SM-CG Sec084_DC

# Smart Meters Co-ordination Group Privacy and Security approach – Part III

**Version: 1.0 final**

**Date: June 2015**

**Authors: Task Force Privacy and Security of the Smart Meters Coordination Group**

## Members of the Task Force in 2014

| Name | Representation | Role |
|---|---|---|
| Willem Strabbing | ESMIG, SM-CG, SG-CG | Convenor |
| Eric Farnier | TC294, Eureau | Member |
| Uwe Pahl | TC294 - WG4 | TC 294 liaison |
| Roman Picard | CRE/CEER | Member |
| David Johnson | SM-CG, SG-CG | Member |
| Peter Berends | Netbeheer NL | Member |
| Michele Struvay | ETSI-M2M | Member |
| Marc Vauclair | ETSI-M2M | Member |
| Olivier Rochon | TC13 | TC13 liaison |
| Marylin Arndt | ETSI-M2M | Member |
| Colin Blanchard | ETSI-M2M | Member |
| Sylvie Wuidart | STMicroelectronics | Member |
| Hans Baars | ESMIG | Editor |

## Version Control

| Version | Date | Modifications |
|---|---|---|
| 0.1 | 26/09/2014 | First draft version by Hans Baars and Willem Strabbing |
| 0.2 | 23/09/2014 | Certification approach for SMI added |
| 0.3 | 07/10/2014 | Certification approach for SMI deleted (too much in draft to be used in this document) |
| 0.4 | 23/10/2014 | Overview of ENISA/SOG-IS workshops<br>Explanation of threat landscape and security requirement spreadsheets<br>Status of the work by technical committees |
| 0.5 | 27/10/2014 | Improvement based on review comments (Dominique Beck) |
| 0.6 | 30/10/2014 | Improvement based on review comments (David Johnson)<br>Change made because of adoption STRIDE threat model. Explanation of the STRIDE model added |
| 0.7 | 30/10/2014 | Improvement based on review comments (Dr. Konstantinos Moulinos Expert in Network & Information Security- Resilience and CIIP European Union Agency for Network and Information Security - ENISA) |
| 0.8 | 07-11-2014 | Improvement based on review comments. Explanation of SOGIS and SOGIS MRA added to chapter 3.2 |
| 0.9 | 1-12-2014 | Some minor text changed based on comments (David Johnson)<br>Included contributions from TC13 (Bernd Schulz) and TC294 (Ortwin Pfaff) |
| 1.0 | 26-05-2015 | Incorporation of comments following presentation to SM-CG Plenary in January 2015, agreed at Task Force on 11th June |

# Contents

# 1 Introduction

## 1.1 Background and objectives

The Smart Meters 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 into 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 and a second (Part II) in November 2012. The first report comprised a repository of P&S requirements and an approach to select requirements for a final architecture and local situation. The second report focused on the definition of privacy requirements and contains an overview of certification approaches.

This document is the third document in the continuation of the work since June 2012. It represents the results of the work performed in 2014 and comprises:

- Overview of the smart grid threat landscape (introduction in document, spreadsheet in annex)
- Overview of mitigating measures to the threats defined in the threat landscape
- Result of ENISA workshops with respect to smart grid certification
- Recommendations concerning certification for Smart Meters
- Current status of security aspects in standardization
- Recommendations on further work by the Task Force on Privacy & Security 2015

The workplan for 2015 envisages:

- assisting the EG2 with identifying Best Available Techniques for the 10 common minimum functional requirements for smart metering roll-out under a cyber-security & privacy perspective
- completion of the SM-CG security package (use cases, threats, requirements) and working with ENISA on a security approach (general protection profiles) for smart meters
- the definition of a minimum set of requirements based on major threats and experience from the field.

This work will serve as input to EG2.

## 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 (figure 1). 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.

