SM-CG Sec073_DC

Smart Meters Co-ordination Group
Privacy and Security approach – part II

Version: 1.0
Date: June 2014
Authors: Task Force Privacy and Security of the Smart Meters Coordination Group

MEMBERS OF THE TASK FORCE

Name	Representation	Role
Willem Strabbing	ESMIG, SM-CG, SG-CG	Convenor
Jan Van Cauter	ESMIG	Editor
Eric Farnier	TC294, Eureau	Member
Uwe Pahl	TC294 - WG4	TC 294 liaison
Roman Picard	CRE/CEER	Member
David Johnson	SM-CG, SG-CG	Member
Joost Demarest	TC205 - WG16	TC205 liaison
Juergen Kuhnert	TC205 - WG18	TC205 liaison
Michele Struvay	ETSI-M2M	Member
Marc Vauclair	ETSI-M2M	Member
Olivier Rochon	TC13	Member
Johan Rambi	SG-CG, SG-TF EG2	Member
Michael John	SG-TF EG 2	Member
Marylin Arndt	ETSI-M2M	Member
Colin Blanchard	ETSI-M2M	Member

VERSION CONTROL

Version	Date	Modifications
0.1	20/09/2013	1st draft version by Filip De Belie & Willem Strabbing
0.2	17/10/2013	Update on chapters: 2.2.3. Smart Grid Task Force Expert Group 2 2.2.4. EG2 DPIA template 4.1 Results of DPIA application on SM-CG Use Cases Conclusions
0.3	07/11/2013	Update on chapters: 2.2.1. SGIS in 2013 2.2.2. SGIS Toolbox 3. Repository of security requirements (incl. Annex A): Dutch P&S reqs v2.0 5.1 TC13 (by Olivier Rochon) 5.3 TC294 (by Uwe Pahl) 6 Comparison of security certification schemes: 6.1.4.3: comment on ISO/IEC based schemes in table 2 Annex B: comments on ISO19790 by Michele Struvay (NXP) Whole document: editorial changes by David Johnson
0.4	2/12/2013	Update on chapters: 3.3.6. ISO27001:2005 5.2 TC205 (by Dominique Beck) 5.3 TC294: amended conclusion 5.4 ETSI (by Marylin Arndt) 6 Comparison of security certification schemes: 6.1.2.4 ISO/IEC19790 (by M. Bagnon, ISO/IEC SC27) Whole chapter: reviewed by Trusted Labs Conclusions: amended recommendation 3 & 4 + new recommendation 5 Whole document: editorial changes by David Johnson and Willem Strabbing
1.0	13/06/2014	Include comments from ANEC (by Jan Van Cauter / ESMIG)

CONTENTS

1 Introduction 6
1.1 Background and objectives 6
1.2 Scope 7

2 The approach to defining requirements for standards 9
2.1 Introduction 9
2.2 Definition of Privacy and Security requirements 9
2.2.1 The Smart Grid Information Security Group (SGIS) in 2013 9
2.2.2 The SGIS toolbox 12
2.2.3 Smart Grid Task Force Expert Group 2 14
2.2.4 EG2 DPIA template 15
2.2.5 Identifying requirements for standards and final implementations 17

3 Repository of security requirements 18
3.1 Introduction 18
3.2 Scope 18
3.3 Sources 18
3.3.1 Dutch Privacy and Security requirements of the AMI (version 2.0) 19
3.3.2 U.K. Industry's Draft Technical Specifications 19
3.3.3 SM-CG requirements repository 20
3.3.4 ENISA – Appropriate security measures for smart grids 20
3.3.5 NIST-7628 (U.S.A.) 20
3.3.6 ISO27001:2005 – Annex A – Controls & objectives 21
3.4 Requirements uniformity 21
3.5 Overview of the requirements repository 22

4 Privacy 23
4.1 Results of DPIA application to SM-CG Use Cases 23

5 Status of the work by Technical committees 26
5.1 TC13 26
5.2 TC205 27
5.3 TC294 27

62	5.4	ETSI	29
63	5.4.1	Work on security	29
64	5.4.2	Work on Privacy	30
65	5.4.3	EC Workshops and Expert group Works.	30
66	6	Comparison of security certification schemes	32
67	6.1	Comparison CC – CPA – CSPN – ISO/IEC 19790 & 24759	32
68	6.1.1	Introduction	32
69	6.1.2	Overview of certification schemes	33
70	6.1.3	Roles in certification	37
71	6.1.4	High level comparison of schemes	39
72	6.2	Certification approaches in European member states	48
73	7	Conclusions	49
74	8	References	51
75	9	Annex A: Repository of security requirements	51
76	10	Annex B: Detailed description of security certification schemes	51

77
78

1 INTRODUCTION

1.1 Background and objectives

The Smart Meter Coordination Group (SM-CG) published a Technical Report (TR): "Functional reference architecture for communications in Smart Metering Systems" (CEN/CLC/ETSI TR 50572, reference [1]) that comprises a reference architecture, an overview of communication standards and the work programs of the European Standards Organizations (ESOs) regarding these standards.

Although the standards needed for interoperability of components of the Advanced Metering Infrastructure are dealt with in TR 50572, the privacy of consumer owned data and the security of transactions and data access within the AMI need further attention, given their importance to many stakeholders involved in or influenced by the implementation of Smart Meters.

In the SM-CG plenary meeting on 27 June 2012 it was decided that a new chapter about the approach of the ESOs regarding Privacy and Security should be included in the SM-CG deliverables. A Task Force was formed to define such an approach and give insight in the work planned by the Technical Committees to address privacy and security. The Privacy & Security Task Force produced a first report (Part I) in November 2012 that was finally released in February 2013.

This document represents the results of the additional work initiated in June 2012. It comprises:

- an approach to define requirements for privacy and security standards
- a repository of privacy and security requirements
- the application of the European Data Protection Impact Assessment (DPIA) template to smart metering
- a description of the present status of standardisation work by the SM-CG Coordinating Technical Committees, related to privacy and security
- a comparison of available security certification schemes

The repository of privacy and security requirements forms a basis for:

- Evaluating standards regarding their compliance with these requirements

- Enhancing the Technical Requirements defined by the SM-CG (see reference [4]) that are used to be linked to Use Case steps (see reference [3]).

1.2 Scope

The scope of the work of the Task Force is privacy and security within the boundaries of the functional reference architecture defined in TR 50572 shown below. The approach of the Privacy and Security Task Force in standardisation and the current work of the TCs will focus on the interfaces as shown in this figure.

However, even though the particular architecture being implemented by a member state may respect the M/441 generic reference model, when considering P&S solutions in practice it is essential to take account of all the factors associated with the metering infrastructure concerned (gas, electricity, water or heat), including the specific architecture being adopted by the member state concerned, the nature of the data involved and any differences of approach which may be necessitated by the very different characteristics of battery and mains powered meters.

Although privacy and security issues are related, they require separate consideration. Whilst privacy cannot be assured without adequate security measures, ensuring security will not be sufficient to guarantee privacy.

