SM-CG Sec0064_DC

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

Version: 1.02
Date: November 2013
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
Tim Sablon	ESMIG	Editor
Eric Farnier	TC294, Eureau	Member
Pascal Sitbon	TC294, Eureau	Member
Sylvain Orthlieb	TC 294, WG4	Member
Uwe Pahl	TC294, WG4	Member
Roman Picard	CRE/CEER	Member
David Johnson	SM-CG, SG-CG	Member
Joost Demarest	TC205 WG16	Member
Olivier Rochon	TC13	Member
Michael John	SG-TF, Expert Group 2	Member
Marylin Arndt	ETSI	Member
Michelle Struvay	ETSI	Member

VERSION CONTROL

Version	Date	Modifications
0.1	01/09/2012	1st version for information to the Task Force
0.2	20/09/2012	Including 1st comments by the AHWG
0.3	12/10/2012	Including contributions from TC's and recommendations
0.4	15/10/2012	Including results from the AHWG meeting
0.5	29/10/2012	Including ETSI contribution and aligning the sections
0.6	31/10/2012	Including suggestions by Eric Farnier and David Johnson
0.7	1/11/2012	Including new versions of ETSI and TC294 sections
0.9	5/11/2012	Results from the meeting on 5-11-2012. Final version for distribution in SM-CG
1.00	05/03/2013	Implemented changes based on consultation in 2012

1.02	17/07/2013	Updated chapter 3.2 on with feedback from TC205 related to the security requirements for the H1 interface, following an ANEC comment

CONTENTS

1 INTRODUCTION

1.1 Background and objectives

The Smart Meters Coordination Group published a Technical Report (TR): “Functional reference architecture for communications in Smart Metering Systems” (CEN/CLC/ETSI/FprTR 50572) that comprises a reference architecture, an overview of communication standards and the work programs of the European Standards Organizations (ESO's) regarding these standards.

Although the standards needed for interoperability of components of the Advanced Metering Infrastructure are dealt with in the current TR, another important issue still needs additional attention: Privacy of consumer owned data and the Security of transactions and data access within the AMI. Various stakeholders involved in or influenced by the implementation of Smart Meters still have serious concerns about the Privacy and Security of their assets.

In the SMCG plenary meeting on 27 June 2012 it was decided that a new chapter about the approach of the ESO's regarding Privacy and Security should be included in the SMCG deliverables. A Task Force was formed to define such an approach and give insight in the work planned by the Technical Committees to tackle the Privacy and Security requirements.

1.2 Scope

The scope of the work of the Task Force "Privacy & Security" can be derived from the functional reference architecture as defined in TR 50572 shown below. The approach of the Privacy and Security in standardisation and the current work of the TC's will focus on the interfaces as show in this figure.

However, even where the particular architecture being implemented by a member state respects 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, water or electricity), 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.

The scope of this work is privacy and security within the boundaries of the architecture mentioned above.

The EG2 DPIA [6] defines that privacy is a term that has received many interpretations over time, and often means different things in different contexts. A variety of definitions can be found and each culture and even each person has a different expectation on what constitutes as an invasion of privacy. In the context of this document, privacy is defined as data privacy and includes elements of protecting private life such as integrity of a person's home, body, conversations, honor and reputation following the Article 7 of the Charter of fundamental rights of the European Union.

Furthermore, this document [6] states that cyber security aims at safeguarding of the confidentiality, integrity and availability of information assets that support vital physical assets (such as the electricity grid) against attacks, malware etc., which will disrupt the delivery of electricity.

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.

