification of Next Steps
15:45 – 16:00	Plenary Discussion, Next Steps, Closing Remarks
16:00 – 18:00	Visit of the BASF plant

Agenda

1. **Introduction to the project**
2. Contents of the report
3. Topics for discussion

Introduction to the project

- Objective
- Working method
- Discussions with stakeholders
- Aggregated comment results
- Addressing of the comments

Objectives

- Perform a desktop research
- Identify the gaps between different certification schemes
- Produce technical advice, recommendations and good practices for certification in smart grid security.
- Provide recommendations on how to develop new or improve existing approaches to a pan European harmonised smart grid security certification.

Working method

- Desk research regarding cyber security certification
- Qualitative analysis of cyber security certification schemes
- Recommendations and roadmap development
- Discussion of approach with stakeholders
- Draft report for comments
- Addressing of comments with stakeholders
- Workshop for discussion of main topics
- Final report

Desk research

Separation between certification schemes and other information

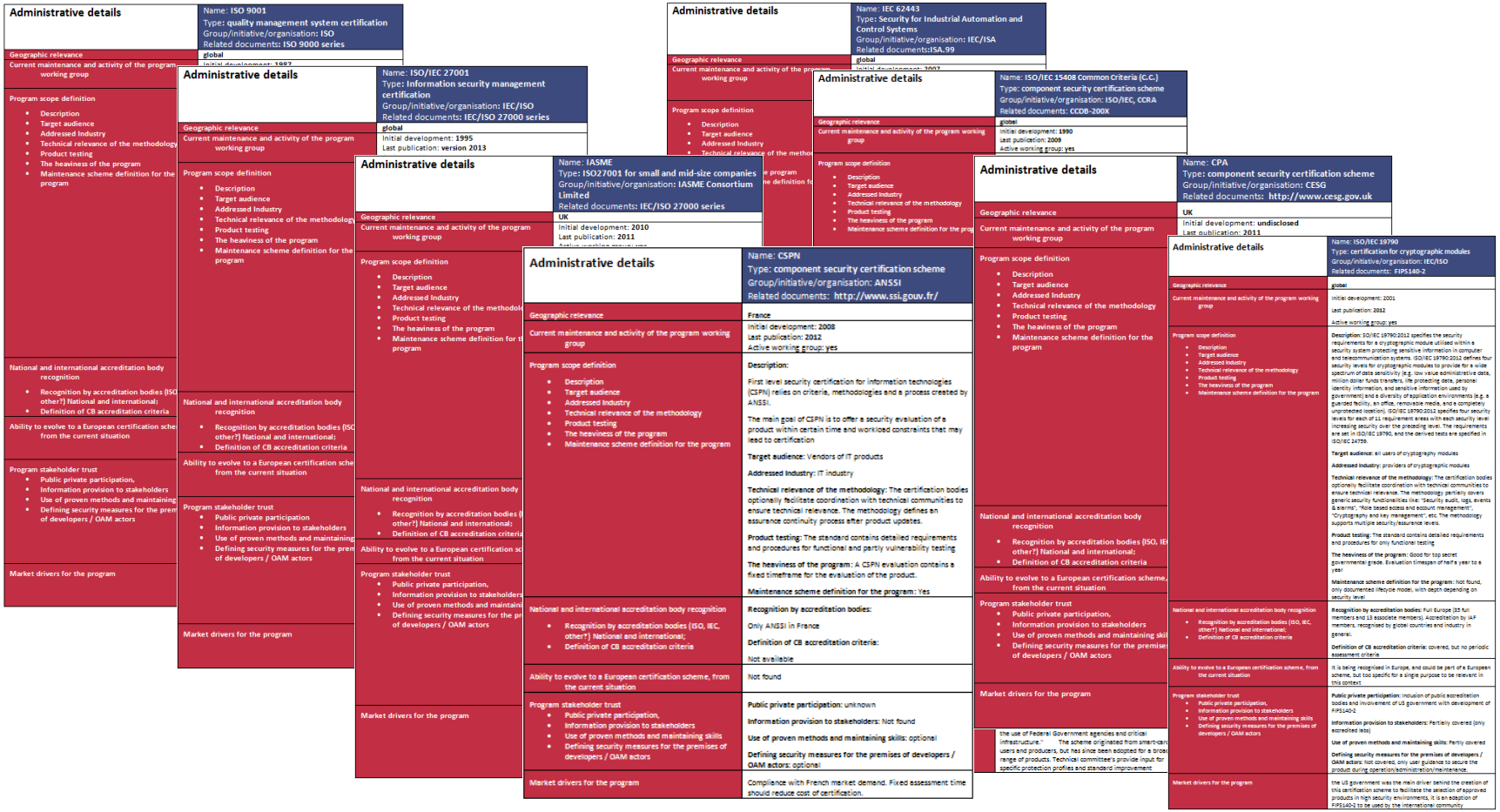
- Articles and investigations
- Security and/or smart grid standards and schemes
- Smart grid related security services
- Current stocktaking lists the following additional sources and initiatives eligible for investigation