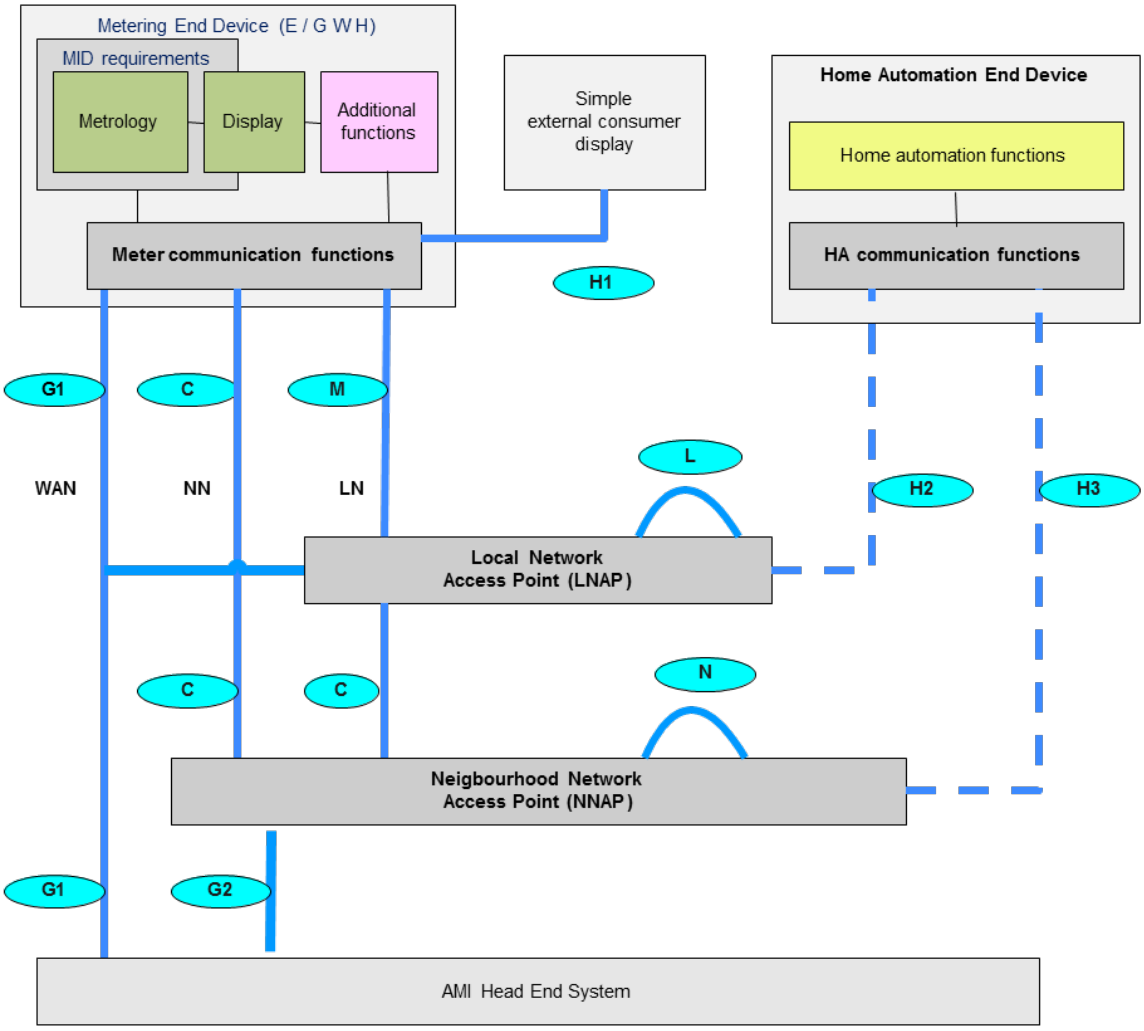

Figure 1 – The SM-CG functional reference model

2 THE APPROACH TO DEFINING REQUIREMENTS FOR STANDARDS

2.1 Introduction

In 2012 the Smart Grid Information Security (SGIS) 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 process of defining or selecting security requirements was described in Part I of the Privacy & Security Task Force report (reference [2]).

A similar approach has been adopted by Expert Group 2 of the EU Smart Grid Task Force. This EG, responsible for *Regulatory Recommendations for Data Privacy and Data Protection in the Smart Grid Environment,* has produced a Data Protection Impact Assessment template, which is also based on use cases and uses risk analysis to help identify measures necessary for risk mitigation. This DPIA (reference [5]) has been used as input for this Part II report to provide an approach for defining or selecting privacy requirements for Smart Metering.

At workshops in July & November 2013 the SM-CG Privacy & Security Task Force, together with members of EG2 and the SG-CG, applied the DPIA template to one of the SM-CG use cases in order to evaluate and improve the approach as regards smart metering. The results of this workshop have been incorporated in the recommendations in this report.

2.2 Definition of Privacy and Security requirements

2.2.1 The Smart Grid Information Security Group (SGIS) in 2013

Currently the SGIS is working with sub teams and each sub team (Work Package) produces its own report.

A single report comprising 4 issues: standards selection, security recommendations, privacy considerations and toolbox application is expected by the yearend 2013.

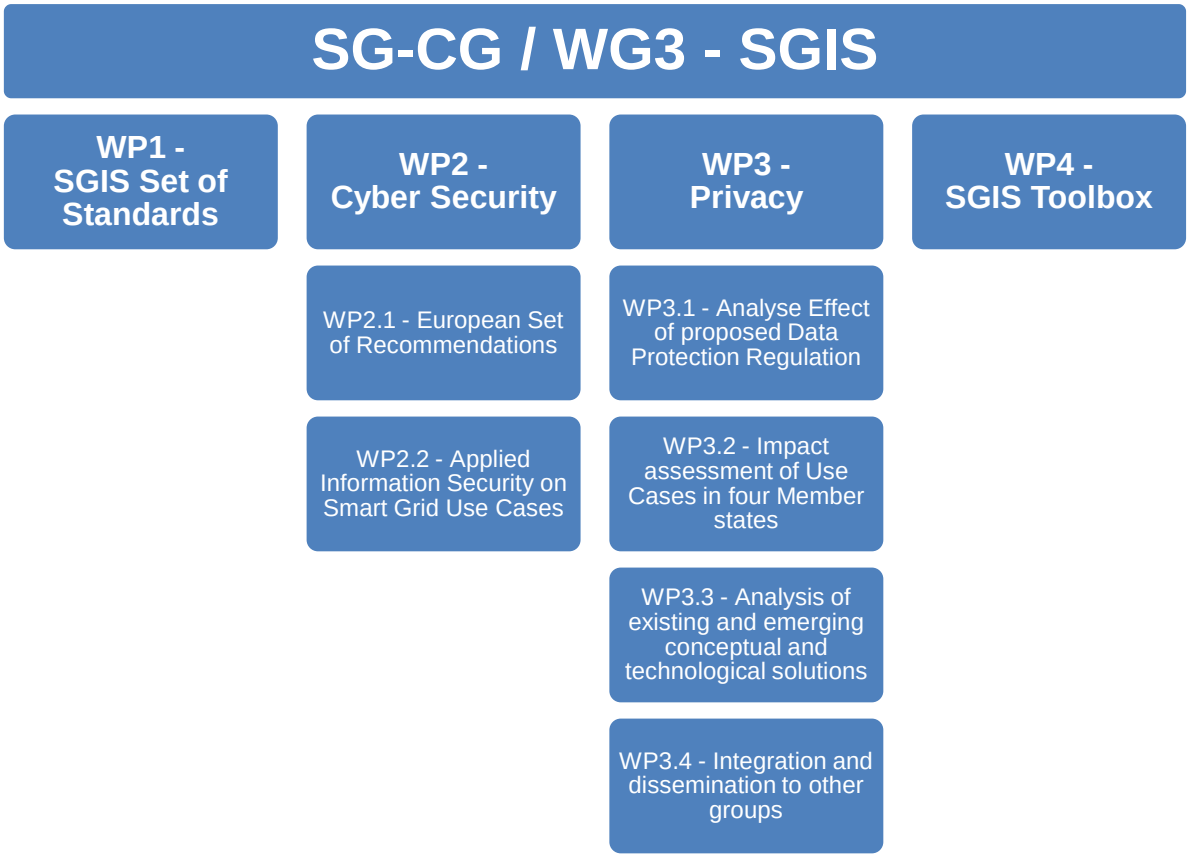

Figure 2 – SGIS organization in 2013

WP1 – SGIS Set of Standards

A draft report for Smart Grid Set of Security Standards has been compiled and circulated within the sub team. Currently addressed standards in terms of overview description, mapping to the SG-CG Smart Grid Architecture Model (SGAM), and gap identification in the report are:

•IEC 62351
•IEC 62443-2-4, IEC 62443-3-3, IEC 62443-4-2
•ISO/IEC 15408 + ISO/IEC 18045

Further investigation into selected standards and potential gaps, based on selected use cases, is due by the end of the year 2013.

WP2 – Cyber security

WP2.1 – European Set of Recommendations

Security recommendations from ENISA, NERC CIP, NISTIR 7628, SM-CG and other team inputs are presented in a final report, which is due mid-December 2013. These proposed recommendations are mapped to the Smart Grid Architecture Model (SGAM).

WP2.2 – Applied Information Security on Smart Grid Use Cases

The SGIS Toolbox v2 (see reference [2] for a description) is applied on Smart Grid Use Cases that are clustered in 3 groups: Substation Automation, DER, and Electric Vehicles. The following deliverables per Use Case will be available: Use Case summary, mapping to the Smart Grid Architecture Model (SGAM), ad hoc recommendations based on Toolbox usage.

WP3 – Privacy

WP3.1 – Analyse Effect of proposed Data Protection Regulation

The current Data Protection regulatory framework is compared with the potential new regime on EU and national level. More specifically, data privacy regulation is reviewed in four Member states. Currently a draft outline document with a first analysis of the market overview has been made. The final report on National Data Privacy Regulation is due at the end of January 2014.

WP3.2 – Impact assessment of Use Cases in four Member states

In two workshops the Data Protection Impact Analysis (DPIA) template developed by EG2 of the Task Force Smart Grids (see 2.2.3) has been applied to specific Smart Metering Use Cases (developed by the SM-CG, see reference [3]) in 2013. The regulation, deployments and market structure of Germany and France were reviewed in detail, and this work was informed by input from the UK and The Netherlands. The results and recommendations from these workshops are intended to lead to the development of an improved approach to data protection within the SGIS toolbox in 2014.

WP3.3 – Analysis of existing and emerging conceptual and technological solutions

In 2013 the WP group has identified potential concepts, technological solutions and described and analyzed potential mitigation solutions. In January 2014 the development of the final report will commence.

WP3.4 – Integration and dissemination to other groups

Throughout 2013 links to EG2 DPIA, Security Levels, Toolbox, European institutions, USA (NIST) and other stakeholders were established. Moreover, a new link to SM-CG AHWG Privacy & Security was introduced in 2013 during a workshop meeting with SMCG, EG2 and WP3 to perform a DPIA on Smart Metering Use Cases.