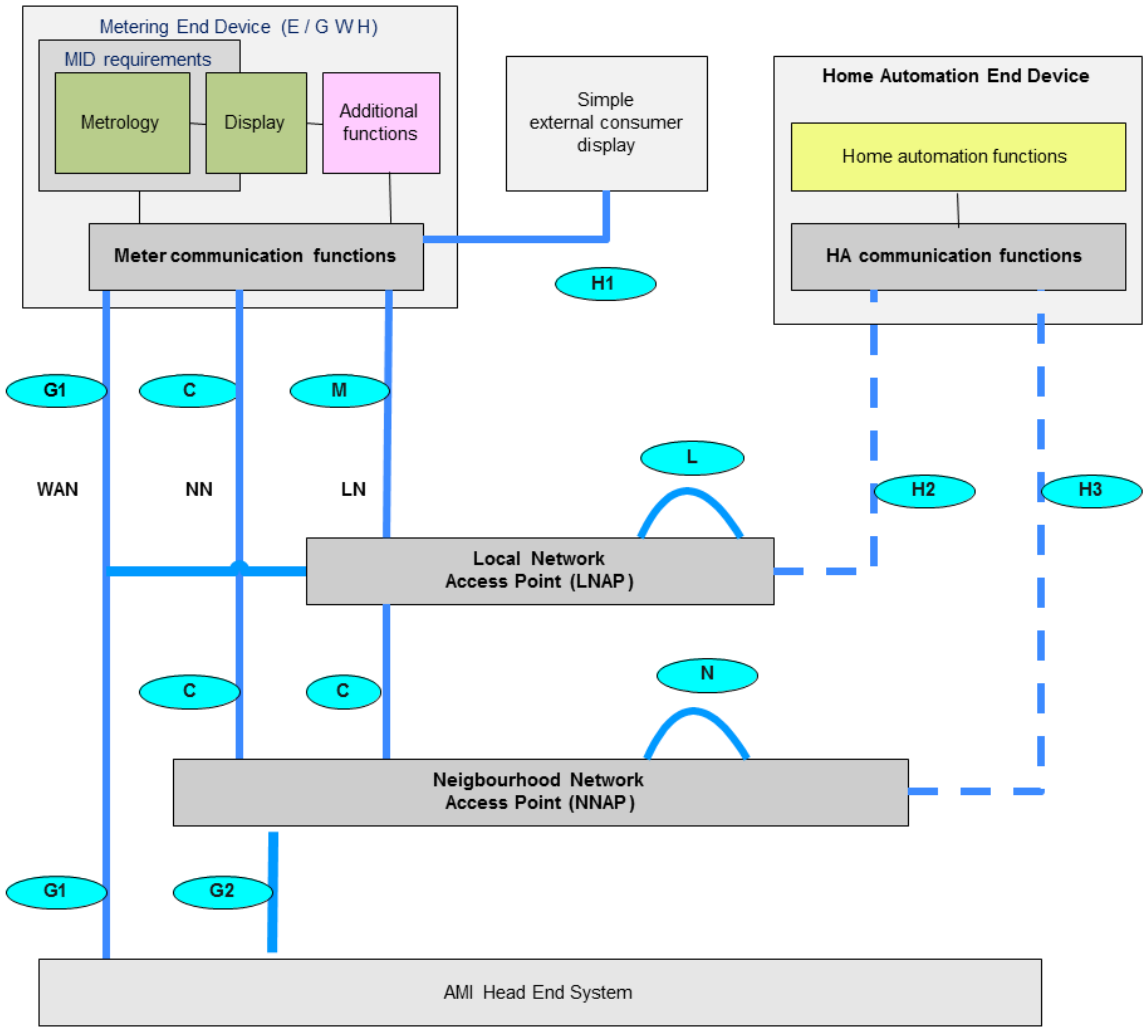


**Figure 1 – The SM-CG functional reference model**

The Task Force focuses on smart metering within the context of a smart grid and the privacy and security risks in this landscape. This 2014 report gives an overview of the work done by the Task Force to define

the smart grid threat landscape, the threats defined specific for the SM-CG reference architecture and mitigating measures.

# 2 Overview of the smart metering threat landscape

Various organizations have in recent years published reports on the threats in the field of cyber security in general, and smart grid security in particular. ENISA published their 2013 Threat landscape and a smart-grid threat landscape reports. NIST paid much attention to threats and vulnerabilities in general in its standard SP800-30r1. Expert Group 2 delivered their Data Protection Impact Assessment (DPIA) which contains a large overview of threats to personal data in a smart grid environment. All these reports are written with a general use in scope. The threats and vulnerabilities are general, and the measures are used worldwide. This is logical. Attackers are not bothered by borders or legislation.