Further analysis to select schemes for qualitative analysis:

- 8 out of 19 certification schemes were selected

See Appendix C and D for detailed analysis

Detailed scheme analysis



Discussions with stakeholders

Stakeholders included:

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

Aggregated comment results

- Total of 123 comments
- 88 comments could be processed or revised in the document
- 18 comments needed further discussion
- 17 comments were rejected (mainly due to conflicts with other comments made)

	Organization	Line num	Clause/ Subclause	Paragraph/ Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	
1	EDF R&D	63			General	Specify that the challenges are about achieving harmonized "smart grid security certification approach"	Replace "smart grid certification approach" by "smart grid security certification approach"	Ok, ch
2	EDF R&D	75			General	Define SG-AM and SG-IS, and give references; at least, the first time these acronyms are mentioned in the text.	SG-AM (Smart Grid Architecture Model) and SG-IS (Smart Grid Information Security).	Ok, ch
3	EDF R&D	82			General	Define EA and SOG-IS, or give references		Ok, ch
4	EDF R&D	130-133			General	It is recommended to create a public EU body overseeing smart grid certification, pan European requirements definition and the generation of national protection profiles. It should be responsible for centralised storage and publication of smart grid certificates and adopted schemes, to facilitate clarity on what is certified and how.	What would be the legal aspects of such EU body? How could this EU body acts in the different member states? This role must be accepted by the different member states; Please add an explanation in the Executive Summary Section to explicitly clarify required conditions of the feasibility of such proposal (EU body managing smart grid security certification) even it is mentioned at the end of the document.	Please canno
5	EDF R&D	131			General	It should be responsible for centralised storage and publication of smart grid certificates and adopted schemes	Please add an explanation to explicitly clarify required conditions for the feasibility of such proposal (EU body managing smart grid security certification).	Please canno
6	EDF R&D	135			General	The EU body should be responsible for ratification of national schemes	Please add an explanation to explicitly clarify required conditions for the feasibility of such proposal (EU body managing smart grid security	Please We ca
7	EDF R&D	311			Editorial	Delete ".pdf"		Ok, ch
8	EDF R&D	313			General	Define ESMIG	ESMIG (European Smart Metering Industry Group)	Ok, ch
9	EDF R&D	343-345			General	Add a reference for the statement of SMEG; in which document?		Ok, re
						"There is a need for a European minimum set of controls that can be used for assessing the	I propose to rephrase by "There is a need for a European minimum set of	

- **Most comments were general, some technical, few editorial**

Addressing of the comments

Processed comments

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

Discussed comments

- More complex issues
- Unclear issues

Rejected comments

- Opinions
- Misinterpretations

Agenda

1. Introduction of the project
2. **Contents of the report**
3. Topics for discussion

Main topics in the report

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

What is this report about?

IS NOT

-Proposal for a new certification scheme

-Recommendation for the use of any particular standard

IS

-Creation of a steering working group/ task force

-A proposal for a certification framework (chain of trust)

-A proposal for using an existing reference model (SGAM)

-A mapping between different certification standards and the SGAM layers

-A recommendation to reuse existing mechanisms

-Roadmap to implement the framework

Why to certify?