WP4 – SGIS Toolbox

See following section 2.2.2.

2.2.2 The SGIS toolbox

Version 1

Part I of this document (reference [2]) describes version 1 of the SGIS toolbox in detail.

Version 2 (2013)

SGIS Toolbox v2 update covers the comments received in 2012 and provides additional elements of likelihood analysis. It includes following major changes:

- Updated scope & objectives
- Clear indication of which aspects of risk analysis are covered by v2 of the toolbox and which are for v3
- Update of risk impact categories
- Included an asset list to assist with likelihood analysis
- Included an overview of threat scenarios to assist with likelihood analysis

This version of the toolbox describes in more 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[1] in a use case.

[1] Definition : *An Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization*

The following picture summarizes how the present toolbox is intended to be applied:

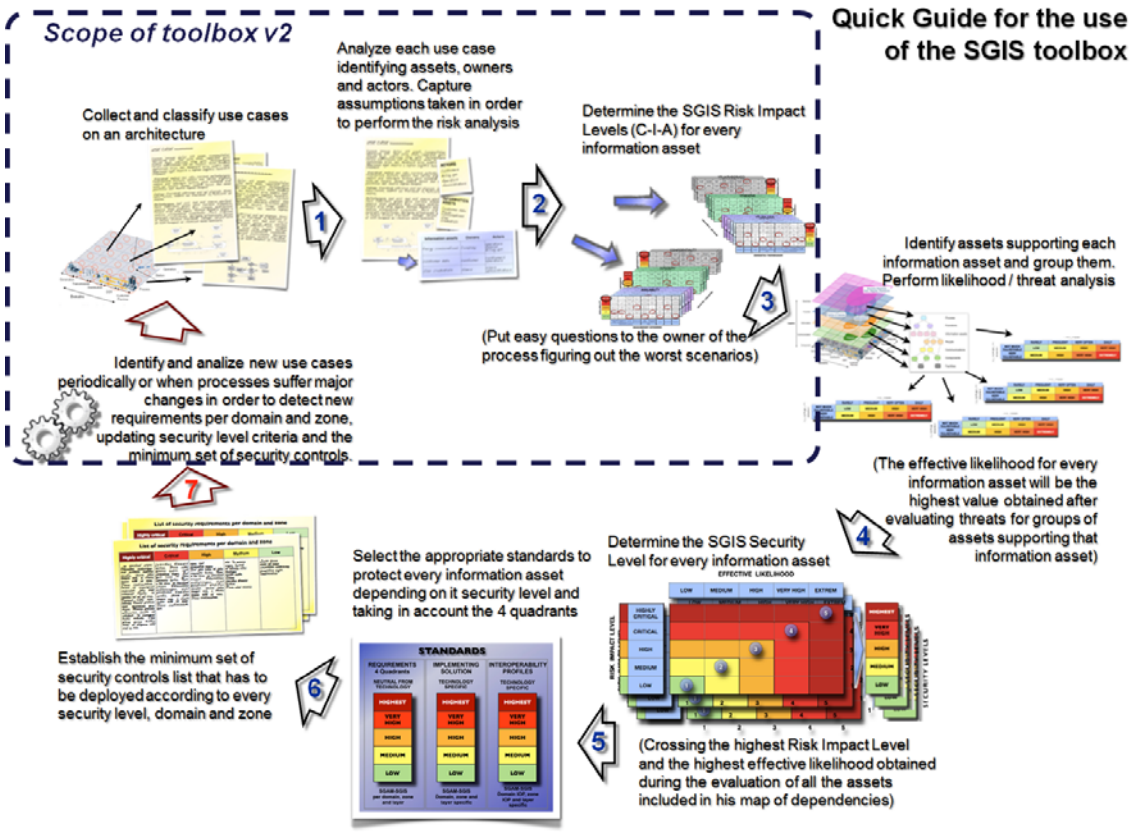

Figure 3 – SGIS toolbox v2.0

The process starts with collecting and analyzing use cases by identifying activities and assets. Based on this description of the functionality, the assets and the operational environment, the approach continues with determining the risk impact level for every information asset.

In the next step of the process the user assesses the likelihood of threats. At this stage of the toolbox, this assessment is based on general user experience. Currently, the toolbox does not contain a model for likelihood assessment. It does however contain a number of elements that may assist the user in the likelihood assessment like, for example:

- an asset list
- a dependencies map

- threat scenario's based on the UK IS1 method

The risk impact combined with the likelihood of a threat occurring to an asset results in a notion of inherent risks.

Version 3 (2014)
SGIS Toolbox v2 is an intermediary step towards a pragmatic risk analysis approach for smart grids. Version 2 already describes elements of how to build a dependencies map for supporting assets, how to perform a threat and likelihood analysis and how to combine impact and likelihood to get the inherent risk as a result.

These "loose" elements will be expanded upon in a consistent threat analysis approach in the next version 3 of the SGIS toolbox, which is planned for Q2 2014. Version 3 will also consider other risk assessment methods and a likelihood assessment model for privacy risks. In the end SGIS Security Levels as countermeasures should lead to appropriate security standards.

As explained in part I of this document (reference [2]), the SGIS toolbox leads to a final selection of privacy and security control/requirements out of a reference list. A reference list for Smart Metering has been included in this document (see chapter 3).

2.2.3 Smart Grid Task Force Expert Group 2

Expert Group of the EU Task Force Smart Grids was working on three deliverables in 2013.

1. Data Protection Impact Assessment (DPIA): Subsequent to the request in Commission Recommendation 2012/148/EU of 9 March 2012 to develop a DPIA template and to submit it to Article 29 Data Protection Working Party (WP29) for opinion, EG2 was tasked to develop this template. After issuing a draft version early 2013, several improvements were suggested resulting in among others: (i) introduction of a risk assessment methodology; (ii) a revised list of Energy stakeholders; (iii) a new clarified list of threats and corresponding controls. EG2 submitted a final version to WP29 in August. Subject to WP29's opinion, the Commission may consider the adoption of the DPIA Template in the form of a Commission Recommendation.

2. Best Available Techniques (BATs): Commission Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems asked for the development of a set of BATs. They focus on the security risks involved with the Commission's common minimum functional requirements for electricity smart metering and identify controls to mitigate these risks. As an additional source for the ad-hoc selection of best available techniques, a set of BATs is being drafted by EG2, with information collected via (i) a questionnaire; (ii) contact points within the organisations and (iii) projects for smart metering system roll-out listed in the JRC inventory.

3. Minimum security measures: This activity is chaired by ENISA, with the support of EC and is based on ENISA's report which identifies minimum measures for security and resilience for the smart grid service providers and completes the Best Available Techniques which focus merely on Smart Metering. The objective is to organize consultations, collect feedback on these measures from relevant stakeholders, to draft minimum requirements. The Commission might consider adopting a Recommendation on minimum cyber security requirements for Smart Grids which could be issued in 2014.

2.2.4 EG2 DPIA template

Background : The Data Protection Impact Assessment, developed and published by EG2[2], comprises eight steps:

Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA

In this step the answers on various questions will identify the need to conduct a DPIA:

Criterion 1: Is personal data involved?

Criterion 2: Is the concerning party a data controller or data processor?

Criterion 3: Is there a specific risk to the individual (article 33)?

Criterion 4: Is it the right time?

Criterion 5: What is the nature of the system/application under review?

Criterion 6: Is there a legal basis for the envisaged data processing operations?

[2] *Expert Group 2 ('EG2') of the EC Smart Grid Task Force ('SGTF')*

Step 2 - Initiation

In this step the basics for conducting the DPIA are arranged:

- Motivation (see step 1)
- Budget
- Human resources
- Support of senior management

Step 3 - Identification, characterization and description of Smart Grid systems / applications processing personal data

Now the system architecture and its components (assets) are described. A distinction is made between primary assets (processes and personal data elements) and supporting assets (hardware, software, networks, etc.). Use Cases are created describing the data exchange among the actors and system components.

Step 4 - Identification of relevant risks

As with the SGIS toolbox, also the DPIA describes a risk analysis. This step will deliver a list of threats that might influence the system and/or its processes.

Step 5 - Data protection risk assessment

Following the threats and feared events, a quantification of severity level and likelihood will result in risk levels related to the threats.

Step 6 - Identification and Recommendation of controls and residual risks

For all the risks identified in the assessment, a treatment will be defined (e.g. modification, retention, avoidance, sharing, etc.). The treatments (controls) should lower the likelihood and/or severity of a risk. Accepted residual risks have to be clearly described, so stakeholders understand the risks that are remaining and can be accepted.

Step 7 - Documentation and drafting of the DPIA Report

Step 8 - Reviewing and maintenance

Since threats are changing over time, it is important to keep a process in place to monitor the threats and related risks and change or define new controls if needed.

2.2.5 Identifying requirements for standards and final implementations

The methods in the former sections show how Use Cases can be used to identify the appropriate Privacy and Security controls/requirements. However, since system architectures and Use Cases may differ per Member State or even within Member States, a final Risk Analysis and definition of requirements can only be done when the ICT architecture and functionalities are fixed. Member states can use the method described and Generic Use Cases to finalise their Use Cases and requirements.