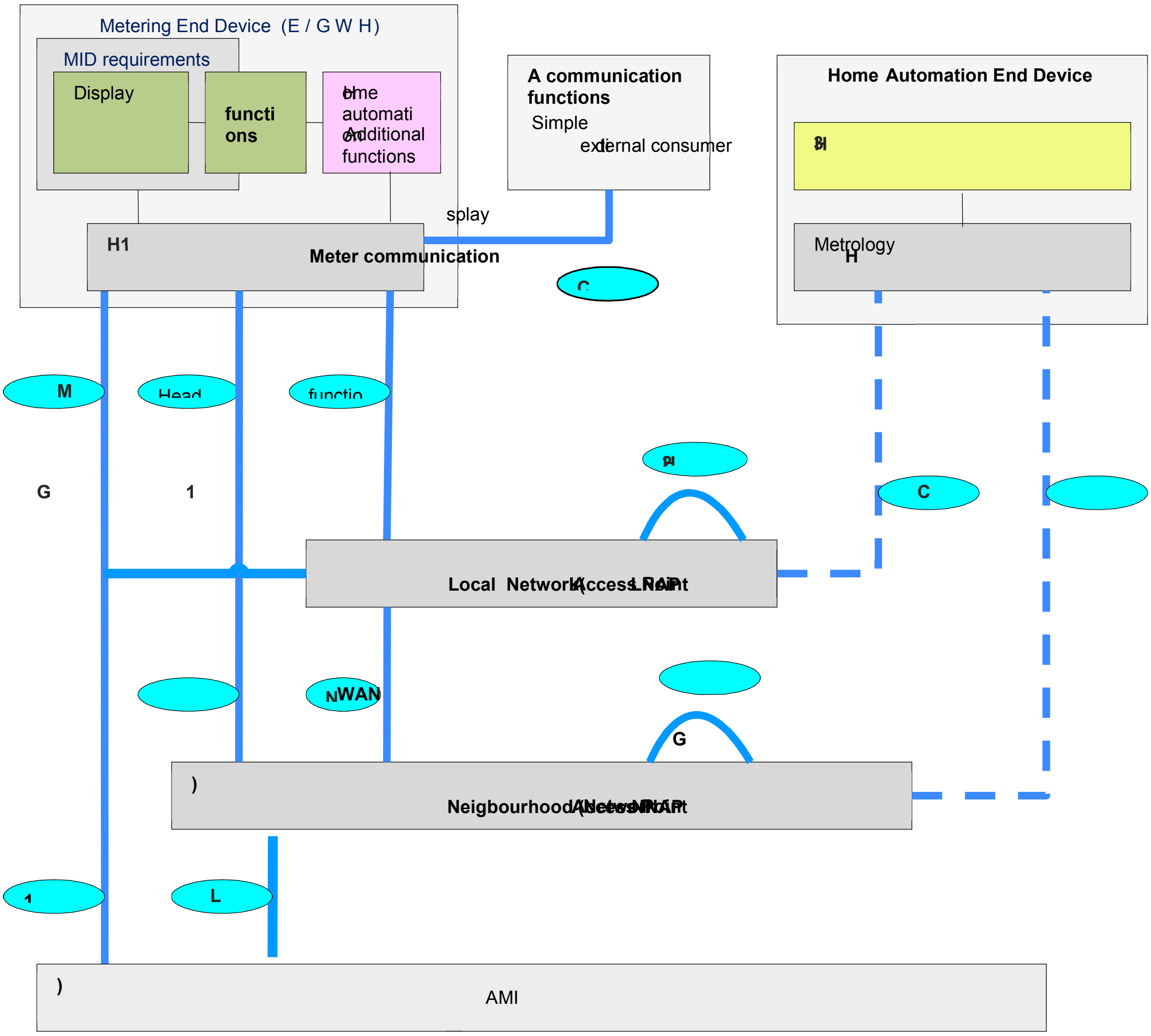


Figure 1 – The SM-CG functional reference model

2 THE APPROACH TO DEFINE REQUIREMENTS FOR STANDARDS

2.1 Introduction

The Smart Grid Coordination Group (SG-CG), acting on the M490 mandate, has provided in 2012 a methodology to maintain standards and keep them updated to the latest developments in functionality and technology. In this methodology the basis for evaluation of existing standards is formed by the definition of basic functions which are represented as generic use cases. By using generic use cases as the basis of further standardization it can be assured that the resulting standards framework meets the desired quality level.
Basically, the SG-CG is applying the principles of system engineering to standardization, in this case in the area of Smart Grids. Furthermore it can be applied in other areas of complex systems, e.g. Smart Metering is using the same approach in its work for the Mandate M/441. The Task Force "Use Cases" of the SM-CG has been working on the definition of Use Cases since 2011 and its deliverables are reviewed by the SM-CG members mid 2012. These Use Cases are also the basis for the definition of Technical Requirements, which standards have to comply to. These Technical requirements include Security and Privacy requirements.

In general the following steps are needed for the use case approach in standardization:

1. <u>Collecting and analysing requirements</u>
    a. <u>Providing use cases</u>

    Different sources might suggest use cases to standardization. As these use cases should be considered as market needs, they might come from internal sources of the standardization organisation (e.g. Technical Committees) or from external stakeholders like R&D projects, regulation, legislation, or cooperation partners like associations. Ideally the requirements are directly formulated in the given use case template, see also the "Guidelines for developing Smart Metering Use Cases" (***SMCG_Sec0044_DC***).

    b. <u>Discussing and harmonizing (different) use cases in order to generate or adapt broadly accepted Generic Use Cases.</u>

During the evaluation further information is provided in the Use Case template. According to the suggested transparent and open process different stakeholders (e.g. different TC's) might participate in the evaluation process and provide information in one common use case template. The external source can follow up the detailing and can comment on it. In case variations of use cases with same functions were provided, they have to be reviewed and combined to generic use cases.
Every Generic Use Cases will be accompanied by a system architecture, showing the system components that are internal system actors in the Use Cases. For Smart Metering this is the SM-CG reference model (see figure 1 in 1.2)

c. **Deliverable :** Generic Use Cases (GUC), which are used for further analysis in relation to standardization

For Smart Metering the Use Cases are described in SMCG_Sec0051_DC. The Use Case repositories are: SMCG_Sec0052 (primary UC's) and SMCG_Sec0053 (secondary UC's) and Technical Requirements are listed in SMCG_Sec0054.

2. Analysis: The GUC and its systems architecture are mapped to

   a. the reference architecture (here: Smart Grid Architecture Model developed by the SG-CG, SGAM, see figure 2)

      The different layers of the architecture are providing lists of standards applicable for the relevant use case. Once the Use Cases and standards are linked, the Functional and Technical Requirements that apply to these standards are identified.

      .

   b. and via a Risk Analysis to required privacy and security levels

      Based on the analysis of the use cases, the security and privacy risks can be evaluated separately and the applicable security level can be identified (see next section).

As recursive process this step might lead again to an update of the GUC (requirements, additional information like actors).