According to stakeholders:

Create a common reference model for security in EU

Lower costs of smart grid certification

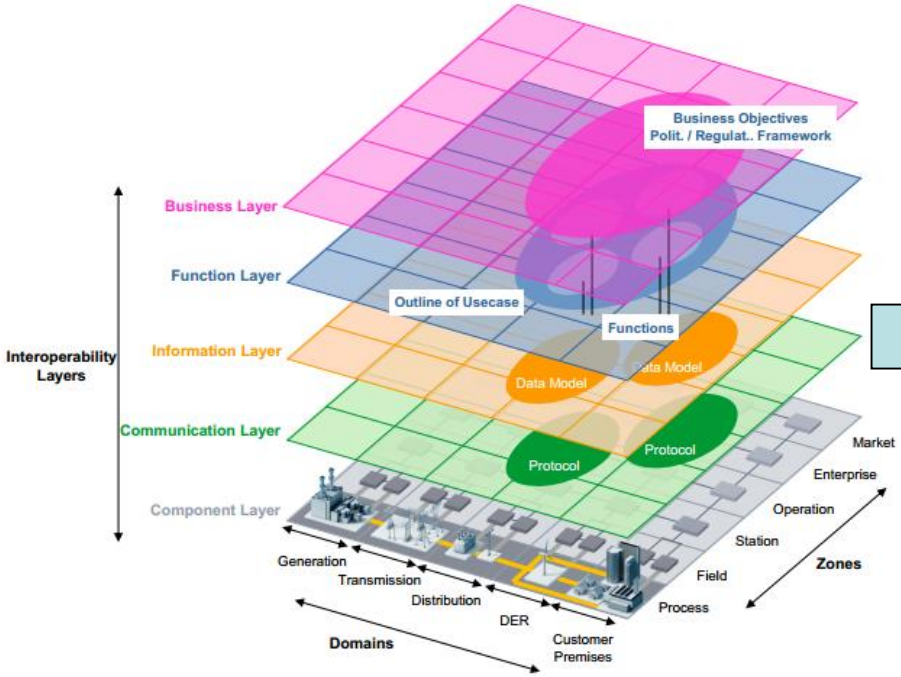
Improve the maturity level of security in the EU smart grid

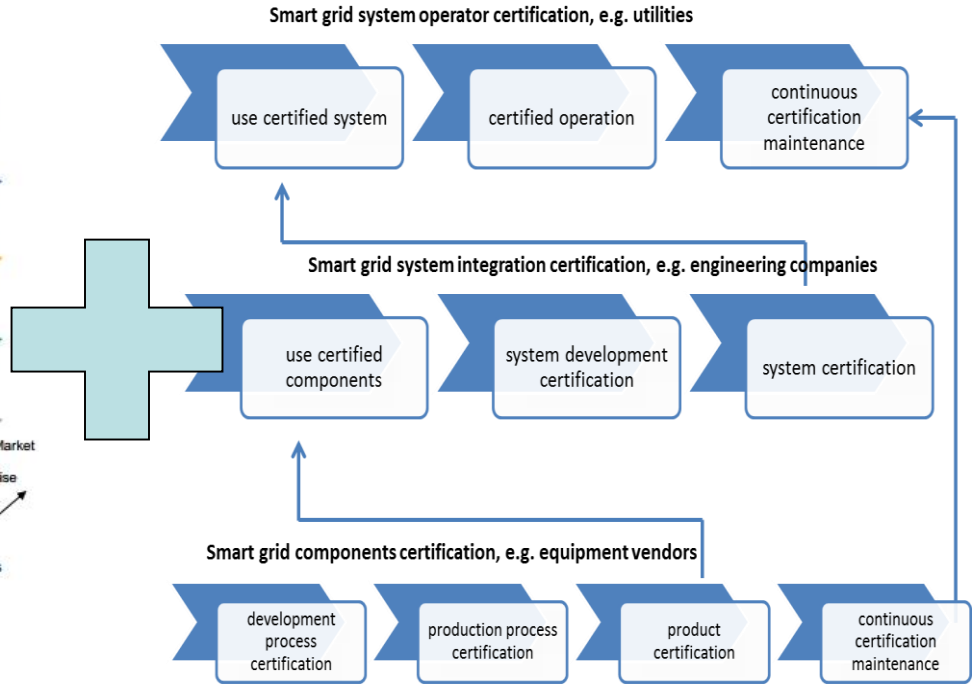
Promote public and private interaction on smart grid security