The Generic Use Cases and the reference list of requirements will be maintained by one or more horizontal Technical Committees, so the latest technical and functional developments will be taken in account and the material is updated.

Although they are of generic nature, the Privacy and Security (P&S) requirements identified by the SM-CG Task Force (see chapter 3) are input for the ESOs to check if their standards can meet these generic requirements. It is therefore recommended by the Task Force that the relevant Technical Committees take these requirements as input for their work and select which of these apply to their scope.

When selecting and defining P&S requirements it is important to take notice of the differences between architectures and products used in the scope of the M/441 mandate and the technical and economic feasibility and consequences of implementation. For example certain requirements can be unrealistic for battery powered meters because of the power usage related with the technologies that should fulfil these requirements. Where possible alternative approaches should be explored to mitigate privacy risks where requirements cannot be accommodated.

Furthermore it is important to note that a list of generic P&S requirements can only serve as a guideline for reference purposes by TCs and member states.

3 REPOSITORY OF SECURITY REQUIREMENTS

3.1 Introduction

The SM-CG Privacy & Security Task Force aims to reach a multi-stakeholder, European wide approach for identifying (technological and economic) security and privacy risks for smart metering in order to be able to derive appropriate requirements and countermeasures based on smart meter use cases. This contributes to ensuring interoperability on European level for products and systems in smart metering. It also facilitates greater economies of scale and supports different market models.

As a part of the European approach, the Task Force created a repository of privacy & security requirements related to smart metering. In the current stage of the work, the repository is kept in an Excel file. This section provides background to this repository.

3.2 Scope

The collected privacy & security requirements can be divided into requirements related to the business (governance, processes, organization) and requirements related to the advanced metering infrastructure (functionalities, information, communication and physical requirements).

3.3 Sources

The repository has been built by collecting privacy & security requirements from the following sources:

- Dutch Privacy and Security requirements of the AMI (version 2.0)
- U.K. Industry's Draft Technical Specifications
- SM-CG requirements repository
- ENISA - Appropriate security measures for smart grids
- NIST-7628 (U.S.A.)
- ISO27001:2005 – Annex A – controls & objectives
- Comments from stakeholders

The following section describes which method has been used to select the privacy & security requirements from the sources mentioned above.

3.3.1 Dutch Privacy and Security requirements of the AMI (version 2.0)

Whereas the Dutch Smart Metering Requirements (DSMR 4.0) contain general AMI requirements and requirements derived from NTA 8130 (the Dutch architecture definition), the AMI P&S requirements (version 2.0) formulated by Netbeheer Nederland have a slightly different scope:

- The organisational aspects of setting up and managing the AMI within grid operators' organisations are included in the scope.
- All systems and devices within the advanced metering infrastructure, from the meter up to and including the interface between the grid operators and other market parties (P4), are included in the scope.
- The information types to which these requirements apply are explicitly defined (e.g. connect/disconnect is included in scope).
- The processes to which these requirements apply are explicitly defined (e.g. installation, asset management ...).
- The following elements are deemed out of scope:
    - Smart grids – local devices that control these grids;
    - Advanced grid management using information about domestic consumption;
    - Next generations of PLC communication;
    - Next generations of data communication;
    - 'Meshed-RF'.

The security requirements in version 2.0 have been based on a risk analysis which in its turn was based on a list of high level security goals. These security goals have been defined based on a "rule base" (e.g. security standards, European / national legislation) which was compiled after performing a stakeholder analysis. Additionally, the requirements are linked with identified threats in version 2.

3.3.2 U.K. Industry's Draft Technical Specifications

This document contains an overview of the UK communication architecture and a large number of extended functional requirements, none of which touch on security. There is however a separate chapter listing the security requirements. These were based on a risk assessment.

Important note: The requirements presented in this document are only those that have a functional or technical impact on the design and implementation of a customer premises Smart Metering system. They are not intended to mitigate every risk in the end-to-end system and require the support of the wider requirements set (e.g. many security risks are partially addressed by monitoring controls within the DCC and/or its Users).

3.3.3 SM-CG requirements repository

The security requirements of the Smart Meters Coordination Group, Task Force use cases, were developed based on the SM-CG architecture and use cases and were all taken into this repository (see reference [4]).

3.3.4 ENISA – Appropriate security measures for smart grids

This document provides technical guidance addressing security of smart grid networks and services which are critical and whose malfunctioning would have a significant impact on society. Data privacy issues, however, are considered out of scope of the document.
Since this document was developed based on similar sources as in our requirement repository, there was already quite a lot of overlap. Where gaps were identified, requirements from this guidance document were taken over in the repository.

3.3.5 NIST-7628 (U.S.A.)

Within the smart grid, NIST defines 130 logical interfaces, grouped in 22 interface categories which belong to one of 7 smart grid domains. While some security requirements apply in all cases, some security requirements' applicability depends on the interface category and/or the security level.

The scope of ESMIG's smart metering security approach was mapped to logical interface "U24", which belongs to interface category 18. Security requirements that are not applicable to interface category 18, are marked with "out of scope"; these could in principle be removed from the repository because they are not in scope, but have been left in for reference. The NIST maps the security requirements to three security levels; this mapping is also taken over in this repository.

3.3.6 ISO27001:2005 – Annex A – Controls & objectives

This document provides organizational requirements for information security. This standard is not specific to smart metering / grids but is very good to complement the repository where some gaps were still present. It is also clear that the smart metering specific requirements (see 3.3.1 - 3.3.5) have also taken ISO27001 into account since there is quite some overlap with this standard.

Note that currently the 2005 baseline of the standard is referred to; in September 2013 this information security standard has been replaced by a newer version ISO/IEC27001:2013.

3.4 Requirements uniformity

The requirements of different countries are defined based on a country-specific smart metering architecture. In order to make a consistent repository out of these requirements, the national architecture elements were replaced by the architecture elements of the SM-CG functional architecture as detailed below.

National architecture element	SM-CG architecture
UK - Communication hub	LNAP
UK - Core devices	Smart meter & display
UK - HAN	LNAP
UK - Handheld Device	Handheld device
UK - Smart metering system	AMI
UK - Core devices & systems	AMI
UK - end-to-end system	AMI
NL - Data concentrator	NNAP
NL - Smart metering system	AMI + LNAP
NL - P1	(Port on) Smart meter H1
NL - P2	(Port on) Smart meter M
NL - P3	(Port on) Smart meter G
NL - P4	Interface from Meter Data Collector to other market parties
NL - Central system	HES
NL - Equipment	AMI
NL - Grid operator	Market role operating the AMI

Figure 4 – Architecture element mapping

Furthermore, as can be expected, there was overlap between the different sets of security requirements. This overlap has been identified and removed.

3.5 Overview of the requirements repository

See Annex A

4 PRIVACY

4.1 Results of DPIA application to SM-CG Use Cases

The Task Force has organised and participated in workshops where the Data Protection Impact Assessment (DPIA) developed by EG2 (see section 2.2.4) has been applied to one or more Use Cases developed by the Task Force “Use Cases” of the SM-CG (see reference [3]). This section gives a summary of the results of these workshops. The information can be used as input when performing a DPIA on Smart Metering Use Cases in local/national situations.

As indicated in section 2.2.4, in the first step, six criteria are checked to determine the need for conducting a DPIA. One of the criteria is to check if personal data is involved. Regarding Smart Metering it is important to have a clear definition of the data captured by the meter and for what purpose. The definition of when data is to be considered to be personal should be further explained. Basically it concerns all data that can be linked to an individual, even if this link is made outside the scope of operation of the concerning operator (e.g. meter <-> consumer). Data that cannot be influenced by this individual (e.g. technical characteristics of the meter) is not considered to be personal however.

A data processor also has its responsibilities regarding data protection, even if this organisation only transfers encrypted data. The risk of accessing or manipulation encrypted data only is lower, so the need to protect data is limited. It is the responsibility of a data controller to perform the DPIA, taking into account the responsibilities of the relevant data processors. Typical examples are the DCC as data processor and the retailer as data controller in GB.

In the first steps of the DPIA, the analysis does not have to be in depth since the objective is only to determine if a DPIA has to be performed. Later on separate risk analyses will prompt consideration of what concrete information security and privacy requirements are needed, taking account of the specific risk to the individual, the nature of the system/application etc.

In the third step of the DPIA, the relevant system and information assets are identified.

In the case of Smart Metering the SM-CG functional reference architecture identifies the systems and data interfaces.

Note: The use of the term “Actor” in the SM-CG Use Cases is not exactly similar to the way it is used in the DPIA. While the SM-CG Use Cases make a difference between external and internal actors, EG2 only refers to external actors (for SM-CG the users of the reference architecture) and identifies internal actors (in SM-CG Use Cases: system components) as “Supporting assets”.