Not only governments and government-driven organizations pay close attention to cyber criminals. Major commercial organizations each year produce reports of the threats identified, mainly organizations in the hardware branch, such as Dell and IBM, and organisations in the anti-virus and anti-malware sphere, such as McAfee and Symantec. American companies like Verizon and Mandiant carry out extensive research into these topics. Also, research organizations are paying more attention to this subject.

During summer 2014 the Task Force performed a study of available reports on cyber threats which are applicable in the advanced metering infrastructure landscape. The Task Force created an overview of recognized threats identified by the institutions mentioned above. The threats and security aspects were added, as well as threat sources and the risks that the threats to the smart metering sector entail. The security aspects are confidentiality, integrity and availability and/or a combination of these security aspects. 'Availability' includes potential impact on security of energy supply resulting from Denial of Service attacks. The spreadsheet created shows an overview of all advanced metering infrastructure related threats known at this moment. Threats however can change day-by-day.

The task force added security measures to every risk. The measures, as always, are divided into organisational and technical measures.

Organisational measures are measures such as:

- Clear policies and procedures
- Segregation of duties
- Documented patch management process
- Secure programming,
    - Secured programming environment, following the OWASP principles if web-based applications are built, removable media stored in a safe during night-time etc.

Technical measures are for example:

- End-to-end encryption
- Certificates
- Use of an automated system to signal connection disruptions
- Use of two factor authentication mechanisms etc.
- Tamper proof smart meters

The Task Force decided to cluster the threat groups into a smaller number so a simpler overview is created. By clustering groups which were connected to (almost) the same kind of threats it was possible to limit the analysis to eight threat groups:

1. Natural disaster (natural/environmental) including major internet outage
2. Eavesdropping, interception, hijacking (directed at the AMI)
3. Employee errors, unintentional damage (accidental), failures / malfunction
4. Information leakage, combining abuse of personal data and damage/loss (IT assets)
5. Lack of (maintenance) personnel
6. Legal e.g. unlawful collection of personal data, or forwarding it without consent
7. Nefarious activity/abuse (directed at the individual customer)
8. Physical attack (deliberate/intentional)

**STRIDE model**

STRIDE is a system developed by Microsoft for thinking about computer security threats. It provides a mnemonic for security threats in six categories. The STRIDE name comes from the initials of the six threat categories listed below. It was initially proposed for threat modelling, but is now used more broadly.

The threat categories are:

| STRIDE Categories | Explanation |
|---|---|
| **S**poofing identity. | An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password. |
| **T**ampering with data | Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet |
| **R**epudiation | Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Nonrepudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package. |
| **I**nformation disclosure | Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers. |
| **D**enial of service | Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability. |
| **E**levation of privilege | In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defences and become part of the trusted system itself, a dangerous situation. |

STRIDE considers the possibility of threats to the following types of data:

- Configuration data: connection strings to databases
- Authentication data: user names and passwords stored in the user's Profiles database.
- Persistent data: data stored and used by Commerce Server processes such as SQL Server data, XML data, registry data, files, authentication and authorization data, and logs.
- Data that travels over communications channels: cookies, authentication information, purchasing and ordering information, and credit card numbers.
- State data: data that indicates whether the user is logged in or logged out, and data stored in metering databases.
- Temporary data: data that is created by the processes running the site.

There are at least three general approaches for threat modelling:

1. Attacker-centric
   Attacker-centric threat modelling starts with an attacker, and evaluates their goals, and how they might achieve them. Attacker's motivations are often considered, for example, "The NSA wants to read this email," or "Jon wants to copy this DVD and share it with his friends." This approach usually starts from either entry points or assets.
2. Software-centric
   Software-centric threat modelling (also called 'system-centric,' 'design-centric,' or 'architecture-centric') starts from the design of the system, and attempts to step through a model of the system, looking for types of attacks against each element of the model. This approach is used in threat modelling in Microsoft's Security Development Lifecycle.
3. Asset-centric
   Asset-centric threat modelling involves starting from assets entrusted to a system, such as a collection of sensitive personal information.

The STRIDE threat model is attacker-centric based and it fits in the approach of the SM-CG and the privacy & security requirements developed by the Task Force.

