Smart Meter Co-ordination Group
Privacy and Security Approach – Part IV

Version: 1.1

Date: 17th July 2016

Authors: SM-CG Task Force on Privacy and Security

Members of the Task Force in 2015

Name	Representation	Role
David Johnson	SM-CG, SG-CG	Convenor
Willem Strabbing	ESMIG, SM-CG, SG-CG	Co-convenor
Uwe Pahl	TC294 - WG4	TC 294 liaison
Roman Picard	CRE/CEER	Member
Eric Farnier	TC 294	Member
Peter Berends	Netbeheer NL	Member
Denis Noel	ETSI-M2M	Member
Olivier Rochon	TC13	TC13 liaison
Marylin Arndt	ETSI-M2M	Member
Francois Ennesser	ETSI-M2M	Member
Anne-Marie Praden	ETSI-M2M	Member
Sylvie Wuidart	STMicroelectronics	Member

Version Control

Version	Date	Modifications
0.1	11/09/2015	First draft version by David Johnson
0.2	15/09/2015	V0.1 revised in light of initial comments by W. Strabbing
0.3	24/10/2015	V0.2 revised following conference call on 25th September & further input
0.4	05/11/2015	V0.3 revised following conference call on 30th October & further input
0.5	30/11/2015	V0.4 revised in light of input received in November & to ensure alignment with ESMIG report
0.6	10/12/2015	V0.5 with additional text from TC13, TC294 & TC205
0.7	17/02/2016	V0.6 with amendments after ANEC comments & editorial changes
0.8	05/03/2016	V0.7 as agreed by the SM-CG Task Force on Privacy and Security
0.9	18/04/2016	V0.8 plus DPIA comments from EC (section 4.2)
1.0	08/06/2016	V0.9 plus editorial changes
1.1	17/07/2016	V1.0 plus final editorial changes

Contents

1. Introduction to the Part IV report

1.1 Background to work of the Task Force

In 2012 the SM-CG Plenary meeting decided to continue to work on smart metering Privacy and Security and to produce further work as part of the SM-CG deliverables. A Task Force was formed to define the approach of the ESOs in this regard and to present the continuing work of the Technical Committees to address privacy and security.

The Task Force focuses on smart metering within the context of a smart grid and considers privacy and security risks in the context of the SM-CG functional reference model for smart metering communications, as developed in TR 50572.

Three reports (Reports I to III) have so far been produced. This report (Report IV) sets out the results of the work of the Task Force in 2015 and its relationship with the work of EG2.

1.2 Reports I to III

The three documents so far produced by the Privacy & Security Task Force comprise:

- The first report (Part I) in November 2012, which provided a repository of P&S requirements and an approach to select requirements for a final architecture and local situation
- The second report (Part II) in December 2013, which focused on the definition of privacy requirements and contained an overview of certification approaches
- The third document (Part III) giving the results of the work performed in 2014 and comprising:
    - overview of the smart grid threat landscape (introduction in the Part III 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 during 2015
- When Part III was disseminated at the end of 2014, comments were invited on the document and accompanying spreadsheets. Comments were reviewed in early 2015, amendments made and the 2014 documents finalized in the first half of 2015, with Task Force responses on the comments on the report sent to the commenters.

1.3 Part IV scope

The work plan for 2015 that was proposed in the Part III report envisaged:

- Definition of a minimum set of requirements based on major threats and experience from the field. Work under this item is considered in section 2 below.
- 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. This is considered in section 3.
- Working with ENISA on a security approach (general protection profiles) for smart meters (section 5) and
- Completion of the SM-CG security package (use cases, threats, requirements (Appendix & Section 7).

2. Identification of smart meter minimum security requirements

2.1 Introduction

In 2015, the Task Force considered the security requirements of several EU Member States with a view to establishing a set of minimum requirements, based on MS work to date.

The requirements repository consists of some 300 security requirements gathered from a variety of sources and drawing on work at a national level. The first version of this repository was created in 2012 and included in the Part I report. It was evident that these requirements are at different levels and the repository contains overlapping requirements, limiting its use.

The purpose of this aspect of Task Force work therefore was to identify the major areas of security concern, which would form some minimum security requirements for smart metering.

2.2 Security & Privacy

While there are many areas of commonality between security and privacy, confidentiality of information is seen primarily as a security issue. The work of the Task Force in 2015 did not expressly address privacy, which would have required a different approach to defining the risks and selecting requirements and techniques.

For smart metering privacy, the Task Force recognises that DPIA template represents a reasonable starting point. The Commission is currently overseeing work to test the DPIA template – see section 4 below. It is expected that further work on Privacy will be required when the DPIA test phase is complete.

2.3 Clustering approaches

In order to identify minimum requirements, a number of approaches to clustering the repository requirements were discussed and tried.

The first involved narrowing down the list of requirements and trying to select key requirements using a risk scoring method such as "DREAD" or the security risk management approach in ISO 27005 to help identify the most important risks to be addressed. The intention was eventually to be able to create a risk index per threat and then to estimate its probability.

However, as the work progressed, the Task Force found it was difficult to perform a risk analysis at an EU level. There was also the question of direct and indirect impacts, which made it hard to quantify risks in monetary terms.

A further approach was then examined by the Task Force. Rather than defining minimum requirements by using risk analysis, the requirements in the repository were examined, considering which were requirements and those that were more solutions. This in turn facilitated the identification of where there were overlapping or similar requirements. Commonalities in the repository would indicate requirements that a number of Member States think are important.

Another option considered involved basing the clustering on NIST's work (NISTIR 7628) Guidelines for Smart Grid Cybersecurity vol. 1, which considered security strategy, architecture and high-level requirements, and grouping the requirements under the following NIST headings.

1. Access Control (AC)
2. Awareness & Training (AT)
3. Audit & Accountability (AU)

4. Security Assessment & Authorisation (CA)
5. Configuration Management (CM)
6. Continuity of Operations (CP)
7. Identification & Authentication (IA)
8. Information & Document Management (ID)
9. Incident Response (IR)
10. Smart Grid Information System Development & Maintenance (MA)
11. Media Protection (MP)
12. Physical & Environmental Security (PE)
13. Planning (PL)
14. Security Programme Management (PM)
15. Personnel Security (PS)
16. Risk Management & Assessment (RA)
17. Smart Grid Information System & Services Acquisition (SA)
18. Smart Grid Information System & Communication Protection (CP)
19. Smart Grid Information System & Information Integrity (SI)

Each of these headings is further described in NISTIR 7628, together with numerous sub-headings. However many NIST requirements are organisational rather than infrastructure-focused.

Preliminary analysis applying the NIST categories to the requirements repository indicated that some requirements had not been expressed in a sufficiently precise way; it also suggested certain requirements could be considered under more than one heading.

2.4 Common Criteria methodology

The NIST IR clustering approach proved to be useful for grouping requirements into meaningful categories, but the following limitations were observed:

1. requirements and categories are tied to the Smart Grid business domain rather than Smart Metering
2. technical and organisational security requirements are mixed together
3. some technical security requirements specific to the smart metering technology are missing

So, in order to help to further refine the infrastructure security requirements, Trusted Labs, a security certification company, advised considering security requirements categories expressed in the Common Criteria terminology in terms of functional class names[1]. An advantage of using the Common Criteria categories is that the step towards a certification approach (see also the Task Force Part II report) is easier to make.

As a result, the following seven Common Criteria security classes were deemed relevant and were selected for the clustering of infrastructure requirements:

- Class FAU-Security Audit → Security Notification
- Class FCO-Communication → Secure Communication
- Class FCS-Cryptographic support → Cryptographic support
- Class FIA-Authentication and Identification → Access Control
- Class FDP-User Data Protection → Data Protection (at rest)
- Class FPT-Protection of the TSF → Self Protection

[1] The Common Criteria approach was explained in the 2013 report written by the Task Force (Part II). For more details, please refer to the document Common Criteria (CC) for Information Technology Security Evaluation in the security Part 2: Security functional components September 2012 Version 3.1.