In case of remote meter reading (Use Cases “Obtain meter read on-demand” and “Obtain scheduled meter reading” , see reference [3]), the primary assets are meter data elements such as:

Billing data: All data measured by the meter - consumption and demand per tariff, load profiles - that is necessary to establish the bill;

Local generation data and management: Measurement and management data related to energy generated locally;

Supply and load control: status of the switches;

Contractual data: Data generated by the meter related to the contract and contract changes, including price information, payment tokens. This is particularly relevant for smart meters operating in payment mode;

Power quality data: Data measured by the meter related to power quality, like voltage surges, voltage dips, power outages, harmonics;

Tamper data: Data related to tamper events - physical, electromagnetic, metrology, communication related - detected by the meter;

Technical data (meter health): Data related to the operation of the meter, in particular total operating time and per tariff, battery voltage, battery life, number of operations of the supply and load control switches, internal temperatures etc.;

Communication related data: Number of connections, statistics on good and erroneous messages.

In the following steps of the DPIA, identification of the relevant risks and a risks analysis can be performed, based on the Smart Metering

- System architecture (see also SM-CG reference architecture, reference [1])
- System components (internal actors / supporting assets)
- System Users (actors)

- Use Cases (see also SM-CG repository of Use Cases, reference [3])
- Primary assets (see list of data elements above)

Finally when privacy controls are identified (DPIA step 6), these can be linked to the relevant Use Case steps in the column for Technical Requirements. The figure below shows an example where various technical requirements, among which are privacy requirements/controls, are linked with Use Case steps.

Scenario Name :		Basic Flow				
Step No.	Event	Description of Process/Activity	Information Producer	Information Receiver	Information Exchanged	Technical Require-ments ID
1	Actor A decides he wants a particular meter read or meter reads.	The request is sent to the HES.	Actor A	HES	Meter Data Request	
2	HES receives the request	The HES checks Actor A's access rights and triggers a meter read through a pull communication, invoking secondary UC SU3.				TR-Conf 6/7/8/9 TR-QoSn 1 TR-SEC 21 TR-PRIV 3
3	The HES receives the requested data	The HES creates and sends a response message.	HES	Actor A	Metering Data	

Figure 5 – Link between technical requirements and Use Case steps

The figure below shows examples of technical requirements / controls related to privacy that were gathered by the Task Force Use Cases (see reference [4]).

Req. TR-PRIV	Owner	Relevant to use case	Specification
1	TC294	ALL	Data integrity is preserved in all data exchanges.
2	TC294	ALL	Confidentiality of critical data is preserved in all data exchanges
3	TF use cases	BI.01	The actor requesting the meter read information has the right / is authorized to obtain this specific information.
4	TF use cases	BI.02	The frequency of the transmission of the reading does not exceed requirements for billing unless the consumer has given explicit permission.
5	ETSI	ALL	The ETSI M2M gateway (on each interface of the LNAP / NNAP / HES) checks that requested data respects the privacy policy.

Figure 6 – Technical requirements examples

5 STATUS OF THE WORK BY TECHNICAL COMMITTEES

5.1 TC13

The TC13 WG02 Privacy and Security taskforce has been carrying on the work of bringing security extensions to the IEC 62056-x DLMS/COSEM standard, in order to address national security requirements of member states. A new version of the IEC 62056-5-3, 62056-6-1, 62056-6-2 DLMS/COSEM standards has been published this year and provides application layer level cryptographic protection of messages exchanged between DLMS/COSEM clients and servers. The crypto-algorithm chosen is AES-GCM 128 as defined in the NIST SP 800-38D publication and provides authenticated encryption. For the transport of new security keys, the NIST AES key wrap algorithm has been specified.

The DLMS User Association security task force is working to extend the security model with asymmetric cryptography to support end-to-end protection of messages between one or multiple third parties and smart meters via DLMS clients acting as brokers. The new algorithms comply with the NSA Suite B, i.e. elliptic curve digital signature (ECDSA) and elliptic key Diffie-Hellmann key agreement (ECDH) using P-256 and P-384 NIST named curves. Multiple protection layers can be composed and applied by different parties along the communication chain. These protection algorithms can be applied the same way on privacy sensitive data conveyed in COSEM objects. The security level is configurable in relation with the security use cases of the project via security policies and access rights applied to COSEM object attributes and methods both on requests and responses, limiting overhead and providing flexibility.

This on-going work should be completed by the DLMS UA by end of 2013, and then the results will be brought to the IEC.

5.2 TC205

In its plenary in November 2013, TC205 has again endorsed its conclusions laid down in the AHWG PS report V1 (SM-CG Sec0064_DC):

"Security is ensured by the Smart Meter (for H1-interface) and the LNAP / NNAP (for the H2-H3 interfaces), all connection points between home/building and WAN are secured.
Therefore, there is no need for additional security precautions for the SG Demand Side elements that are in scope of TC205 WG16 &18.
Therefore, there is no need for additional security precautions for the SG Demand Side "behind" the gateway"

As priority is set on the development of the Data Modelling standards (prEN50491-11 and prEN50491-12), there will be no additional work on the topic until mid-2014.
However, in a second phase, TC205 WG16 and WG18 look forward to apply the SGIS tool box in order to refine the PS requirements for HBES.

5.3 TC294

This section summarizes the current status of work in CEN/TC 294 succeeding the process referenced in the previous report "Smart Meters Coordination Group Privacy and Security approach – part I (April 2013)" (reference [2]).

In 2012 CEN/TC 294/WG 4 started the work on security amendment. An intensive discussion within the working group showed a conflict between security demands of the smart meter system, which should resist attacks during the long life time of meters and the hard limitation of energy and computation power of a battery operated meter. Therefore no consensus was found, the issue of unsolved security amendment was sent back to the CEN/TC 294 end of 2012.

The following is an extract of the decision for action during last CEN/TC 294 plenary:

DECISION 143/2012 – Assignment on data security requirements (privacy, integrity and authenticity) regarding CEN/TC 294 standards

CEN/TC 294 …

- decides to **allocate the following tasks to the working group CEN/TC 294/WG 4** with respect to security (privacy, integrity and authenticity):

(a) analyse and identify the constraints (technical and economic) for security handling in the metering world within the scope of CEN/TC 294;

(b) elaborate an overview of current levels of security technology for communication;

(c) analyse solutions for key distribution (single/multiple) and key exchange (secret/public and private)

- requests that the outcome of the above assignment shall be documented by CEN/TC 294/WG 4 and reported to CEN/TC 294.

The working process started immediately by expert meetings and web-sessions, tasking subgroups with dedicated items and involving external experts from other domains.

The report tries to value the needs of secure system architecture against the additional effort and cost for the commissioning and operation of such a system.

Major results of the report from analysis and discussion topics:

- Description of constraints in CEN smart metering (technical and economic)
- Identification of State-of-the-art security mechanisms with a subset applicable for Smart Metering
- Overview of potential market roles in future smart metering systems and relationship to measured or process data of meters
- Threats and risks analysis with impact, likelihood and security measures
- Supporting two modes of security architecture - an End to End security (Transparent mode) as well as a separation of security elements for data provided from meter device and data accessed by the operator or consumer (Data processing mode)
- Description of cryptographic algorithms and key management

This report focuses on security elements needed for secure communication between meter and communication partner (gateway).

Conclusion

Based on a risk analysis the report of WG4 recommends the security services Privacy, Data Integrity, Authentication for a smart meter. The Security level should be augmented by services like Key derivation or Key distribution. All security services bases on symmetrical cipher methods like AES128, to consider the power limitation of battery operated devices.

It is noted that a standard for meter communication supporting these security services allows the establishment of a secure smart meter system. However the standard itself is not able to ensure a secure smart meter system.

The report was presented to CEN/TC 294 in the Plenary 13th of November 2013. The TC294 Plenary accepts this report and decides to start a preliminary work item for the realization of the Security amendment of the EN13757-3. This will be handled by the WG4.

5.4 ETSI

5.4.1 Work on security

ETSI TC M2M has developed a general approach about security in close relationship with the M2M architecture, as to be able to include in the architecture itself the security requirements in an End to End Vision. WG2 (architecture) and WG4 (security) have developed specifications that include the link from the “device” to the “service platform” into the network, when this link is

The deliverables specifically related to smart Metering and security in ETSI SmartM2M are:

- ETSI TR 103.118 Machine-to-Machine communications (M2M); Smart Energy Infrastructures security; Review of existing security measures and convergence investigations
  Extension and harmonization of Smart Energy Security Solutions

- Review of security methods provided by deployed standards used in the Smart Energy industry (e.g. IEC 62351, IEC 62443...) or mandated by regulation (e.g. Requirements from the German BSI for Smart Meter Gateways and Secure Element) as well as gaps identified by

the Smart Grid Information Security group for the M/490 mandate, in order to identify areas where ETSI in general and ETSI TC M2M in particular may bring additional value, e.g. by extending or harmonizing security solutions where possible. This could result in recommendations for areas of work shared with other ETSI groups (for potential actions falling outside the scope of TC M2M), new work item(s) proposals, or CRs within the scope of ETSI TC M2M, as applicable.

A Stable draft is expected on S1 2014, that will be communicated to SMCG and SGCG.