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

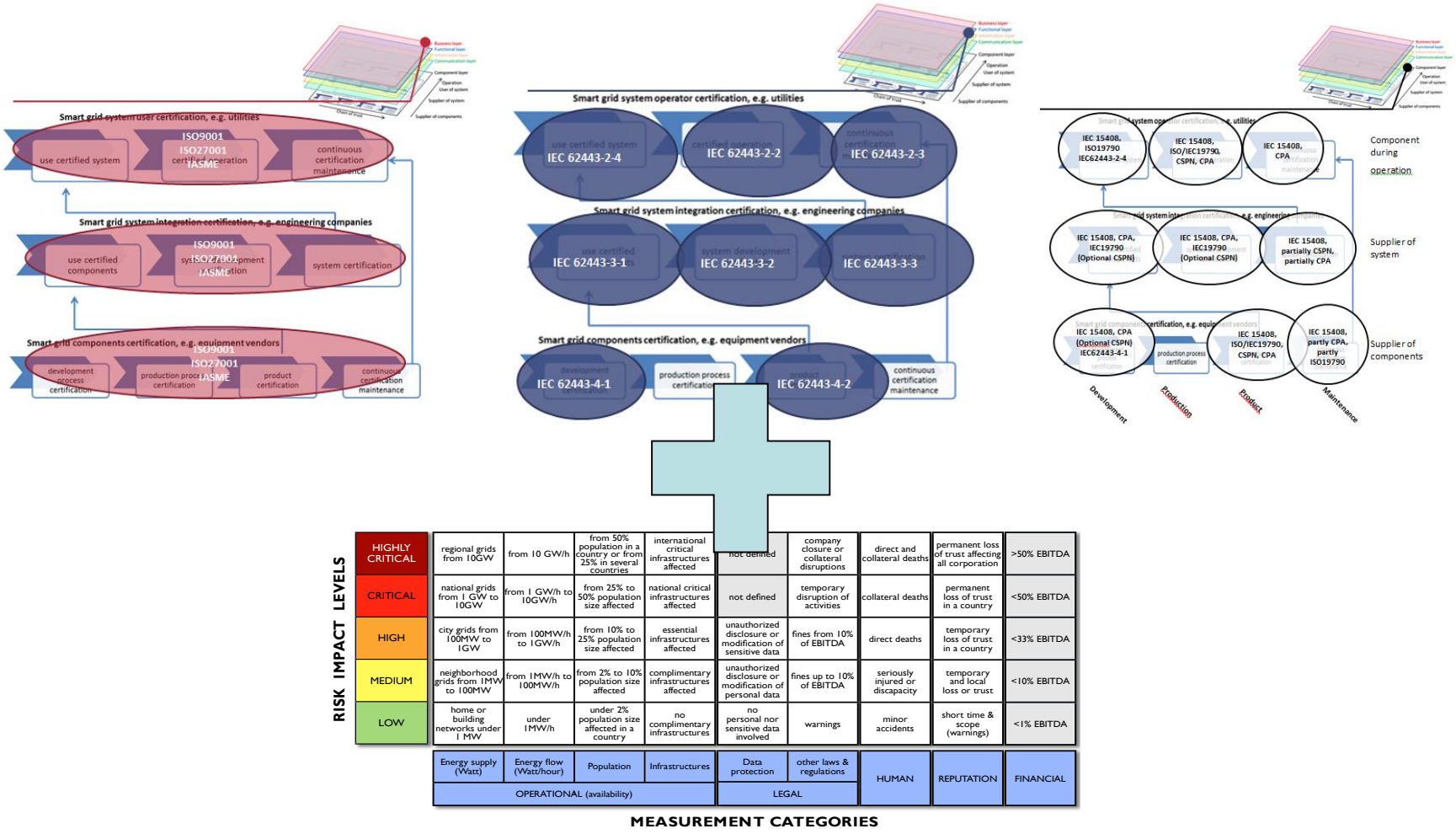
The need: A pan EU smart grid security certification

What to certify: SGAM, lifecycle and chain of trust





What is available: SG-AM/SG-IS usage



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	fines 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	fines up to 10% of EBITDA	seriously injured or discapacity	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

How is it currently applied in EU

- France – CSPN and common criteria, ISO 27002
- Germany – common criteria EAL4+, DIN 27001
- Netherlands – common criteria EAL2, ISO27001
- United Kingdom – CPA, ISO27001, IASME
- SOG-IS MRA and EA (European cooperation for Accreditation)
- No legislation, only Germany is going to mandate ISO27001
- Different requirements and designs per country
- No public-private participation in half of the countries

Conclusion: there is no harmonisation, different methods, schemes and different levels of security per country