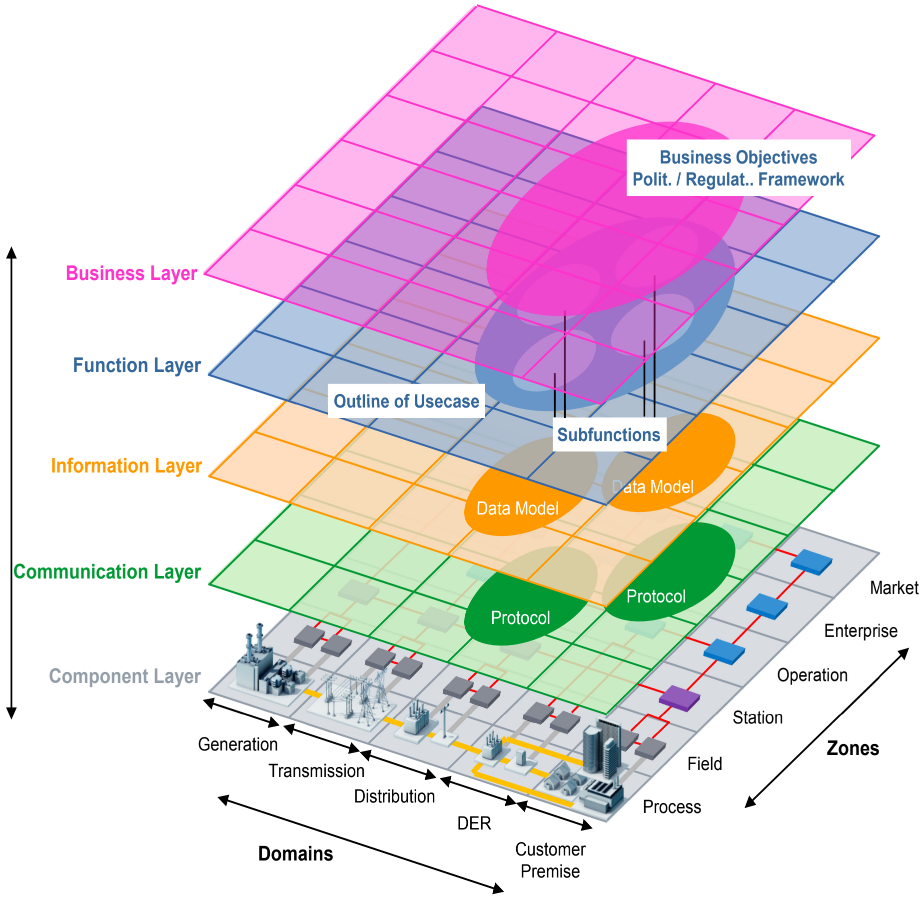


Figure 2 – The Smart Grid Architectural Model (SGAM)

3. Link privacy and security requirements

   See section 2.2

4. Gap Analysis

   By comparing the functionality and Technical Requirements given by the Use Case with the characteristics of the standards, the completeness and compliance of these standards can be checked.

   If a gap is identified, the missing standards (or features of the standard) leads to a further item in the work programme for standardization.

The process described above is represented in Figure 3 below. It shows that the use cases are a basis for identification, evaluation and maintenance of Smart Grid standards.

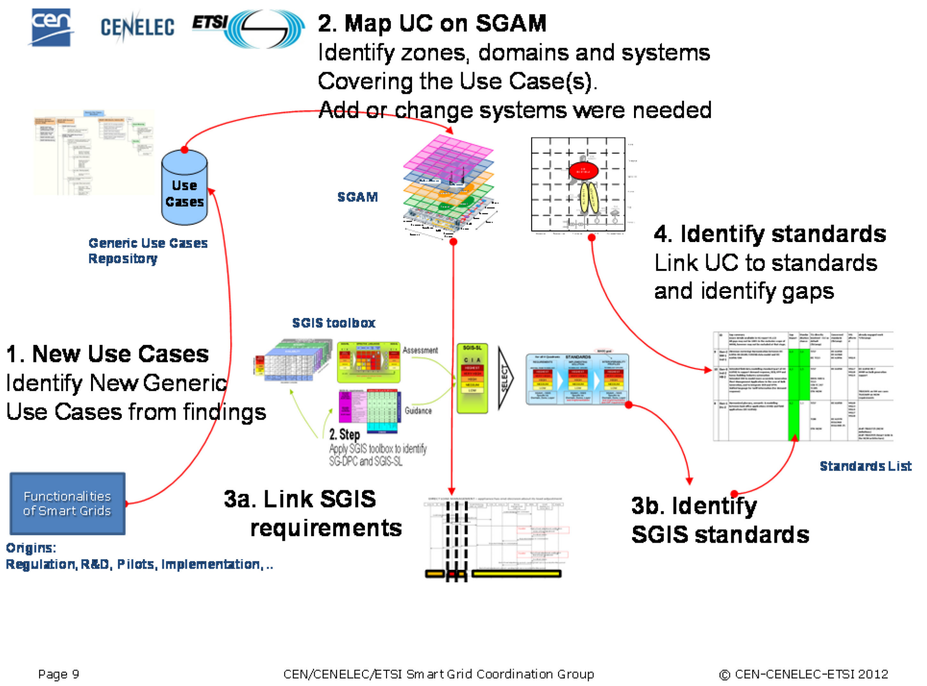


Figure 3 - The maintenance of Smart Grid Standards

2.2 Definition of Privacy and Security Requirements

2.2.1 The SGIS toolbox

The Use Cases comprise functional and technical requirements for Smart Grid standards. According to step 2 “Analysis” in the former paragraph, Use Cases are mapped on the Smart Grid Architectural Model (comprising definitions of Domains, Zones and Systems). This activity starts with mapping the system architecture on the zones in this model. In doing so, the detailed activities shown in the step-by-step description of the Use Cases describing the interaction of system components among each other, can be mapped on the zones.

u Figure 4 shows the mapping of the SM-CG architecture; see ref [1] for an explanation.