5.4.2 Work on Privacy

Note : ETSI TC M2M did not conduct formalized study work on Privacy for the moment, even if requirements and questions have already come, at a general level. Some discussions have been initiated concerning the data coming from geolocalized devices and containing an identifier which is a human owner for example. Their full availability on the Web set up trivial Privacy concerns.

In the work Item : DTR/SmartM2M-00021, with document TR 103.118 under construction, .a paragraph related to Privacy for Smart Metering and Smart grid Communication and Information System chain will be included, in collaboration with utilities and with energy equipment manufacturers, working in their Technical committees (CLC TC13, CLC TC 205, CEN TC294).

5.4.3 EC Workshops and Expert group Works.

An expert group mandated by the EC DG CNECT for evaluating the needs for setting in place the Internet of Things, has made a study to evaluate how the individual end user can slow down the process when he does not trust the system or if he experiences privacy concerns.

All the public information on the Internet of things can be found on the Digital Europe website at http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation
The public consultation was held between April and July 2012 (see IP/12/360). 600 people, associations and various groups from academics and civil society, as well industry players responded to the consultation. Through the public consultation, the Commission sought views on an a policy approach to foster a dynamic development of Internet of Things in the digital single market while ensuring appropriate protection and trust of EU citizens.

The chapter 7 related to Security and Privacy can be consulted at the address :
http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

The document addresses propositions of European policy, with needs of standards for Security, and Code of Conduct book for Privacy.

797 Note : TC M2M delegates and security experts working in various ETSI TCs including TC
798 M2M, participate actively to tasks related to security including M441, M490 and M462,
799 and are often individually requested to provide expertise into their National Body
800 (example : DIN, AFNOR, AENOR, etc). Moreover they also participate to Workshops and
801 Studies organized by the European Commission.
802 (examples tbd)
803
804

6 COMPARISON OF SECURITY CERTIFICATION SCHEMES

6.1 Comparison CC – CPA – CSPN – ISO/IEC 19790 & 24759

6.1.1 Introduction

Acronyms

CC	Common Criteria
CPA	Commercial Product Assurance
CSPN	Certification de Sécurité de Premier Niveau
CEM	Common Criteria Evaluation Methodology
PP	Protection Profile
EAL	Evaluation Assurance Level
OAM Actor	Operation / Administration / Maintenance Actor
SPD	Security Problem Definition
CB	Certification Body
ANSII	Agence Nationale de la Sécurité des Systèmes d'Information
CCMC	Common Criteria Maintenance Committee

Scope and objectives

The objective of this chapter is to describe security certification schemes[3] related to information security, looking at requirements they define for developers of a product and on relevant inherent features of the schemes. The document attempts to summarize the most relevant differences between the security certification schemes in scope, without implying that one scheme would be better than another. It is up to regulators and the market to decide which certification scheme enforces the required level of trust in a given situation.

One key aspect in this document is to distinguish the technical aspects of the testing or evaluation standard which a specific security certification scheme may be using from the legal foundation and international recognition of the scheme itself.

[3] *Currently there are no certification schemes in the privacy area.*

The schemes in scope are:

- *Common Criteria* (CC), which is an international scheme
- *Commercial Product Assurance* (CPA), which is a scheme from Great Britain
- *Certification de Sécurité de Premier Niveau* (CSPN), which is a French certification scheme.

6.1.2 Overview of certification schemes

The following section briefly explains the scope, organization and evaluation methodology of the certification schemes in scope.

6.1.2.1 Common Criteria (CC)

Scope

Common Criteria are 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.

Organization

The scheme is maintained under and 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.

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

6.1.2.2 Commercial Product Assurance (CPA)

Scope

CPA[4] (Commercial Product Assurance) is a national GB scheme intended for commercial security products. CPA is defined and maintained by CESG (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,

[4] *CPA is a recent scheme and is still under modification. Some of the information in this report may change in the future.*

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 Of-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 CESG 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.

6.1.2.3 Certification de Sécurité de Premier Niveau (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 compliance and 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 part 2&3) the developer uses guidelines described in CSPN. CSPN also has common features with CPA, especially the domain-specific approach.

6.1.2.4 ISO/IEC 19790:2012 and ISO/IEC 24759:2013

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, like 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.

6.1.3 Roles in certification

The following play a role in the certification process:

- The **developer** of the evaluated product must ensure that he himself as well as his product complies to a set of requirements;

- The **evaluator** assesses whether the developer and the evaluated product complies to a set requirements;
- The **certification body** accredits the evaluator and emits the certificate for the evaluated product. In case of CC, it needs to comply to certain requirements;
- The **certification scheme** is a separate entity in case of CC (see below).

The **actor in charge of Operation / Administration / Maintenance** (OAM) of the evaluated product, is himself not evaluated, but is an important stakeholder since several requirements will relate to guiding and supporting him.

The figure below summarizes the role and relation between these actors.

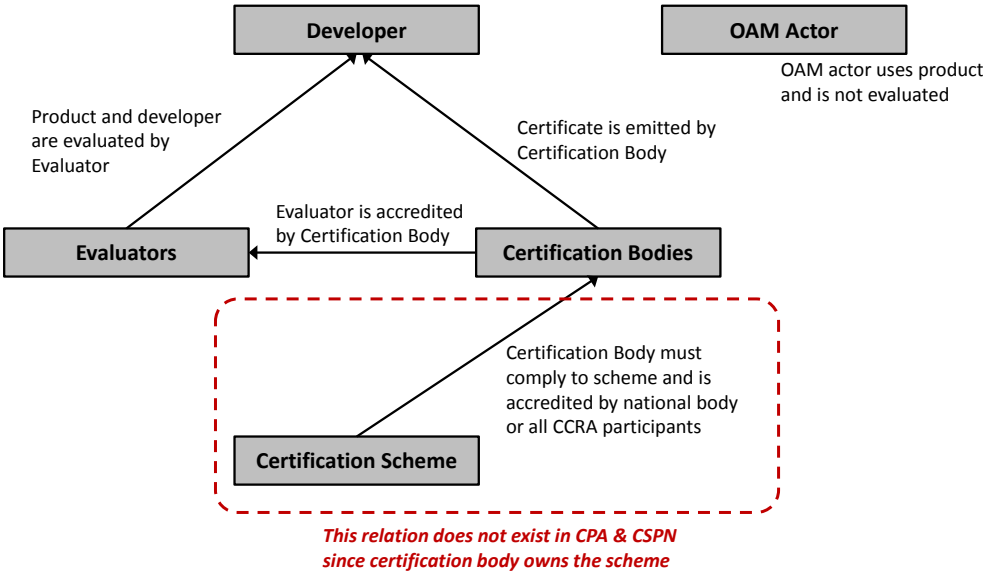

Figure 7 - Roles in certification

The developer, evaluator and OAM-actor play similar roles in CC, CPA and CSPN.

In CPA and CSPN, the certification body is owner of the certification schemes, which implies that the certification body does not need to comply with specific requirements. In CC at the other hand, the certification scheme is managed by a separate body, the Common Criteria Management Committee (CCMC). Since in this case, one certification body does not “own” the scheme, it has to follow the requirements of the CC Recognition Agreement (CCRA) and be accredited by a national accreditation body (or by all CCRA participants) before being able to issue certificates and accredit evaluators.

6.1.4 High level comparison of schemes

6.1.4.1 Introduction

The very principle of existing security certification schemes consists in guaranteeing confidence:

- In a set of certified products or services;
- Between several actors of a given domain or activity (particularly the providers of products and services).

In the smart metering domain, some actors have a **"need for trust"** regarding the products or services they will use (e.g. the consumer, the regulatory actors, the utility, etc…). Some actors symmetrically have a **"need to be trusted",** such as developers and actors operating, administrating and maintaining the system (OAM actors).

The criteria used to compare certification schemes will be deduced from the trust relationships they have to enforce.

A certification scheme typically enforces:

1. **Trust in the products or services**;
2. **Trust in developers and OAM actors**. Trust in these actors is obtained through assurance by evaluators and certification bodies. This assurance is valid only to the extent that the certification **scheme can be trusted**.

Following the above, the two key questions that a certification scheme typically addresses are:

1. **How to enforce trust in products or services?**
2. **How to enforce trust in the certification scheme itself?**

In the following tables, we will compare 4 certification schemes (CC – CPA – CSPN – ISO/IEC 19790 & 24759) on how they address these questions.

6.1.4.2 Enforcing trust in products

The following are elements that contribute towards the developer enforcing trust in his products:

1. Implement security requirements which cover a threat analysis;

2. Test their products;
3. Define security measures to prevent unauthorized access or modification of products / services within their premises;
4. Use proven methods and maintain skills within their teams;
5. Provide the end-user with security-related information and obligations and commit on flaw remediation delays.

In the following table, these points are described more in detail. Furthermore, for each criterion, we indicate whether or not it is fully or partially covered by each of the certification schemes. Note that Annex B contains more information on the elements below. Also note that as stated above, the extent to which criteria are covered by the schemes in scope does not imply that one scheme would be better than another. It is up to regulators and the market to decide which certification scheme enforces the required level of trust in a given situation.