The desired situation: Harmonization

A EU based certification scheme should

- **Have a chain of trust that increases trust in the supply chain of the smart grid**
- **Have a common baseline set of requirements recognized by all participating EU member states**
- **Facilitate public and private interaction**
- Contain a common EU smart grid security reference model that is supported by ISO/IEC, EA and SOG-IS
- Use internationally equal security and risk levels based
- Include support for components, systems and operation
- Not be an EU mandated scheme, but a scheme providing EU guidance for implementation
- Improve the maturity of smart grid security in the EU
- Use a chain of trust to provide clarity on what responsibility lies where
- Have a harmonized approach which eliminates the barriers and silos created by fragmented markets
- Address patch management problems and it should include a maintenance scheme

Gap analysis

- **Need a pan EU accepted definition of security levels for smart grid components**
- **Need a common set of EU requirements**
- Need a scheme that enables a pan European approach
- Need EU based approach to facilitate legislation
- Need a centralised place for certificate storage and distribution
- Need a EU body to facilitate public-private interaction and provide guidance scheme implementation and keeping the scheme up to date

Challenges

- **There is no EU body to facilitate public-private interaction**
- There is currently no established model for a smart grid chain of trust in the EU that can be used
- There are no certification schemes for systems certification in Europe
- it will take considerable effort to create a harmonized approach that has consensus
- There is no harmonized approach causing higher costs for certification per country
- There is not one single scheme that can provide EU guidance for implementation, and supporting national legislation

Practical issues

- **A scheme with flexibility for national specific requirements**
- **Scalable for large and small players**
- **Balance of cost/effort and threat**
- **Avoid a false sense of security by only complying to a part of the scheme**
- Pan EU Requirements and security level accepted across EU countries
- Usage of immature standards
- Instating legislation
- Avoid compliancy cultures
- Allow coexistence between legacy and smart grid systems

Recommendations

- It uses a chain of trust that provides transparency and increases trust
- It uses a common reference model based on the combined chain of trust and SG-AM model
- It has a common baseline set of high level requirements and guidelines that are recognized by all participating EU member states
- Have an EU security level based on SG-IS and use case risk assessment
- It uses the currently available standards
- It includes support for components, systems and operation
- Address guidelines for patch management problems and include a maintenance scheme.
- The scheme contains specific national profiles for all topics

Recommendations

National profiles

- **Contain the national specific technical requirements regarding the required security features related to the national use cases**
- Refer to standards for details, amend them to provide the flexibility to incorporate national requirements
- Contain test procedures for the national specific requirements, and provide required testing depth for the national use cases based on the international SG-IS toolbox risk levels