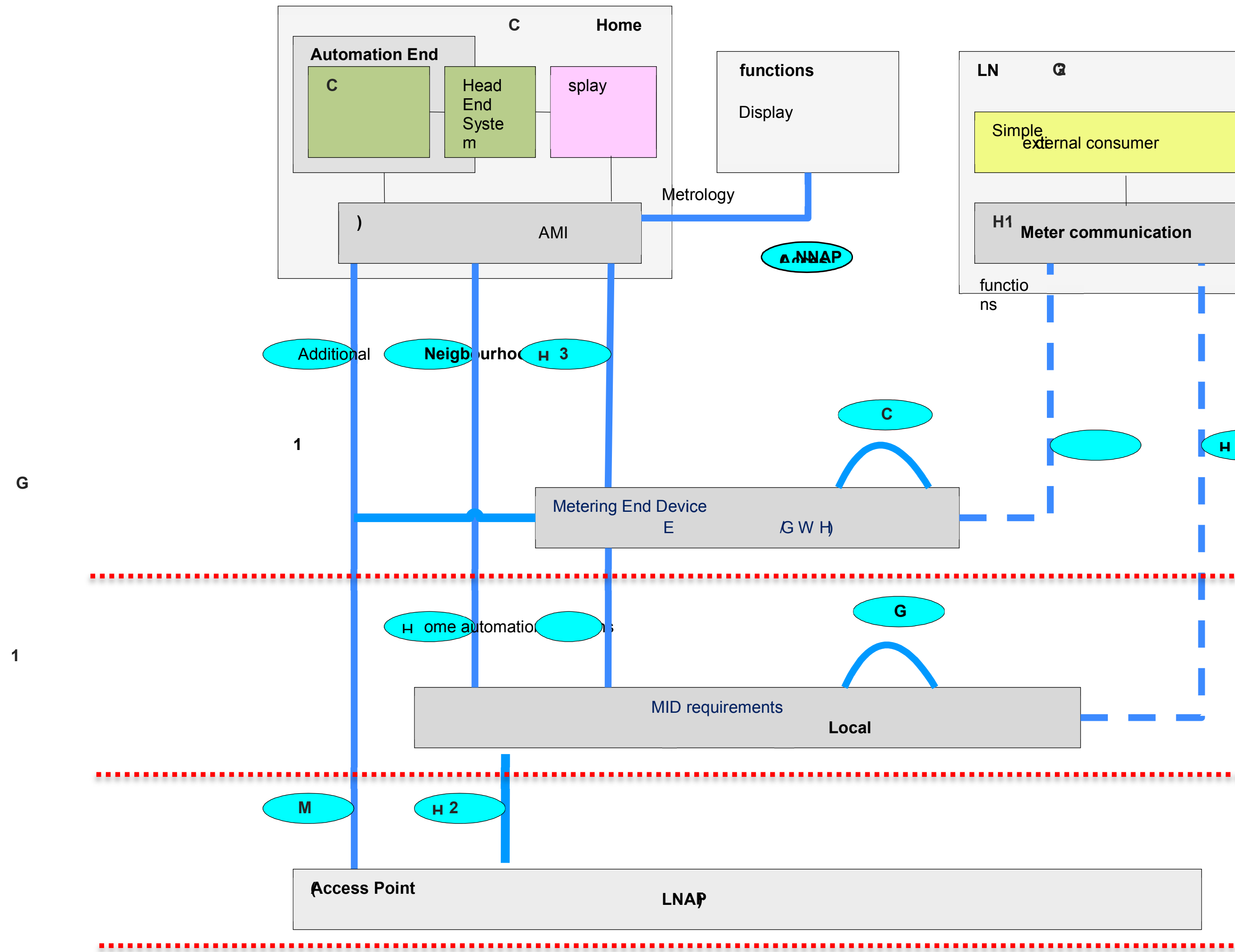


Figure 4 - Mapping SM-CG reference architecture on SGAM zones

As a next step, the use cases are mapped on the SGAM in order to be able to perform a risk analysis on the use case, because the risks are depending on the concerning domains and zones.

For every use cases, mapping on domains/zones and a risk analysis can be performed based on the toolbox developed by the Smart Grid Information Security (SGIS) group [ref 5] of the SG-CG. Depending on the domain/zone and the type of data a Risk Impact Level can be attached to every step/transaction in the Use Case.

Figure 5 shows a table that is used to define the risk impact level.