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

	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."*	(depth depends on EAL)			
	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.*	Fully covered (depth depends on EAL)	Not covered	Fully covered	Not covered
	The certification scheme requires that **developers are properly trained** on security related subjects.	Optional	Optional	Fully covered	Not covered
	The certification scheme demands that **sufficient user guidance** is being provided to actors responsible for operation / administration / maintenance of the system.	Fully covered	Fully covered	Fully covered	Fully covered
	The certification scheme requires a **flaw remediation procedure** tracking (amongst others) product flaws, their effects, corrective measures, etc.	Fully covered (depth depends on EAL)	Not covered	Fully covered	Not covered
	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.	Fully covered (depth depends	Not covered	Not covered	Fully covered (depth depends on security level)

		on EAL)			
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.	Fully covered (depth depends on EAL)	Not covered	Fully covered	Not covered

1070 **Table 1 - Enforcing trust in products**

6.1.4.3 Enforcing trust in the certification scheme itself

As noted above, trust in developers and their products is obtained through assurance by evaluators and certification bodies. This assurance is valid only to the extent that the certification scheme itself can be trusted. In order to achieve this, the scheme can:

1. Strive for (national / international) recognition
2. Define strong criteria for accreditation of the Certification Body
3. Provide sufficient information to stakeholders
4. Guarantee the technical relevance of the methodology
5. Guarantee the business relevance of the methodology

In the following table, these points are described more in detail. Furthermore, for each criterion, we indicate whether or not it is fully or partially covered by each of the certification schemes. Note that Annex B contains more information on the elements below. Also note that as stated above, the extent to which criteria are covered by the schemes in scope does not imply that one scheme would be better than another. It is up to regulators and the market to decide which certification scheme enforces the required level of trust in a given situation.

Criteria	Description / sub criteria	CC (under the CC Recognition Agreement)	CSPN	CPA	ISO/IEC 19790 and 24759 (under the EA multilateral agreement)
Recognition	Scope of the recognition agreement	Inter-national (17 authorizing members and 9 consuming members)	National	National	Full Europe (35 full members and 13 associate members)
Definition of CB accreditation criteria	The recognition agreement organization defines requirements for accreditation of individual Certification Bodies.	Fully covered	N/A	N/A	Fully covered
	The recognition agreement organization defines criteria for periodic assessment of Certification Bodies' continued compliance to accreditation requirements.	Fully covered	N/A	N/A	Not covered
Information provision to stakeholders	The recognition agreement organization publishes certificates and provides information on accredited certification bodies.	Fully covered	N/A	N/A	Partially covered (only accredited labs)
Technical	The certification bodies facilitate coordination with	Fully covered	Optional	Fully	Fully covered

relevance of the methodology	technical communities to ensure technical relevance.			covered	
	The methodology covers generic security functionalities like: “Security audit, logs, events & alarms”, “Role based access and account management”, “Cryptography and key management”, etc.	Partially covered	Not covered	Not covered	Fully covered
	The methodology or recognition agreement defines an assurance continuity process after product updates.	Fully covered	Fully covered	Not covered	Not covered
	The methodology supports multiple security/assurance levels.	Fully covered (Evaluation Assurance Levels)	Not covered	Not covered	Fully covered (security levels)
Economics	The scheme includes measures to limit the cost and/or workload and/or duration of evaluation	Not covered	Partially covered (fixed time)	Partially covered (fixed lab fees)	Not covered
Scope	The certification scheme applies to a wider product scope	Fully covered	Partially covered	Partially covered	Not covered (only applies to cryptographic modules)

Table 2 - Enforcing trust in the scheme

6.2 Certification approaches in European member states

A survey has been performed by ENISA in cooperation with the Task Force among EU member states, to gather information on existing certification approaches or concrete plans to develop such approaches. The outcome of this survey was that Germany, GB and France are considering the approaches as described in section 6.1.2. Both GB and France have indicated that they might consider the CC approach in a later stage when this approach can be adopted according the local requirements. Other countries did not take a decision yet, but those that are looking at certification schemes, concentrate on CC.

At an ENISA workshop in 2012 the conclusion was drawn that a majority of stakeholders (from various member states), would prefer a European approach in favor of multiple different national approaches.

7 CONCLUSIONS

Having considered Data Protection Impact Assessment for Smart Metering Use Cases and collected new Technical Requirements from various sources, the Task Force came to the following conclusions regarding its further work.

The exercises to apply risk analysis to the SM-CG Use Cases generate valuable information about the process to define or select the appropriate privacy and security requirements and controls.

> **Recommendation 1:** Task Force to continue with applying the (newer versions of the) SGIS toolbox and DPIA template to Smart Metering Use Cases in order to improve the process for selection of the appropriate requirements/controls and evaluate the list of requirements made available by the SM-CG.

At the time of writing this report, Expert Group 2 of the Smart Grid Task Force and WP3 of the SGIS were still working on the DPIA and related lists of privacy threats and controls. Furthermore EG2 was working on the list of Best Available Techniques to approach privacy risks. The SM-CG repository of Technical Requirements does not contain the latest list of privacy related controls and Best Available Techniques created by EG2.

> **Recommendation 2:** Task Force to extend the SM-CG repository of Technical Requirements with the latest Privacy controls and relation to the Best Available Techniques identified by EG2.

When performing a risk analysis it seemed to be important to be able to link the final selected requirements and controls to identified threats. List with commonly recognized threats related to Smart Metering and Smart Grids are becoming available through the risk analyses in some EU Member States and the work of the SGIS group in the SG-CG and EG 2.
Furthermore the study of certification approaches, such as Common Criteria, showed that a link between security requirements and threats is needed, in order to understand which threats can be mitigated when complying with specific requirements.

Recommendation 3: Task Force to define a reference list of security threats and link the security related Technical Requirements in the SM-CG repository to the identified threats. Consideration will also be given to privacy threats.

Various stakeholders from EU member states have indicated that they would prefer a European approach for certification of AMI components on privacy and security aspects. Some states have adopted approaches based on Common Criteria or similar schemes. CC is based on the ISO/IEC 15408 standard, but has additional rules to follow in order for certificates to be accepted in specific EU countries (currently not EU wide). Certificates based on ISO/IEC standards would be accepted under the general EU rules in all EU countries.

Recommendation 4: Task Force to investigate if and, if yes, how a European approach should be developed for certification of AMI components on security aspects. Currently there are no certification schemes in the privacy area.

The Smart Grid Coordination Group continues its work in 2014 and the SGIS working group will further evaluate security standards, privacy recommendations / regulations and develop the risk analysis toolbox.

Recommendation 5: Task Force to continue its cooperation with the SGIS working group in order to evaluate and improve the applicability of its deliverables for Smart Metering.

8 REFERENCES

[1] SM-CG report “Functional reference architecture for communications in Smart Metering Systems” (CEN/CLC/ETSI TR 50572)”

[2] SM-CG report Privacy & Security for Smart Metering Part I (SMCG_Sec0064_DC_SMCG_PSreportfinal V1.0)

[3] SMCG_Sec0060_DC_UseCaseReport

[4] SMCG_Sec0060_DC_UseCaseTechnicalRequirements

[5] Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems - Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, December 2012

9 ANNEX A: REPOSITORY OF SECURITY REQUIREMENTS

This is a separate document (spread sheet): reference SM-CG Sec073_DC.

10 ANNEX B: DETAILED DESCRIPTION OF SECURITY CERTIFICATION SCHEMES

This annex describes in more detail how the security certification schemes in scope cover the elements enforcing trust as summarized in Table 1 and Table 2 in section 6.1.4.

Table 1 - Enforcing trust in products

Implementing security requirements that cover a threat analysis

CC, CPA and CSPN cover this aspect of trust enforcement by requiring that the evaluator/certification body verifies the consistency of security requirements against a security problem definition. This means all schemes in scope demand that requirements are defined as countermeasures to specific threats.

ISO/IEC 19790 & 24759: Different security levels are defined, but it is unclear in which case / for which threats one should go for a specific security level. CC schemes are based on threats and assets; FIPS schemes are based on functionalities and security mechanisms

Product testing

Product testing in the sense of security certification encompasses security functional testing (e.g. Test of user guidance - protection against misuse by purchaser) and vulnerability testing (e.g. penetration testing).

The four certification schemes fully cover security functional testing by requiring functional testing to be conducted and/or reviewed by the evaluator. There are some differences in how this is implemented in each certification scheme:

- CC requires full functional testing by developer and sample testing by an evaluator while, depending on the evaluation level, the evaluator should also perform a full documentary review of the functional tests;
- CSPN requires full functional testing by an evaluator
- CPA requires full functional testing to be *witnessed or performed* by an evaluator

- ISO/IEC 19790 & 24759: much functional testing is performed (see ISO/IEC 24759)

CC, CPA and CSPN cover vulnerability testing by requiring evaluators to perform security testing based on available documentation. In CSPN the implementation (source code) is used for vulnerability and cryptographic assessment, when available. In CC and CPA it is only required to use the implementation for such test at higher assurance levels. Additionally, CC also requires the evaluator to review a security architecture documentation, which describes self-protection measures of the TOE and non-bypass ability of the security function. Furthermore at higher EAL's, CC requires that focused penetration testing is performed by the evaluator to assess the resistance to high profile attacks.