Recommendations

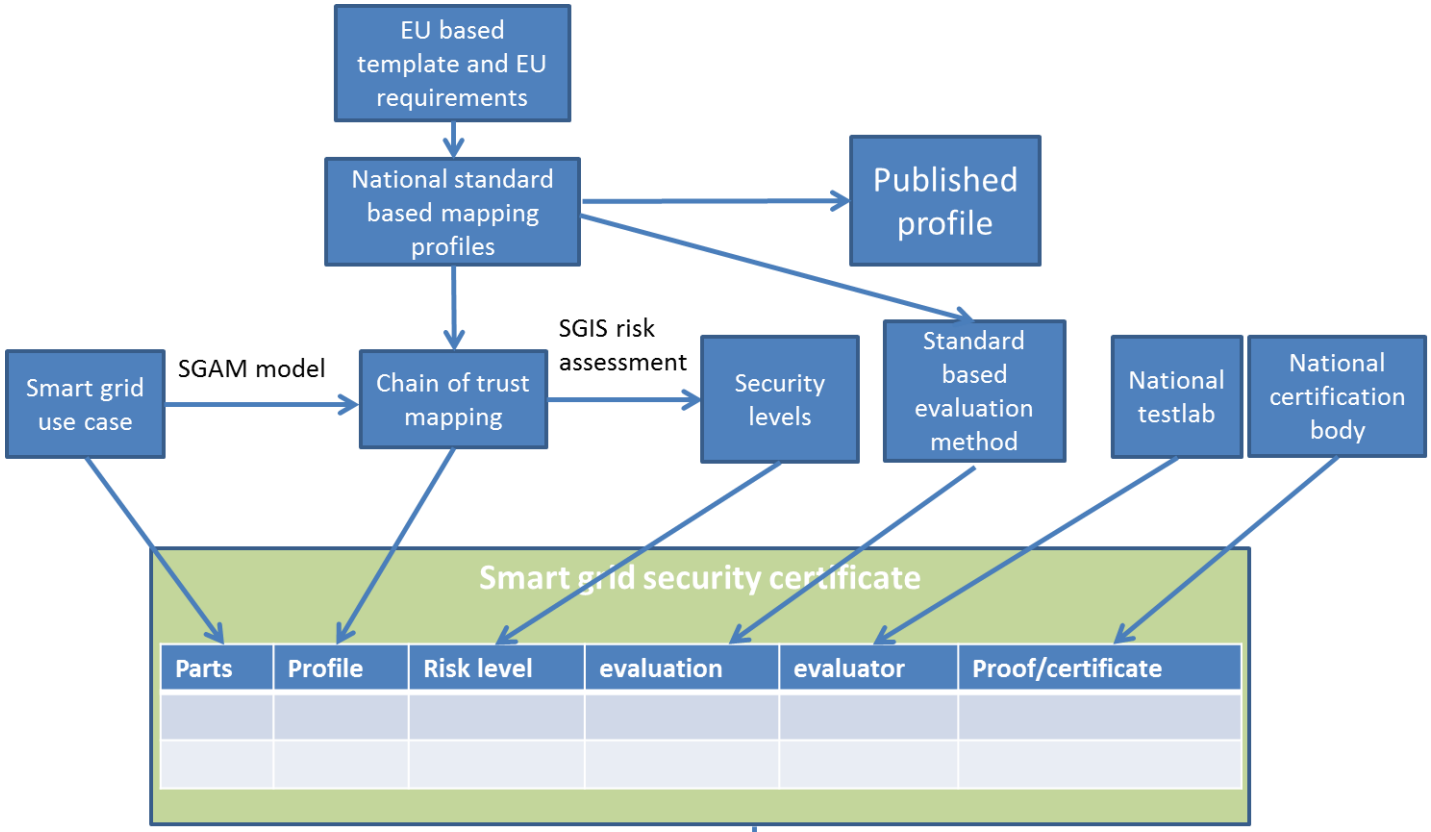
- Create a smart grid certification meta-scheme that provides guidance on an EU level for smart grid security certification
- Ensure the EU Scheme contains elementary properties that national schemes need to comply to
- Each country should be able to map its preferred standard/scheme to the EU scheme properties
- The scheme should provide options for including national requirements.
- Use European accreditation bodies for ratification of national scheme according to EU meta-scheme
- Provide official third party certification and self-assessment tools for pre-assessment
- Updates in schemes should be announced so that they can be incorporated in the national profiles
- The certification scheme should provide guidance and facilitate national legislation.
- There should be promotion of implementation recommendations based on accepted best practices.
- The assessed level of security should be explicit for each certificate