RISK IMPACT LEVELS	OPERATIONAL (availability)				LEGAL		HUMAN	REPUTATION	FINANCIAL
	Energy supply (Watt)	Energy flow (Watt/hour)	Population	Infrastructures	Data protection	other laws & regulations			
HIGHLY CRITICAL	regional grids from 10GW	from 10 GWh	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 in several countries	permanent loss of trust affecting all corporation	Thirth party affected
CRITICAL	national grids from 1 GW to 10GW	from 1 GWh to 10GWh	from 25% to 50% population size affected	national critical infrastructures affected	not defined	temporary disruption of activities	direct and collateral deaths in a country	permanent loss of trust in a country	>=50% EBITDA
HIGH	city grids from 100MW to 1GW	from 100MWh to 1GWh	from 10% to 25% population size affected	essential infrastructures affected	unauthorized disclosure or modification of sensitive data	prison	direct deaths in a country	temporary loss of trust in a country	<50% EBITDA
MEDIUM	neighborhood grids from 10MW to 100MW	from 10MWh to 100MWh	from 2% to 10% population size affected	complimentary infrastructures affected	unauthorized disclosure or modification of personal data	fines	seriously injured or discapacity	temporary and local loss or trust	<33% EBITDA
LOW	home or building networks under 10 MW	under 10MWh	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

MEASUREMENT CATEGORIES

Figure 5 - Definition of the Risk Impact Level

The SGIS toolbox [ref 5] describes how the risk impact level combined with a probability analysis will result in a security level from 1-5.
Finally, these levels are mapped on a large list of security requirements that are currently derived from NIST (NISTIR-7628), so this procedure results in the identification of Privacy and Security requirements per use case and even per step/transaction in a Use Case.
The SGIS approach leads to an accurate definition of appropriate P&S requirements that match the implemented architecture and functionalities.
Please note that the approach described above does not have the intention to select the final security requirements on European level, but just gives the guidelines how to come to these requirements and what would be the technical consequences of implementing specific Use Cases.

2.2.2 Requirements for standards and final implementations

The method in the former section shows how Use Cases can be used to identify the appropriate Privacy and Security 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. The member states can use the method as described and Generic Use Cases to come to the final Use Cases and requirements, so a jump start is possible. The Generic Use Cases and requirements will be maintained by one or more horizontal Technical Committees, so newest technical and functional developments will be taken in account.

Although they are of generic nature, the Privacy and Security (P&S) requirements identified by the SM-CG (see output from the task Force Use Cases) and SG-CG (NISTR 7628) are input for the ESO's 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. It is also recommended that currently available national P&S requirements and the above mentioned available requirements are used as input to define a European reference list of P&S requirements. This new list would tune the SGIS toolbox to Smart Metering specifics and improve its applicability for Smart Metering. 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 M441 mandate and the technical and economical 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. Furthermore it is important to note that a list of generic P&S requirements can only serve as a guideline for reference purposes by TC's and member states.

Various initiatives have been taken by European organisations to formulate recommendations regarding the Privacy and Security requirements that apply to Smart Grid and Smart Metering applications.

The report written by Expert Group 2 (EG2) of the Task Force Smart Grids [ref 4] in 2011 states that:

- ESO's should be tasked with updating, extending or developing new standards covering the security aspects of Smart Grid interfaces based on **European requirements**
- ESO's joint working group should review the Expert Group recommendations and list of relevant standards and add the latest amendments, additions and future work required before starting any new standardisation work, based on the **still to be defined requirements**

The EG2 report further recommends that:

ESO's are tasked with evaluating the current state of cryptographic primitives through their relevant technical committees and make available the most appropriate technologies within the relevant standards framework. This should ensure

- Not to preclude the initial adoption of symmetric key cryptography followed by smooth migration to asymmetric cryptography if required;
- A business model is investigated to make the creation and maintenance of certification authorities (needed for asymmetric cryptography) possible;
- A study is conducted on how to handle multi-national key management (e.g. one supra-national European certification authority certifying national certification authorities) and who should be in charge of performing this key management activity.

The Article 29 Data Protection Party (WP 183 opinion 12/2011 on Smart Metering adopted on 4 April 2011) [ref. 3] concludes that:
Technical and organizational safeguards should cover at least the following areas:

- The prevention of unauthorized disclosures of personal data;
- The maintenance of data integrity to ensure against unauthorized modification;
- The effective authentication of the identity of any recipient of personal data;
- The avoidance of important services being disrupted due to attacks on the security of personal data;
- The facility to conduct proper audits of personal data stored on or transmitted from a meter;
- Appropriate access controls and retention periods;
- The aggregation of data whenever individual level data is not required.

According to the Commission Recommendation [ref. 2] of 9 March 2012 on preparations for the roll-out of smart metering systems, the following conditions apply (and therefore should be included as legal conditions in the Smart Metering Use Cases):

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy

The AHWG recommends analysing the approach for data privacy in line with the EG2 recommendations and DPIA approach defined by EG2. The AHWG will take this action into the work program of 2013.

Regarding data security the Commission Recommendation states that:

- The use of encrypted channels is recommended as it is one of the most effective technical means against misuse.
- Member States should take into account that all present and future components of smart grids ensure compliance with all the ‘security-relevant’ standards developed by European standardization organizations, including the Smart Grid Information Security essential requirements in the Commission's standardization mandate M/490.
- The international security standards should also be taken into account, in particular the ISO/IEC 27000 series (‘ISMS family of standards’).

Based on the input listed above, it is recommended that after defining a European reference list of P&S requirements for Smart Metering, a study is performed to explore a possible certification approach for both products and organizations involved in Smart Metering.

3 STATUS OF THE WORK BY TECHNICAL COMMITTEES

3.1 TC13

3.1.1 Overview of TC13 WG02 P&S task force

The CLC TC13 WG02 (Data models and protocols for additional functionality of and data exchange in interoperable multi-utility smart metering systems) has created a task force for addressing Data Security & Privacy requirements applicable to data exchanges

The task force objectives are to:

- Review the use cases applicable to the SM-CG Reference architecture with a security perspective and in liaison with the WG02 Use Case Task Force
- Identify additional security use cases related to key and certificate provisioning, key and certificate management, security level increase and end to end data and message protection
- provide security requirements at the data model level and the application layer level, independently from any transport or lower protocol layer
- provide a framework for assessing security gaps in existing communication protocol standards

P&S task force members are security experts from the metering, smart card, silicon and utility industries.

3.1.2 Security Use Cases

The main security uses cases are listed below:

- Provide meter with symmetric keys
- Provide meter with asymmetric key pairs
- Provide meter with a trust anchor (PKI)
- Provide meter with public key / certificate of manufacturer and / or client(s)/ third party
- Provide client / third party with meters' public key /certificate
- Perform key establishment
  - a) for transporting a new symmetric key between trusted entities
  - b) for agreeing a new shared symmetric key between trusted entities
- Set the security policy according to security level
- Transfer crypto-protected data / messages to/from the smart meter

3.1.3 Security requirements

Security requirements for device access control and message protection are based on the NISTIR 7628 Smart Grid Guidelines for Smart Grid Cyber Security [Aug 2010].

The Task force TC13 WG02 P&S has issued a document delivering a set of security requirements for message protection and access control which is available on the CENELEC collaborative site.

This set can be used as input for the creation of a European reference set.

3.1.4 Crypto-algorithms

TC13 WG02 P&S Task force is elaborating a new set of modern crypto suites based on Elliptic Curve Cryptography. The aim is to enhance security properties of existing standard protocols with extended security mechanism addressing new needs such as digital signature (for proof of origin and non-repudiation), support of X509 certificates and new key agreement methods for easing the large scale distribution of keys (Diffie Hellman key agreement scheme)

These new crypto-suites have been selected from the NSA (National Security Agency, USA) Suite B. The suite B defines a common suite of public standards, protocols, algorithms and modes allowing interoperability of cryptographic solutions and secure information sharing between partners.

The DLMS COSEM protocol standard (IEC62056 series) is currently being revised to support these new security suites, in addition to the existing AES 128 GCM cipher-suite. A new version of the DLMS COSEM standard will be available by end of 2012.

TC13 WG02 has picked up the following key elements from the NSA Suite B:

- ECDSA (Elliptic Curve Crypto based Digital Signature) scheme for providing strong authentication of metering data and commands/controls . (FIPS PUB 186-3)
- ECDH (Elliptic Curve Crypto based Diffie Hellman) key agreement for establishing a common shared symmetric key between trusted partners. (NIST SP 800-56A)
- NIST standard named Elliptic curves P-256 and P-384, providing a common set of domain parameters over a prime field, for the purpose of interoperability of the crypto-operations
- Suite B Implementers' Guide to FIPS 186-3 (ECDSA)
- Suite B Implementers' Guide to NIST SP 800-56A (ECDH)

Liaisons are established between the TC13, TC57 and SGIS Privacy and Security working groups for leveraging on these new crypto standards and allowing the reuse of crypto algorithm across the Smart Metering and Smart Grid architecture

3.1.5 Data protection and message protection

The level of protection of messages (communication layer) during transport or the level of data protection (information layer) can be determined using different security suites and policies which are selectable in relation with the security level and the security use cases of the project.
This supports a clear separation between the information layer and the communication layer (in line with the SG-CG reference architecture for the Smart Grid) and addresses properly the need for end to end data security between market entities.

3.2 TC205

In the domain of M 441 (Smart Metering) a simple display (a display with reduced functions) is connected via the interface H1 directly to the data collector. Since the display is considered to be an information sink (only receiving information), the necessary security measures should be implemented in the smart meter This would imply for example protection of the data transferred to the display, from external access as specified in the Smart Metering Technical Requirements (SMCG_Sec0060_DC_UseCaseTechnicalRequirements, TR-PRIV-02 and TR-SEC-05).

In the M490 domain (Smart Grid) a display with higher functionality can be connected via the H2/H3 interface. Such a display can be regarded as a (“normal”) HBES device and no additional security provisions are required, as all functions and security provisions of the display are handled within the HBES and the Gateway to HBES respectively. In case of open HBES media, further HBES specific security mechanisms may however have to be put in place and specified.
At field level, in HBES, security is positively influenced by inherent system conditions:

- HBES is a closed system. Physical access is required to impair security.
- In order to impair security, knowledge on the structure and the data of the specific HBES solution is required. Even after recording the data transfer in the specific HBES system, this information provides insufficient knowledge on the HBES installation, to create serious security risks.

The many buildings equipped with HBES over the last decades corroborate the above.

In case an HBES system is connected via a gateway to non-HBES systems, the HBES security level is ensured through specific security provisions in the gateway.
In addition, the security regarding the Smart Grid part in the building is ensured by security provisions in the connection to the WAN, the “Local Network Access Point” (LNAP).

Conclusion:
As security is ensured by the Smart Meter (for H1interface) 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..

3.3 TC294

On the last plenary meeting in November 2011 several resolutions were taken that show the importance of the P&S aspects for the TC.