The deliverables of this study are two spreadsheets which are attached as annexes to this report. The spreadsheets are intended as input to standardisation Technical Committees, to assist them in understanding requirements and to serve as input to certification schemes.

The first spreadsheet, SM-CG threat landscape_2014_09 gives an overview of recognized threats, threat groups, threat actors, threat details and possible mitigating measures. This spreadsheet is mostly based on ENISA, NIST and other important smart grid specific reports.
In this document, all eight threat groups are available and mitigating security measures are connected to each threat. The mitigating measures are best practices based on NIST SP-800, NIST.IR 7628 and ISO/IEC 27002:2013.

The second spreadsheet is called "SM-CG PrivacySecurity requirements_repository_2014_09".
This document is a follow-up version of the repository created by the Task Force in 2012. While the AMI security requirements were already connected to the Dutch privacy and security threats, it was now the possible to use the threat groups from the threat landscape to connect them to the AMI repository.

# 3 Recommendations concerning certification for Smart Grid environments

ENISA performed a study on cyber security certification approaches for smart grid devices, systems and related organisations in 2014.

ENISA organized two workshops to discuss the proposed approaches on certification in the smart grid environment. The first workshop took place on the 30th of September 2014 in Heidelberg (Germany) to discuss the results of the above mentioned study regarding cyber security certification approaches for Smart Grids.

On October 6, ENISA organized an additional workshop in Brussels in joint cooperation with the senior officials' group information systems security (SOG-IS)[1] and the European Commission (EC) to discuss in detail various certification approaches for general IT applications and also the process towards a European approach.

At both occasions the work of this AHWG were presented by Willem Strabbing (SM-CG). Although the final results still have to be reported, the following results were noted:

## 3.1 Heidelberg workshop 30 September 2014

During the Heidelberg workshop, Stakeholders presented existing ICT product certification schemes that could be applied to Smart Grids. The SM-CG report on Privacy & Security for Smart Metering produced by the Task Force, Part II, that analyses certification approaches for Smart Metering, has been used as input for the ENISA studies. ENISA expressed a need for a common EU approach and increased mutual recognition of certificates, to avoid national approaches which today converge to a large extent but not fully.

Because product requirements and specifically Privacy and Security requirements in the EU member states vary, the evaluation of such products has to be based on the individual merits of each product. An EU approach would have to be modular and recognise groups of functionalities instead of being holistic.

One of the conclusions was: there is no harmonization, different methods, schemes and different levels of security per country are used. This raises the question how the certification, which today is product-based, would work when a whole system needs to be secure.

The ENISA analysis points out that there are gaps with regard to systems certification, but that taking a product approach already permits a large spectrum of risks to be addressed. ENISA concluded that the EU should solve the following needs to fill the gaps:

- Need for a pan EU accepted definition of security levels for smart grid components
- Need for a common set of minimum requirements
- Need for a scheme that enables a pan European approach
- Need for EU based approach to facilitate legislation
- Need for a centralised place for certificate storage and distribution

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

- Need for a EU body to facilitate public-private interaction and provide guidance scheme implementation and keep the scheme up to date

**National IT security certification schemes**

The most important results of the Heidelberg workshop were:

- Persons certification:
  - A mandated procedure will not work
  - There should be different approaches for different roles (e.g. SCADA operator vs SCADA developer)

- System/product certification:
  - The approach should be flexible; there are different requirements in different member states
  - Requirements vary with architectures and functional implementations
  - Some ideas for follow-up: create multi stakeholder group to analyze a EU approach

The comment on the reports is now being processed and will be produced for the end of 2014 leading to a final report.

## 3.2 Brussels workshop 6 October 2014

In the 2013 report written by the Task Force (Part II), the Common Criteria approach was explained, that forms the basis for the approaches in Germany, UK and France.

The SOG-IS agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria. Participants in this Agreement are government organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association), representing their country or countries.

The participants work together to:

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

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

- As certificate consuming participants and
- As certificate producers

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

- Certificate recognition up to EAL4[2] (as in CCRA)
- Certificate recognition at higher levels for defined technical areas when schemes have been approved by the management committee for this level.

SOGIS/MRA is a platform for harmonising security certification across Europe. It is organised in co-operation with the European Commission and SOGIS MRA members. While the Common Criteria limits mutual recognition to intermediate levels of evaluation (up to EAL4), the so-called SOGIS MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement), was developed and signed in Europe which looks for the recognition of highest security levels (up to EAL7 level). SOGIS MRA was originally developed in the late nineties and is supported by an EU directive.

At the Brussels workshop the national schemes presented, all part of SOGIS-MRA, included The Netherlands (NLNCSA), France (ANSSI), Sweden (FMV), Germany (BSI). The national bodies mentioned all act as national accreditation bodies (with the addition that for France it is ANSSI together with COFRAC). Their role is to oversee national schemes and to issue certificates based on the testing results of the IT Security laboratories. They also ensure that the technical capabilities and skills of the testing laboratories are adequate. The certificates issued by national accreditation bodies cover product categories for which there is a defined use-case and a security protection profile specified by a technical community (stakeholder group) against which the testing laboratories will test the equipment and certification bodies will issue the certificate.

Protection profiles  A Protection Profile (PP) is a document used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC). As the generic form of a Security Target (ST), it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements. A PP is a combination of threats, security objectives, assumptions, security functional requirements (SFRs), security assurance requirements (SARs) and rationales.

A PP specifies generic security evaluation criteria to substantiate vendors' claims of a given family of information system products. Among others, it typically specifies the Evaluation Assurance Level (**EAL**), a number 1 through 7, indicating the depth and rigor of the security evaluation, usually in the form of supporting documentation and testing, that a product meets the security requirements specified in the PP.

**Panel discussion**

The panel discussion focussed on the advantages and challenges in using Common Criteria/SOGIS. Demand by risk owners (business users or sectorial agencies) is lacking because of the high cost involved in having a product certified; there is a need to share the cost among risk owners. Public procurement would be an important tool to promote compliance with ICT security certificates, but is not used in Europe as actively as in other parts of the world.

[2] EAL: Evaluation Assurance Level

Recommendations for EU action coming out of the panel discussion included the establishment of a forum where risk owners, vendors, testing laboratories and certification bodies can come together to identify areas where there is a need to define use-cases and establish protection profiles (e.g. firewalls, USB-sticks, web browsers, cloud etc.). The Commission should take a stronger role in linking its policy to ICT security certification. This could be done through a voluntary approach, e.g. based on an analysis of European industrial strengths which could inform user requirements; know-how centre; training, or through a regulatory approach. The regulatory push should be used in particular in the case of eIDAS[3], which should require compliance with IT security certificates for components covered by it.

Some conclusions and further steps that can be drawn from the workshop are:

- Contrary to the Common Criteria organization itself, SOGIS covers all EAL's and the certificates among members are recognized. Re-certification after changes being made in the product is not mandatory, but should be considered case by case.
- There are alternative certification approaches from ISO and IEC that should be considered.
- Different applications may require different certification approaches. Per application a stakeholder group should analyze the scope and possible approaches.
- Smart Grids/Metering are good candidates to be considered.
- There should be a clear market request.
- The EC should take into account SOG-IS in future regulation making and security requirements specification activities.
- A security certification and CC educational program should be established.
- The relationship between ISO/IEC 27001 and CC should be further examined.
- The EC should investigate the need for the creation of a 'now how' centre for ICT security certification.
- A security certification element should become part of the ENISA work program.

# 4 Status of the work by technical committees

## 4.1 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 was published last 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 800-627 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

[3] Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market. (Regulation (EU) N°910/2014)

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 work has been completed by the DLMS UA by publishing Green Book Edition 8 - covering the application layer protocol aspects - in July 2014 and publishing the Blue Book Edition 12 - covering the data model related aspects - in September 2014. The results will be brought to the IEC by end of 2014 by revising IEC 62056-5-3, IEC 62056-6-1 and IEC 62056-6-2. There will be no additional work on the topic until 2015.

### 4.2 TC205

In 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.
However, in a second phase, TC205 WG16 and WG18 look forward to applying the SGIS framework in order to refine the P & S requirements for HBES.

### 4.3 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 II (June 2014)".

In NOV 2013 CEN/TC 294 accepted the WG 4 report regarding security and privacy and agreed with "DECISION 153/2013 – Creation of a new preliminary work item for an Amendment to EN 13757-3" to task CEN/TC 294/WG 4.