- Class FMT-Security management → Security Management

Then the whole repository of national requirements was sorted using these new categories with Trusted Labs' guidance and this permitted the derivation of a minimum set of security requirements.

2.5 Collaboration with ESMIG

In parallel with this work, ESMIG was also looking to develop clusters of requirements, derived from NIST and Common Criteria.

It was agreed to collaborate with ESMIG in joint work also based on the repository, again with a view to identifying minimum requirements. A series of joint SM-CG/ESMIG workshops were held in which the requirements repository was analysed, and the original requirements repository of 2012 was extended with new requirements received from Austria and Great Britain. Focusing on the repository requirements mentioned by a number of Member States, it proved possible to evolve a number of minimum requirements, defined using common terminology, under which each of the requirements in the repository could be assigned.

2.6 Results

The following minimum requirements have been identified, all related to infrastructure security.

A All AMI components SHALL provide a log of security events
B All data exchanges SHALL take place in a (end-to-end) secure manner
C Availability of the system (AMI components and communication network) SHALL be sufficient to perform the Use Cases the system has been designed for
D Crypto mechanism and key management SHALL be documented and be compliant with recognized / proven and approved open standards
E Every AMI component SHALL check the authorisation of any entity requesting access to it and grant or deny access based on the result of that check
F Data at rest SHALL be protected in all system components
G AMI components SHALL be upgradable to incorporate new (security) functionalities
H Functionalities in AMI components SHOULD be limited to the intended operational Use Cases and SHALL not be able to compromise security functions
I AMI components and the communications network SHALL be adequately protected against external disturbances and/or attacks and SHALL demonstrate resilience against attacks

The above are considered in more detail in section 7 below, the Appendix and in the spreadsheet included as Annex A to this report. The spreadsheet also relates the high-level infrastructure security requirements A-I to the Common Criteria categories. Furthermore the spreadsheet shows the link between most of the original requirements defined by Member States with the minimum requirements now identified.

A stand-alone definition of the minimum security requirements has also been developed, including sub-requirements, implementation and evaluation guidelines for each requirement. This report is noted in the reference section at the end of this document.

The requirements A-I will also be useful in consideration of security certification (see section 5 below). Specification of a security certification scheme is typically based on a set of security objectives which can be easily derived from these minimum requirements.

As noted in section 8 below, further work related to organisational requirements is envisaged in the Task Force work programme planned for 2016.

3. Best Available Techniques

3.1 Project background & organisation

In 2015, Expert Group 2 of the EU launched an initiative to define the Best Available Techniques (BAT) for Smart Meter related privacy and security, and to evaluate / select the best techniques for securing the Smart Metering Infrastructure. A Technical Experts Group has been established, supported by a Stakeholder Forum to review and agree output.

Members of the Task Force have been involved in this work and are active in the BAT Stakeholder Forum, with William Strabbing formally representing the SM-CG.

So far the first section of the ultimate report has been drafted, proposing an approach for the evaluation of Best Available Techniques. A questionnaire has been prepared to gather information on the techniques used or envisaged to be used, with first responses requested in December 2015. These techniques will then be evaluated by the project team according to the methodology developed in the first half of 2015.

3.2 Alignment of BAT work with SM-CG

To ensure alignment with previous work of the SM-CG, spreadsheets have been sent to the Commission's project leader, together with suggested text to try to position the work. It was noted that while it was valid to evaluate security techniques in terms of what might be most advanced, final selection of techniques by a MS or industry would depend on the nature of the particular deployment, industry structure and other factors. There was also the point that security should be seen as an end-to-end aspect and not restricted to technical security.

Another critical area for alignment was in the representation of communications interfaces. Work was therefore undertaken to use/adapt the M/441 reference model and the work of the SG-GC on flexibility to support the BAT work, in particular in referring to communications interfaces and the mapping of use cases.

3.3 Results to date

The questionnaire is being made available via trade associations and other routes, and information gathered from various market actors. The results of the questionnaire will require careful evaluation, and a Commission report on the findings will be produced in 2016. The Task Force will investigate how its Minimum Requirements link to the BATs when these are published.

4. Data Protection Impact Assessment template test phase

4.1 Background

The purpose of the DPIA is to provide guidance on how to perform a Data Protection Impact Assessment (DPIA) to Smart Grid and Smart Metering systems. With EG2, the Task Force worked on the final version of the DPIA template during 2014 and the application of this template in Smart Metering Use Cases.

The template is being reviewed in the DPIA template test phase in 2015-2016. The testing phase is envisaged as a means to consider the application and usability of the template. The testing phase is due to be concluded in the autumn of 2016.

David Johnson and Roman Picard have represented SM-CG Task Force in the testing phase.

4.2 Work to date

Following its inception in March 2015, the test phase has built up momentum and so far 7 companies (Alliander, EDP Distribucão, ENEL, Endesa, Österreichsenergie, Iberdrola, Enexis) have actively tested the template by applying the ex-ante impact assessment to real-life use-cases. Following a first workshop organised in May 2015 with EDP and Alliander presentations, a second workshop was organised by the Commission in January 2016, with presentations by ENEL, Iberdrola and Enexis. With ERDF, Eandis and CEZ due to participate in a third workshop on 25th April, the industry representatives voluntarily signing up to the test phase cover more than one third of European electricity consumers.

The main highlights of the workshops reveal that the testing conducted so far by the industry is positive in terms of the true complexity of use-cases selected, test team expertise, general awareness raising on data protection and rigorously running the exercise through all the steps of the template. However, results are more mitigated as regards Data Protection Authority involvement and support and general time dedicated to the exercise.

A mid-term assessment held in February concluded that the main findings of the test phase so far focus on streamlining the new General Data Protection Regulation provisions, integrating the Best Available Techniques in the control section, enhancing the connection between the descriptive and operational parts and streamlining redundant steps.

The changes agreed to during the mid-term assessment conducted by DGs ENER and JRC and WP29 will be implemented by an editorial team of beta-testers.

Based on this feedback, and in light of the General Data Protection Reform and the ENER-JRC led identification of the Best Available Techniques for smart metering, the template will be fine-tuned at the end of the test phase, in order to enhance its efficiency and user-friendliness.

5. Work with ENISA on certification

5.1 Background

In 2014, ENISA, the European Union Agency for Network and Information Security, performed a study on cyber security certification approaches for smart grid devices, systems and related organisations. Currently there is no harmonisation; different methods, schemes and different levels of security per country are used. This raises the question how certification, which today is product-based, would work when a whole system needs to be secure.

5.2 System certification

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 to fill the gaps the EU should solve the following needs:

- need for a pan-EU accepted definition of security levels for 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
- need for an EU body to facilitate public-private interaction and provide guidance scheme implementation and keep the scheme up to date

ENISA recognises the 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. The European Commission is also keen to see progress in this area. However, because system and product requirements - and specifically privacy and security requirements - in the EU member states vary, evaluation of products has to be based on individual merits. An EU approach would have to be modular and recognise groups of functionalities instead of being holistic.

5.3 Smart metering certification

ENISA will be considering a number of sectors for possible certification in the course of 2016, having regard to the coming Network and Information Security (NIS) Directive, with a view to advising the European Commission on future action in 2017. ENISA has yet to determine the approach for this work, which will draw on input from a wide range of stakeholders and look at different assurance techniques e.g. Common Criteria or IEC 62443.

ENISA, in common with SOG-IS (the Senior Officials Group - Information Systems Security), recognise that smart grids and smart metering are good candidates for security certification. One option for ENISA work in 2016 would be to associate different risk impact levels in the SGAM model with different conformity assessment and testing techniques.

5.4 General protection profiles for smart meters

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 to 7, indicating the depth and rigour of the security evaluation, usually in the form of supporting documentation and testing, that a product meets the security requirements specified in the PP.

5.5 Future work

The high-level requirements identified in section 2 of this report and described in detail in the Appendix and in the spreadsheet included as Annex A will be useful in consideration of security certification and will assist continuing co-operation with ENISA. The minimum requirements can be used to develop security objectives, which in turn will assist the specification of a suitable security certification scheme.

Further work in this area is planned for 2016, in conjunction with ESMIG. This will be undertaken in collaboration with ENISA, in order to provide input to their further work in this area.

6. Status of the work by technical committees

6.1 TC 13

The Security and Privacy Task Force of CENELEC TC13 WG02 has completed its work - carried out in liaison with the DLMS User Association - related to extending the security features in DLMS/COSEM.

The extended security features provide authentication of the communicating entities using a ciphered challenge-response mechanism (High Level Security authentication), protection of both DLMS/COSEM application layer messages and COSEM data using symmetric key authenticated encryption (AES-GCM) and digital signature (ECDSA) that can be applied end-to end between clients (HES) and servers (meters) as well as between third parties and meters. For key management symmetric key (AES key wrap) and public key (ECDH) algorithms are available.

These results have been brought also to the IEC to be published in new editions (Edition 3) of the IEC 62056-5-3 DLMS/COSEM Application layer, IEC 62056-6-1 OBIS and IEC 62056-6-2 COSEM interface classes standards.

IEC TC13 has become a TC representative in ACSEC, the IEC Advisory Committee on Information security and data privacy. The role of the ACSEC is further described in 6.5 below.

6.2 TC 294

In 2015 CEN/TC 294/WG4 worked on a full revision of existing EN13757-3:2013. The new standard draft contains four new security modes supporting encryption and authentication methods to secure exchange of smart meter messages. These several security modes reflect different national privacy and security requirements within the European Union, also ensuring co-existence to avoid interference in the standard. Nevertheless all security modes provide symmetrical cipher methods (in particular CBC, CCM, CTR, GCM) based on AES128 algorithm, which allows an accepted protection even in context of battery operated devices.

The new draft standard also provides new protocols for key management and for software update allowing keys and security methods in a smart metering system to be kept up-to-date.

Considering that the published standard consists of about 150 pages and considering that a number of new sections were added to cover new security modes, CEN/TC 294 agreed to split the existing EN13757-3:2013 in two new parts:

- EN 13757-3, Communication systems for meters — Part 3: Application protocols

- EN 13757-7, Communication systems for meters — Part 7: Transport and security services.

CEN/TC 294 decided in November 2015 to release these new drafts of EN13757-series to enquiry stage. The new prEN13757-3 and prEN13757-7 will be published in first quarter 2016.

Also CEN/TC 294/WG4 is assigned to generate a new Technical Report providing additional information to the requirements determined in EN 13757-2, EN 13757-3 and EN 13757-7, in particular examples for the implementation, datagram examples with protection by security mechanisms of part 7 and additional non-normative requirements beyond meter communication itself.

6.3 TC 205

In addition to its work on the EN 50491 series, CLC TC205 works on the updating and extension of the EN 50090 Home and Building Electronic Systems communication series. This work is done in close co-operation with the CLC Partner Organization, KNX.

As a new extension to the EN 50090 protocol, KNX is currently finalizing a draft for a new part EN 50090-3-4 on Data Security, which allows for authentication and encryption of data sent from and to HBES device functions according AES 128 CCM.

The new EN part describes the introduction of an additional secure application layer in the HBES stack. This allows manufacturers to foresee data points in applications offering authentication and/or encryption for sending and reception of data. The standard includes also information on tool based assignment of security keys, specifically the use of the Factory Default Setup Key, in addition to access control through roles and permissions. In an informative annex the use of CCM is explained, as well as an example given of a HBES Secure APDU.

6.4 Advisory Committee on Security (ACSEC)

ACSEC deals with information security and data privacy matters which are not specific to one single technical committee of the IEC. It coordinates activities related to information security and data privacy, and provides advice to the SMB on those subjects.

The role of ACSEC is in essence:

- to provide guidance to TC/SCs for implementation of information security and data privacy in a general perspective and for specific sectors.
- to provide a venue for exchanging information between the IEC and other standards developing organizations relevant to ACSEC’s scope.
- to closely follow research activities and trends in Academia

ACSEC guidance to TCs will be formalised through a guide. The structure of this guide has been agreed and a first draft is currently being prepared.

7. Completion of the SM-CG security package (use cases, threats, requirements)

7.1 Repository spreadsheet

The spreadsheet originally developed in 2014 and subsequently refined is a working document bringing together in a convenient form the detailed analysis by the Task Force during 2014-2015 of threats and requirements. It now comprises:

- the 300 or so smart metering infrastructure Privacy & Security requirements assembled in 2014
- analysis of these requirements according to the following categories:
  - Security Notification
  - Secure Communication
  - Cryptographic Support
  - Access Control
  - Data Protection
  - Self-Protection
  - Security Management
- assignment of most of these requirements to the minimum requirements identified in 2015 and noted in section 2.6 above
- a description of each of the minimum requirements, identification in some cases of sub-requirements, implementation recommendations and suggested approach to evaluation.

7.2 Summary of the work of the Task Force

Taken together, the four reports of this Task Force (Parts I – IV) comprise a comprehensive security package covering the following aspects:

- development of smart metering security & privacy use cases and mapping to the Smart Grids Architecture Model (SGAM)
- consideration of smart meter risks and risk impact, within the context of the smart grid threat landscape and smart grid security assessment
- identification of specific threats applicable to the AMI and suggested controls
- gathering of a repository of privacy and security requirements
- application of the European Data Protection Impact Assessment template to smart metering
- development of high level minimum requirements and implementation recommendations and evaluation. These in turn feed into the current Commission initiative on Best Available Techniques.

The reports also present the progress of the work by Technical Committees on security and privacy as the work has evolved over the past three years.

8. Recommendations for further work on Privacy & Security in 2016

8.1 General work of the Task Force

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 continue to act as a focal point for addressing and responding to concerns in this area. It is suggested that the CCMC (Monica Ibido) should serve as the initial contact point for reporting security issues that arise in the field which concern standardisation. This arrangement will be subject to evaluation in 2016 to decide if it should be continued, improved or cancelled.

8.2 Requirements repository & the minimum security requirements for the AMI

The requirements repository will be extended as necessary to reflect new requirements identified in deployments across Europe.

The Task Force intends to produce a stand-alone report with detailed definitions of the minimum requirements, including sub-requirements, implementation guidelines and evaluation guidelines in the first half of 2016.

At the same time, the minimum security requirements for the smart metering infrastructure will be kept under review, related to the repository and major threats perceived and latest experiences.

Work to date has focused on technical security. Further work will be undertaken in 2016 to consider organisational security requirements.

8.3 Smart Metering security certification

As noted previously, the minimum requirements identified in section 2 and described in detail in the Appendix and accompanying spreadsheet (Annex A) can readily be used to derive a set of infrastructure security objectives.

It is therefore proposed that the SM-CG P&S Task Force, in conjunction with ESMIG, works with ENISA, exploring 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 work will be taken forward in 2016, against the background of the proposal from ENISA for a pan-European entity overseeing Smart Grid certification, the generation of protection profiles and the ratification of national schemes.

The ultimate objective is to 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.

8.4 Privacy

Further work on privacy will be undertaken following the completion of the DPIA test phase in October 2016.

Appendix

Summary of smart meter minimum requirements (& sub-requirements) related to infrastructure security

A All AMI components SHALL provide a log of security events

A1 Secure access to the log

A2 Provide memory for a minimum number of entries. Mechanisms shall exist in order to prevent filling up the (FIFO) logs

A3 Every entry SHALL have a timestamp and sequence number

A4 Every entry SHALL identify the source of the security event

A5 Critical events SHALL trigger alarms

A6 Each log entry SHALL be protected against modification

B All data exchanges SHALL take place in a (end-to-end) secure manner

B1 All data exchanges SHALL be cryptographically protected and optionally also physically protected. Since Risk Analysis may indicate different levels of protection are appropriate, exceptions to this encryption requirement MAY be possible for certain data (e.g. the meter serial number)

B2 Different levels of protection MAY be provided, depending on the type of the data

B3 Security SHALL be implemented independently of the communication protocol.

B4 The contextual validity of information exchanged SHALL be checked

C Availability of the system (AMI components and communication network) SHALL be sufficient to perform the Use Cases the system has been designed for

C1 The availability of the system SHALL be monitored

C2 The system and its components SHALL start-up and recover from failures in a defined and secure way

C3 The system SHALL be designed in such a way that If communication failures occur they result in only minimal effects on the system availability

C4 In case of failure, system components SHOULD not compromise their own security or that of other components of the AMI

D Crypto mechanism and key management SHALL be documented and be compliant with recognized / proven and approved open standards

D1 The description of the crypto mechanisms and key management SHALL be publically available (based on open standards).

D2 Documentation SHALL include all implemented features, in particular:
- Cryptographic algorithms
- Key and signature length
- Client/server authentication
- Specification of entropy
- Cryptographic Random Number Generation
- Storage of keys

E Every AMI component SHALL check the authorisation of any entity requesting access to it and grant or deny access based on the result of that check

E1 Every data point and function SHALL have defined access rights

E2 Every entity SHALL be uniquely identifiable

E3 Access SHALL be temporarily denied after a specified number of unsuccessful attempts

E4 Access rights SHALL expire after a pre-defined time

F Data at rest SHALL be protected in all system components

F1 Different levels of protection SHALL be provided, depending on the category of the data. Categories include:
- Metrologically certified data (e.g. consumption/generation measurements
- Credentials
- Configuration
- Firmware

F2 Obsolete data SHALL be permanently deleted

F3 Modifications of data in specific categories SHALL be identified and logged, including initiator details

G AMI components SHALL be upgradable to incorporate new (security) functionalities

G1 Security functionality in AMI components SHALL be updatable (bug fixes) and upgradable (additional functionalities)

G2 AMI components SHALL allow spare capacity (memory and CPU power) for updates and upgrades

G3 Integrity and authenticity of update images SHALL be verified before they are applied or activated

H Functionalities in AMI components SHOULD be limited to the intended operational Use Cases and SHALL not be able to compromise security functions

H1 Interfaces that are not used SHALL be disabled

H2 Disabled functions of AMI components SHALL not compromise security functions

I AMI components and the communications network SHALL be adequately protected against external disturbances and/or attacks and SHALL demonstrate resilience against attacks

References

SM-CG

- SM-CG Privacy & Security Task Force report Part I : ‘Smart Meters Co-ordination Group Privacy and Security approach – part I’ - SM-CG Sec0064_DC (2012, updated July 2013)
- SM-CG Privacy & Security Task Force report Part II: ‘Smart Meters Co-ordination Group 2 Privacy and Security approach – part II’ - SM-CG Sec0073_DC (2013)
- SM-CG Privacy & Security Task Force report Part III : ‘Smart Meters Co-ordination Group Privacy and Security approach – part III’ - SM-CG Sec0084_DC (2014, amended June 2015)
- SM-CG Privacy & Security requirements repository – SM-CG Sec0084_DC_Annex2 (2014)

NIST

- NISTIR 7628 Guidelines for Smart Grid Cybersecurity vol. 1

Common Criteria

- Common Criteria (CC) for Information Technology Security Evaluation in the security Part 2: Security functional components September 2012 Version 3.1.

SM-CG Task Force on Privacy and Security / ESMIG

- Minimum security requirements for AMI components - European level requirements for Smart Metering – July 2016