ISO/IEC 19790 & 24759: Vulnerability testing is not covered by these standards: ISO/IEC 24759 describes conformance test for a cryptographic module against the functional and design requirements detailed in ISO/IEC 19790. The design requirements do contain Physical Security requirements (tamper evidence, detection, response), and higher security levels include mitigation requirements against attacks, but there is no penetration testing involved in the evaluation process.

Security measures for the premises of developers & OAM actors

Examples of such security measures are: organization of information security, human resources security, access control and asset management, etc.
ISO/IEC 19790 & 24759: No measures are required for developers to secure their premises.

CC and CPA formally require that security measures are taken to protect the product in "confidentiality and integrity" during development. However, no method is provided to achieve those measures (developers for example rely on ISO 27001). CSPN includes this verification in the “developer interview” evaluation task, which is optional..

All four certification schemes require that user guidance is provided for evaluated products in order to secure the product during operation – administration and maintenance.

Use of proven methods and maintaining skills

This aspect of trust in developers – OAM actors breaks down into several elements which are highlighted in **bold**.

CPA has strong requirements on **configuration management** (particularly focusing on automated configuration management and authorization) and **management of third party tools & components**, for example requiring that they are subject to the same configuration management requirements. CC also covers these elements; depending on the Evaluation Assurance Level, the requirements may be less strict that in CPA. CSPN includes this verification in the “developer interview” evaluation task, which is optional.
ISO/IEC 19790 & 24759 design assurance is required as from security level 1. There are no requirements on third party tools.

CPA requires that **development teams are trained**, especially regarding flaw remediation process and secure coding and this must be assessed by the evaluator. CC suggests this verification as an example (in CEM) but does not require this verification formally. CSPN includes this verification in the “developer interview” evaluation task, which is optional. ISO/IEC 19790 & 24759 do not have such requirements.

CC, CPA and CSPN require that **user guidance** is provided to OAM-actors.
ISO/IEC 19790 & 24759 requires an administration manual and a user manual

Finally, Common Criteria require that developers and OAM-actors use proven methods covering additional aspects of quality assurance like:

- 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. This requirement is also covered by ISO/IEC 19790 which requires, depending on the security level, annotation to the source code and documentation, documentation of a final state model, etc. More generally, as in CC, assurance must be provided that the module is properly designed and developed.
- A **flaw remediation procedure**, tracking (amongst others) product flaws, their effects, corrective measures, etc… This requirement is covered by Common Criteria and CPA.

Committing to flaw remediation obligations, delays and information provision to end-users

This aspect relates to information security incident management, including a patching policy. CPA heavily covers security flaw detection, correction and information and insists on verifying that flaw correction process is routinely followed in practice. CSPN has no formal requirement on this aspect of trust. ISO/IEC 19790 and 24759 do not have requirements regarding flaw remediation procedures.

Furthermore, CC and CPA require that timely action is taken for flaw remediation; CPA even defines service levels for customer information. CSPN at the other hand does not have formal requirements covering the above.

ISO/IEC 19790 & 24759 does not have such requirements.

Table 2 - Enforcing trust in the scheme itself

Recognition

The certification schemes in scope are all, to some extent, nationally or internationally recognized. This recognition is achieved by:

- The involvement of national authorities: The certification schemes in scope all have national governments involved in the creation, maintenance and endorsement of the scheme. In case of CC, national representatives signed the CC recognition agreement, while in case of CPA and CSPN the certification body itself is a national representative. ISO/IEC 19790 & 24759: the scheme will be delegated to national bodies. The profiling of the ISO/IEC

19790 standard will be tuned nationally. Today, there are ISO/IEC 19790 certification bodies in Spain, Turkey, and Japan.

- Being recognized as a standard: While CC is an international (ISO) standard, CPA and CSPN are both nationally recognized as a certification methodology. The ISO/IEC 19790 is an international standard. But there will be national certification bodies applying it.

Managing Certification Body accreditation

All certification schemes in scope manage which organizations can be Certification Bodies (CB).

CC has put criteria in place for accreditation and revocation of individual Certification Bodies and for periodic assessment of individual Certification Bodies.

In case of CPA and CSPN this is less relevant since there is only one Certification Body which has ownership of the certification scheme. Nevertheless this aspect is considered to be fully covered by these schemes since it is clear to the market who is the CB.

ISO/IEC 19790 does not foresee accreditation of CBs. But there exist international accreditation bodies like ILAC that do it.

Information provision to stakeholders

All certification schemes in scope cover this aspect by publishing the certificates obtained under the scheme on their website. The certificates can be accessed on-demand but only for products that have been evaluated with a request for international recognition.

Furthermore, the CC publishes information on accredited Certification Bodies; as mentioned in the previous section, this criterion is not relevant to CPA and CSPN.

ISO/IEC 19790 does not describe the publication of certificates. It will depend on each national CB.

Technological relevance of the methodology

The methodology to come to security requirements and an evaluation process should be technologically relevant. This breaks down into several elements:

- The conceptual model may make use of CIA notions, is compatible with known risk analysis methods and known vulnerability quotation methods. This is the case for CC and CSPN which allow CIA to be used in the security problem definition, allow for risk formalization to be compatible with known methods and have a vulnerability potential table. In CPA security characteristics, there is no systematic security problem definition or vulnerability quotation. ISO/IEC 19790: CIA - Encryption of sensitive assets for I/O; SW & FW integrity; Availability is not covered. AAA: User authentication required from level 2; optional code authentication; Authorization is supported by Roles; Accounting is supported by security audit.
- The scheme may facilitate coordination with technical communities to ensure technical relevance. CC and CPA involve technical communities by defining and using a process to request comments from the technical community on specific documents. CSPN does not actively involve the technical community, but is limited to domains (firewalls, data deletion, etc.) that are relevant by nature. ISO/IEC 19790 & 24759 does not have such requirements.
- The scheme may cover generic security functionalities. Examples of such functionalities are: Security audit, logs, events & alarms; Role based access and account management; Disabled functions / interfaces; etc. CC and CSPN cover most of the elements as Security Functional Requirements (SFR's). However, some functionality like function disablement and authentication are not explicitly covered and require de creation of ad hoc SFR's. CPA at the other hand is focused on specific technologies and as such covers all security functionalities that are relevant for said technology. ISO/IEC 19790 & 24759: Crypto key management and role based authentication are covered; security audit is required from Level 2.
- The scheme may cover patch management and firmware updates. CC, CPA and CSPN partially cover this by requiring maintenance evaluation for minor updates or full re-evaluation for major updates (although this is costly in case of regular updates). In CC, some national certification bodies performed R&D methods to certify patch mechanisms as security functions, in order to facilitate the certificate maintenance. ISO/IEC 19790 & 24759 do not contemplate the rules for re-certification in case of a change in the tested module. That would be part of the rules concerning the certification body. One can anticipate a retesting or regression testing proportional to the impact of the change in the compliance of 19790.
- The scheme may support multiple security levels. CC supports several Evaluation Assurance Levels which correspond to different security levels. This means that advanced attacks are evaluated only if a high EAL is chosen which implies performing more thorough assurance verification. CPA and CSPN do not differentiate between security levels. ISO/IEC 19790 & 24759 define 4 security levels.

Economics

Next to being technologically relevant, the scheme can also be relevant in the business context in which it is designed to operate. This breaks down in several aspects:

- The scheme may give the developer / user some means to manage to cost of certification or at least to give an up-front idea of what this cost can be.
    - CC covers this by linking certification duration and complexity to the Evaluation Assurance Level (EAL). Furthermore, supporting documents approved for a specific domain can include duration indicators for certification.
    - CSPN at the other hand commits to an evaluation duration of 8 weeks and a fixed number of working days. ANSSI can request certification requests if products are too complex to be evaluated under these conditions.
    - CPA fixes the evaluation lab fees (currently 4000 GBP) but does not formally provide a means to manage certification duration.
    - ISO/IEC 19790: not covered - there is no direct influence. It will depend on the CB and the lab.
- The scheme may give an indication of duration and cost of certificate management and has procedures that limit this cost of such maintenance
    - CC, CPA and CSPN are only applicable to a specific version of a product but do have an assurance continuity process. When a product is updated, an impact analysis has to be performed. When the impact of the update is considered minor, a simple maintenance report is published. When the impact is significant, re-certification is performed, but the evaluator makes maximum use of evidence collected in the previous certification.
    - ISO/IEC 19790 and 24759 do not contemplate the rules for re-certification in case of a change in the tested module. That would be part of the rules concerning the certification body. One can anticipate a retesting or regression testing proportional to the impact of the change in the compliance of 19790.

Scope

CC: applies to a broad product range, going from access control to operation systems and smart meter gateways. Common Criteria is industry / product independent.

CSPN: IT products can currently apply to CSPN if they belong to a specific list of domains. Only for products that can be tested in the pre-defined timing

CPA covers only specified types of products/features of products.

ISO/IEC 19790 and 24759: scope is broader than just a Security Module, but focusses on cryptographic functionalities.