According to this decision the working process work on amendment of EN13757-3 started immediately by expert meetings and web-sessions, tasking subgroups with dedicated items and involving external experts from other domains.

Based on the New Work Item Proposal the final draft of amendment will cover:

- 4 new security modes extend the existing two security modes 3 and 5
- (Each new security modes provides methods for encryption and authentication)
- Reservation of 4 security mode numbers for national usage.

- Additional methods for key derivation
- Additional method for key distributions
- A new layer for Authentication and fragmentation
- A generic procedure for Software update

The current draft of amendment was developed in WG4 by consensus.

With respect to this draft of amendment CEN/TC 294 agreed in NOV 2014 the following decisions (summarized):

- DECISION 163/2014 – Decision to convert WI000294021 (EN13757-3/prA1rev) from amendment to revision (EN13757-3 rev)
  due to higher complexity in developing an amendment

- DECISION 164/2014 – Activation of the work item on prEN 13757-3 rev
  due to maturity of first draft proposal

- DECISION 165/2014 – Guidance on the revision of prEN 13757-3 rev
  to prioritize specification of secure system architecture

In consequence the CEN enquiry draft pr EN13757-3 rev finalization schedule is within 12 months.

# 5 Recommendations on further work on Privacy & Security 2015

The Task Force proposes to the SM-CG that the Task Force continues in 2015 with the following activities

- Representation of the SM-CG in the work of the SG-CG on smart grid security and privacy

  - Via the SG-CG Smart Grid Information Security workgroup, we have had good dialogue with ENISA, with collaboration on SGIS security levels and integrating the EG2 Data Protection Impact Analysis (DPIA) template into the SGIS Framework. The work of the Smart Meter P&S Task Force has been especially useful in focusing on the threats associated with the AMI and agreeing a pragmatic approach to privacy threats.
  - The SGIS will continue as the Smart Grid Cybersecurity workgroup, advising and recommending on cybersecurity and privacy issues related to smart energy grids, including on standardisation. The SGC work programme is currently being scoped but is likely to include security standards, IT certification and security use cases.

- Involvement in the definition of Best Available Techniques (BAT) of Smart Meter related privacy and security by the Stakeholder Forum and Technical Experts Group of Expert Group 2 of the EU Task Force Smart Grids

  - With EG2 we have worked on the final version of the DPIA template and the application of this template in Smart Metering Use Cases. Improvements of the template have been made on our request. The template will be reviewed in the DPIA template test phase in 2015-2016
  - EG2 has installed a Stakeholder Forum (SF) this year that will work on an inventory of Best Available Techniques (BAT) for securing the Smart Metering infrastructure

- Reference to the BAT for mitigation actions related to the security risks in the Advanced Metering Infrastructure

  - The SM-CG has produced until now Use Cases and for Privacy & Security: a threat landscape and technical requirements
  - The BAT, being developed by EG2, would complete the documentation with an overview of techniques that can be used to mitigate the threats and comply with requirements.

The SM-CG AHG has made use of the methodologies developed both by SGIS (which are security focused) and EG2 (data protection). In its planned work to identify minimum requirements, the SM-CG will focus on security, recognizing that privacy may require a modified approach. The DPIA testing phase, in which the SM-CG AHG will be active, is an opportunity to refine the proposed methodology for security & privacy.

- Definition of minimum security requirements for the AMI, related to the major threats and latest experiences.

- As smart meters are deployed, there will be an increasing focus on security and privacy issues associated with the AMI and AMI communications
- The SM P&S Task Force will act as a focal point for addressing and responding to concerns in this area
- Liaise with ENISA for the on-going research study on Smart Grid (Cyber) Security Certification and explore how to apply the outcome of the study for helping capturing a minimum set of security requirements for smart metering

- Smart Metering security certification

- The proposal from ENISA for a Pan European entity overseeing Smart Grid certification, the generation of protection profiles and the ratification of national schemes make also fully sense for the Smart Metering domain
- It is therefore proposed that the SM-CG P&S taskforce utilizes the ENISA findings and explore how to leverage this work for defining a minimum set of security objectives in a protection profile, enabling accredited security testing labs at the European level to conduct security evaluations. This will ensure that smart meters put onto the network incorporate minimum 'security mitigations by design' against major identified threat which can be independently verified and certified at a national level