- One is the enhancement of general scope of CEN/TC 294 with the paragraph: “Secure communication covering data privacy as an inherent property, providing a scalable mechanism for security services, data integrity, authentication and confidentiality.”
- The other is the decision for a preliminary new work item to create an Amendment to prEN 13757-3 "Communication systems for and remote reading of meters - Part 3: Dedicated application layer" to include applications requiring data security, data integrity, authentication and confidentiality.
  This decision was based on the special aspects that different national legislative requirements regarding communication security will be standardized in this Amendment to ensure interoperability of Smart Meters by adding new cryptographic modes and insert methods as well as data elements to provide an integrity check to cover legislative requirements.

After this resolutions the working group 4 (WG4) of CEN/TC 294 starts actions for this amendment. The current modes and methods in prEN 13757-3 are limited to more or less one symmetrical encryption mode (AES128) but no authentication. All members of WG4 agreed that a definition of additional techniques is necessary to fulfil the requirements for privacy and security.

Starting the work in WG4 several countries (Italy, France, Germany) presented their national approach for this aspect. After that it was directly clear that the national requirements are different and WG4 could not get to a consensus which techniques to be implemented in the standard and which not. Therefore WG4 asked CEN/TC 294 for further instruction how to handle this point.

To prepare a general decision for the next CEN/TC 294 plenary meeting in November 2012 a ballot was launched to get a European wide view, which direction for the member states is appropriate to solve requirements of security and privacy in terms of scalability. The result is just available and shows again the diversity of this aspect. **It will be discussed** in the plenary meeting in November and decisions for actions may be taken according this preliminary work item (“Amendment”). ***The TC294 intends to*** *use the guidance developed by the SMCG and SGCG regarding the approach of privacy and security* ***where appropriate****.*

3.4 ETSI

In 2009 ETSI Telecommunications and Internet converged Services and. Protocols for Advanced Networking (TISPAN) developed a methodology for analysing security of mobile and fixed communications which was published as TVRA (threat, vulnerability and risk assessment).

http://docbox.etsi.org//Workshop/2009/200903_TVRA/TVRA_006_TVRA_web_user_guide.pdf

More recently the ETSI M2M group has undertaken some work on the risks and vulnerabilities of M2M architecture and services. It was found necessary to augment the basic framework of the analysis for a number of reasons.

Some of these relate to the distinctive characteristics of M2M working. For instance the use cases considered were those from the SM-CG regarding smart meters, where there is a mixture of automated functions, such as periodic meter reading by the responsible party, and consumer-initiated ones such as monitoring own consumption.

These features meant the need to take into account two further factors in the security analysis.

- The first of these was detectability; the need for the machine to become aware of and react to a security breach such as meter-tampering. This is especially important where the infrastructure is the sort of ‘street furniture’ that goes unremarked by passers-by.

- The second is recoverability: since the equipment may be dispersed or inaccessible, it must be possible to undertake at least some remediation and reset functions remotely.

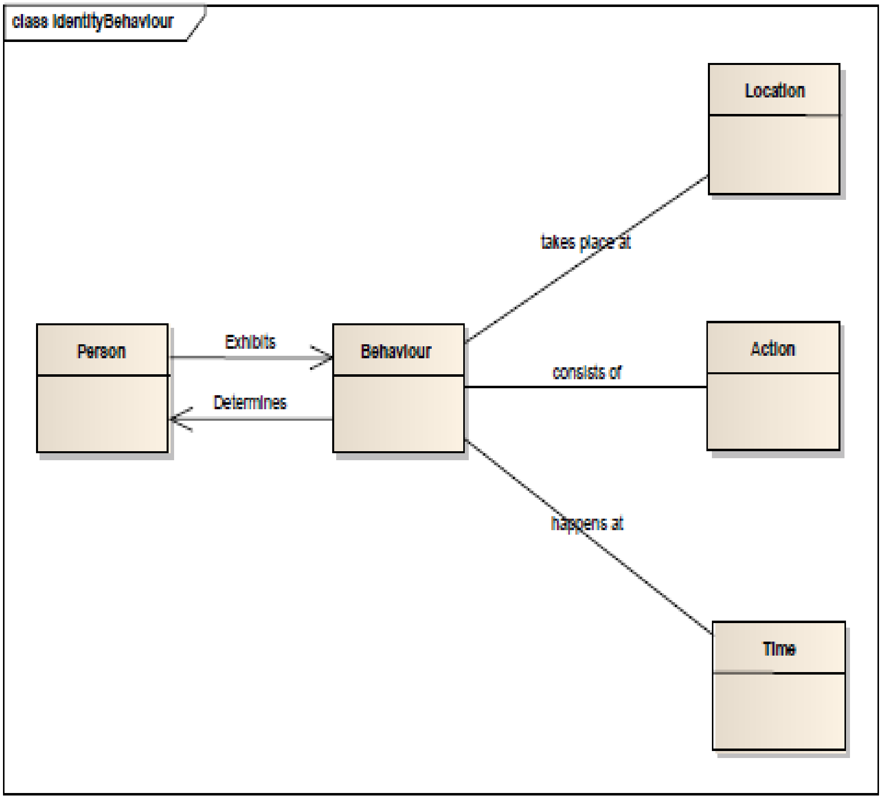
As risk is a function of probability and impact, these two new factors influence all aspects of traditional assessment: for instance, the probability of a successful attack on a remote or unmonitored device could be either higher or lower, but the impact is likely to be higher.

An example of such an analysis performed by ETSI can be found in:-

http://www.etsi.org/deliver/etsi_tr/103100_103199/103167/01.01.01_60/tr_103167v010101p.pdf

Security has traditionally been analysed in terms of Confidentiality, Integrity and Availability. More recently the EU has asked that the additional aspects of Privacy and Service Resilience are also considered.

- **Privacy:** This could be typified as the mere existence of a message rather than its actual content. It is necessary. Therefore, to limit possibilities for the collection of data from which inferences could be drawn about lifestyle leading to unsolicited marketing. The following working definition of Privacy was agreed *“Definition of Privacy: The right of the individual to have his identity, agency and action protected from any unwanted scrutiny and interference”*



- This leads us to define two new concepts of ‘unobservability’ and ‘unlinkability.’
    - **unlinkability:** act of ensuring that a user may make multiple uses of resources or services without others being able to link these uses together
    - **unobservability:** act of ensuring that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used

- **Service Resilience:** This has to do with the availability of alternative channels for communication. Unlike for example, a mobile phone, which is typically locked to a particular service provider, the smart electricity meter, should be able to communicate on any available network. For example, at any given point in a street or even house, one particular supplier’s radio signal will be the strongest – and this may well change during the 15-year installed life of the meter. This has a large impact on the way security credentials are provisioned and re-provisioned or exchanged. As a result of joint work with ENISA ETSI has agreed that Service Resilience will be an additional factor its analysis and specification of security features:- see http://www.enisa.europa.eu/activities/Resilience-and-CIIP

The next stage in ETSI's work will be to analyse:

- Differences and commonalities between National security requirements for smart metering, to find a suitable path for a common approach
- Apply the augmented ETSI TVRA framework to identify potential threats and ensure that suitable countermeasures are addressed in applicable ETSI standards
- Use Cases for smart meter implementation from M/441 and M/490 to become aligned with the ETSI M2M Smart Metering Use Cases (TR 102 691)
- Apply SGIS toolbox to the resulting use cases to propose a consistent mapping between SGIS Security Levels and TC M2M security specifications.

A new work item in ETSI M2M (DTR/M2M-0021) has been agreed to create an amendment to ETSI TR103 167:

M2M(12)21_108_Machine-to-Machine_communications__M2M____Smart_Energy_Infras.zip

http://docbox.etsi.org/M2M/M2M/05-CONTRIBUTIONS/2012/M2M(12)22_100_Annex_1___Vertical_Application_Specific_Threats_-_Smart_Mete.zip

So far, one national smart meter security requirements document has been analysed and 54 potential vulnerabilities listed. Since the SM-CG already has progressed regarding these topics and the Task Force recommends following the SG-CG approach for defining P&S requirements, the augmented TVRA framework could be further exploited / adapted to be used for the use case based Risk Assessment process inherent to the use of the SGIS Toolbox: In this manner, specific threats and countermeasures applicable to a particular use case could be identified.

All further work on P&S requirements for Smart Metering is proposed to be performed in the context of the SM-CG (see recommendations in chapter 4).

4 FINAL CONCLUSIONS

Based on the work performed by the Smart Grid Coordination Group regarding the definition and selection of Privacy and Security requirements and the recommendations from various organisations, the Smart Meter Coordination Groups recommends:

- That the SG-CG toolbox for defining security requirements is adopted for defining and selecting requirements for Smart Metering when available;
- That the EG2 DPIA template will be considered for defining and selecting privacy requirements for smart metering when available;
- That a European reference set of P&S requirements is defined and integrated with the SG-CG toolbox and the EG2 DPIA;
- That the Technical Committees use the SG-CG toolbox, EG2 DPIA and reference set of requirements as input for their work on P&S related aspects in their standards;
- That a study is performed to explore a possible European level approach for certification of Smart Metering related products, within the scope of the M441 mandate, based on the reference set of P&S requirements.

When following the above recommendations it is important to note that the applicability of requirements is depending on the nature of architectures and products in the scope of the M441 mandate.

5 WORK PLAN FOR 2013

Based on the above conclusions, the following work plan for 2013 is proposed:

Action	Timing
Process comments on 2012 report by ANEC and ETSI	Done
Deliver new report and work plan to SMCG	Done
Develop collection of Smart Metering security requirements	March 2013
Describe and compare existing certification approaches for security (Common Criteria, CPA, CSPN …)	Q2 2013
Work with SGIS to integrate the Smart Metering P&S requirements	Q3 2013

Define recommendations / next steps regarding the use of Smart Metering security requirements and an approach for certification	Q3 2013
Expand the report with a chapter on Privacy: • Considering the EG2 DPIA template, for privacy impact assessment • Identifying privacy related recommendations and best practices • Including some information on cooperation on this topic with the SG-CG SGIS	Q3 2013
Follow the work of the SGIS updating the toolbox and evaluate which domain specific adaptations for smart metering are needed. Create a guideline/approach on how to use the SGIS risk impact table for smart metering	Q3 2013
Deliver final version 2 of the AHWG P&S report	Q4 2013
Include the latest work plans regarding privacy and security of the coordinating Technical Committees	Q4 2013

6 REFERENCES

[1] Functional reference architecture for communications in Smart Metering Systems - CEN/CLC/ETSI/FprTR 50572

[2] Commission recommendations on preparations for the roll-out of Smart Metering Systems, COM2012-148, March 2012.

[3] WP 183 opinion 12/2011 on Smart Metering

[4] EG2 report Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection, December 2011

[5] SG-CG SGIS draft Summary Report, August 2012

[6] 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