Recommendations

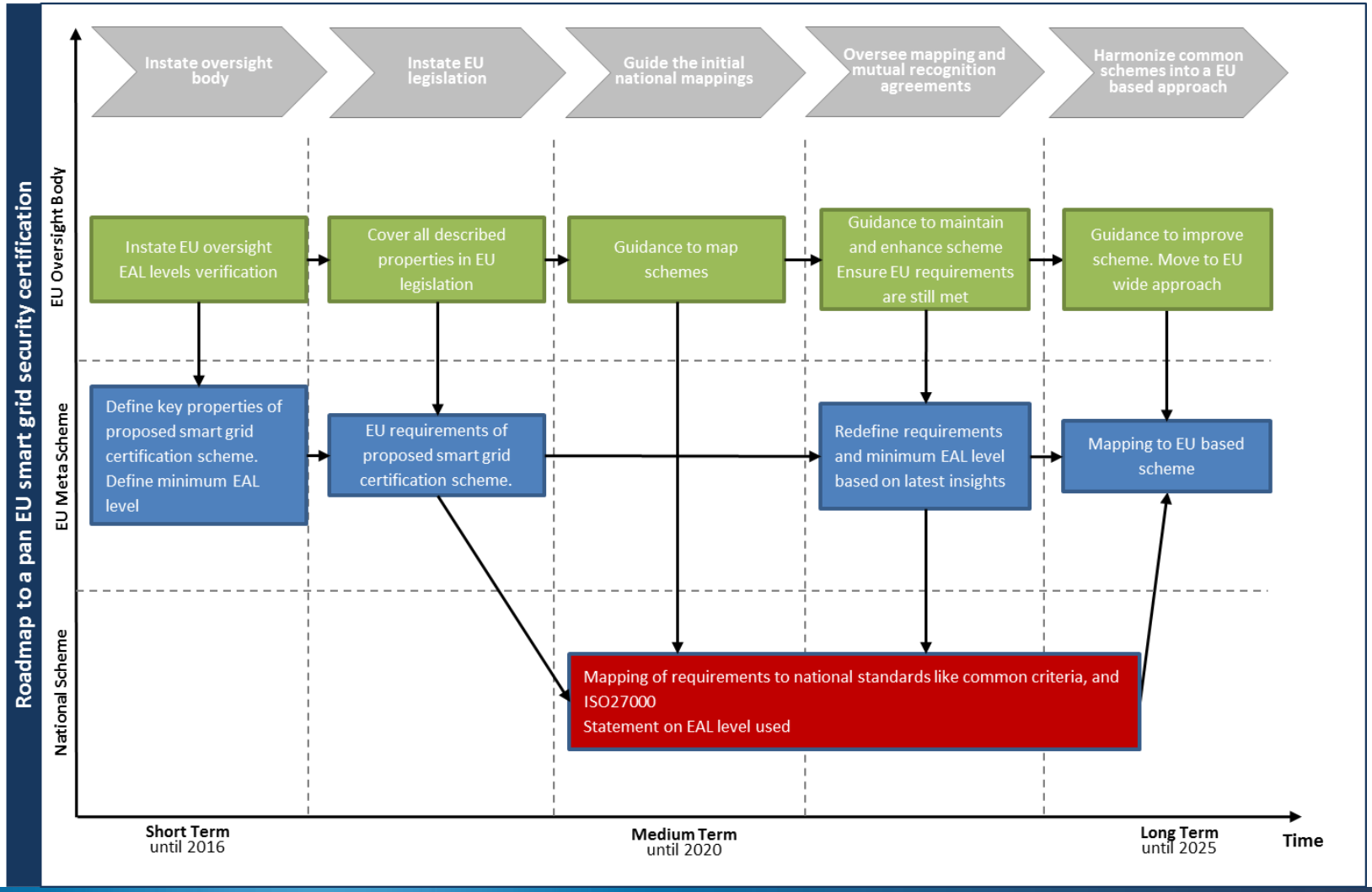
Scheme operation

- **Create an EU body overseeing smart grid certification, requirements definition, and generation of protection profiles**
- **Have the EU body responsible for ratification of national schemes**
- **Have the EU body create a landing page with specific explanations for all stakeholders how to implement the scheme**
- Have the EU body responsible for centralized storage of smart grid certificates
- Have the EU body responsible for centralized storage and publication of a national scheme
- Have the EU body making sure the scheme is kept up to date regarding the latest threats
- Have the EU body provide implementation guidance and recommendations based on best practices and informative standards.

Scheme implementation



Roadmap


Roadmap to a pan EU smart grid security certification
Instate oversight body
Instate EU legislation
Guide the initial national mappings
Oversee mapping and mutual recognition agreements
Harmonize common schemes into a EU based approach
EU Oversight Body
Instate EU oversight EAL levels verification
Cover all described properties in EU legislation
Guidance to map schemes
Guidance to maintain and enhance scheme Ensure EU requirements are still met
Guidance to improve scheme. Move to EU wide approach
EU Meta Scheme
Define key properties of proposed smart grid certification scheme. Define minimum EAL level
EU requirements of proposed smart grid certification scheme.
Redefine requirements and minimum EAL level based on latest insights
Mapping to EU based scheme
National Scheme
Mapping of requirements to national standards like common criteria, and ISO27000
Statement on EAL level used
Short Term
until 2016
Medium Term
until 2020
Long Term
until 2025
Time

Agenda

1. Introduction of the project
2. Contents of the report
3. **Topics for discussion**

proposed elements for discussion and dialog

- Recommendations: what are the gaps?
- Approach: is it clear?
- Roadmap: do we miss something?
- Terminology: “certification scheme”?
- Chain of trust: is it complete?
- SG-AM usage: how far to go?
- SG-IS usage: official or ‘inspired’?
- Legislation: where do we stand on legal aspects?
- System certification: should it be done?

Thank you

With special thanks to

All who took the time to provide their insight and expertise!

Follow ENISA: