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

Minimum security requirements for AMI components

European level requirements for Smart Metering

Version: 1.1

Date: 17th July 2016

Authors: SM-CG Task Force on Privacy and Security / ESMIG

Contents

References

[1] - Functional reference architecture for communications in smart metering systems, CEN/CLC/ETSI TR 50571, December 2011

[2] - CEN/CENELEC Internal Regulations Part 3:2015 (Annex H) http://boss.cen.eu/ref/IR3_E.pdf

[3] – ISO/IEC 15408 (*Common Criteria for Information Technology Security Evaluation)*

[4] – Requirements Catalog, End-to-End Security for Smart Metering, version 2014-1.0, ENCS, 3 December 2014.

[5] Use Case definitions SMCG_Sec0060_DC_UseCaseReport (November 2012)

Some acronyms

NIST: National Institute of Standards and Technology

NSA: National Security Agency

MISRA: The Motor Industry Software Reliability Association

Introduction

Scope

This document describes minimum security requirements for components of AMI infrastructures. Based on the work done under the Smart Metering Co-ordination Group (SM-CG) in which the security requirements of some major EU Member States were assembled, the Security and Privacy Working Group of ESMIG and members of the ad hoc SM-CG Task Force on Privacy and Security have developed a set of generic minimum requirements that are valid for most of the European Member States.

The scope of these requirements is any AMI infrastructure following the architecture defined in the SM-CG report "Functional reference architecture for communications in smart metering systems" [ref.1]. The requirements cover all components from the Smart Meter(s) to the Head End System.

Whereas the requirements collected by SM-CG consider the technical and the organisational aspects, this document focuses only on the technical aspects concerning the components and communication links of the AMI.

Objectives

The requirements defined here can serve as a basis for the specific requirements of the Member States. Such specific requirements shall be based on a Risk Analysis assessing the local situation, where the specific assets and the actors are considered.

The minimum requirements can also serve as a basis to specify the security certification scheme for the AMI components. The SM-CG has investigated various approaches applied in Member States for security certification and concluded that it would be beneficial to have a common approach in order to support the European internal market. The specification of the security certification scheme is typically based on a set of security objectives which can easily be derived from the minimum requirements.

Process

The process to define the minimum requirements started with clustering the comprehensive set of requirements collected in the SM-CG repository. The clustering categories were derived from Common Criteria [ref.3]. Clustering these requirements shows that for many common requirements the EU Member States use different naming schemes. Further, prioritisation of specific requirements is heavily dependent on the Member State. The identified clusters are:

- Security Notification
- Secure Communication
- Cryptographic Support
- Access Control
- Data Protection
- Self-Protection
- Security Management

These clusters are uniquely linked to Functional Requirement categories of the Common Criteria [ref.3].

Each of the seven resulting clusters contains a set of similar requirements from the SM-CG repository. The cluster based minimum requirements are added to the original SM-CG repository to preserve the link to the original requirements from member states.

The SM-CG reported about this process and its outcomes through the updated repository and in the 2015 report of its Ad-Hoc working group “Privacy and Security”.

Summary of the requirements

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

Wording

The wording used to define the requirements follows the definition of keywords in CEN/CENELEC Internal Regulations Part 3:2015 (Annex H) [ref.2]:

SHALL - This word (or the terms "IS REQUIRED" or "IS NECESSARY") indicates requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.

SHOULD - This word (or the phrase " IS RECOMMENDED") indicates that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

MAY – indicates a course of action permissible within the limits of the document.

Minimum requirements specification

Structure of the requirements

The format of this report has been inspired by the Requirements Catalogue that was developed by the European Network for Cyber Security (ENCS) authorised by Oesterreichs Energie [ref.4].

Each requirement below covers five parts:

1. The requirement title
2. The requirement description (generally mandatory)
3. Any sub-requirements
4. Implementation guidance on suggested way(s) in which the (sub-)requirement may be met
5. Assurance guidance on suggested way(s) of testing / evaluation of the (sub-) requirement

A: All AMI components SHALL provide a log of security events

Description	For a list of security events see Annex A.
Implementation guidance	The AMI components are equipped with sufficient capabilities to: - register communication sessions and identify the users; - register attempts to compromise the security of the device; - provide alarm functionality for specific events; - make the log accessible for evaluation via a standardized interface.
	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The registration of multi-user successful and unsuccessful access is tested by accessing the component with multiple users. A minimal set of security compromising actions is applied to the component and the corresponding registration and alarms are checked.
	The evaluator checks the documentation.

Sub-requirement	**Secure access to the log.**
Implementation guidance	Access control to access the security log is implemented.
Assurance guidance	The evaluator checks the access control by performing authorised and unauthorised access.

Sub-requirement	**Provide memory for a minimum number of entries.** **Mechanisms shall exist in order to prevent filling up the (FIFO) logs.**
Implementation guidance	The resources available for the log are documented.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**Every entry SHALL have a timestamp and a sequence number.**
Implementation guidance	Evident.
Assurance guidance	The evaluator checks the log.

Sub-requirement	**Every entry SHALL identify the source of the security event.**
Implementation guidance	E.g. for tampering identify the nature of the event (broken seal, magnetic interference, etc.).
Assurance guidance	The evaluator checks the log

Sub-requirement	**Critical events SHALL trigger alarms.**
Implementation guidance	The criterion for a critical event is defined and configurable.
Assurance guidance	The evaluator checks the alarms for specific events.

Sub-requirement	**Each log entry SHALL be protected against modification.**
Implementation guidance	Role based access control is implemented only for clearing the log (resulting in a new event).
Assurance guidance	The evaluator checks the access control by performing authorised and unauthorised access.

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

Description	Protection against Replay, Disclosure, Modification, Impersonation during data exchange (e.g. readings, commands, alarms, credentials, etc.).
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**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**
Implementation guidance	Implementation of encryption (and authentication) is possible for messages exchanged between any AMI system component independent of the communication medium used for the data exchange.
Assurance guidance	AMI components are tested by sending correctly protected messages and incorrectly protected messages to the components.

	The responses of the AMI components are checked for correct protection.
Implementation guidance	The manufacturer documents the security mechanisms and the protocols used in the AMI system.
Assurance guidance	The evaluator checks the documentation for the security mechanisms used.
Implementation guidance	The manufacturer adds an incrementing counter per message to assist in detecting message replay or implements another replay protection such as a time based mechanism (e.g. token).
Assurance guidance	The evaluator checks that replayed messages are detected and rejected.
Implementation guidance	Encryption and authentication is accessible for evaluation via a standardized interface. The protocols used for the message exchange are based on open standards.
Assurance guidance	The evaluator confirms that the AMI component has been certified for implementing a standard protocol.

Sub-requirement	**Different levels of protection MAY be provided, depending on the type of the data.**
Implementation guidance	Data is classified into pre-defined application categories. The protection level is made configurable depending on the application category of the data.
Assurance guidance	The evaluator verifies the correct protection for the different application categories of data in commands, responses and alerts.

Sub-requirement	**Security SHALL be implemented independently of the communication protocol.**
Implementation guidance	Application layer security is implemented. In addition, lower layer security mechanisms may be implemented.
Assurance guidance	The evaluator verifies that end-to-end security is provided without communication protocol security being in place.

Sub-requirement	**The contextual validity of information exchanged SHALL be checked.**
Implementation guidance	Validation of messages on system or on device level (where the context is available) is considered and the validation rules specified. For example the grid or credit status can be used as a context when activating the switch in a meter
Assurance guidance	The evaluator modifies the context of messages at system level and then checks the validation based on the specified validation rules.

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

Description	The AMI system requirements describe the Use Cases to be supported by the system. The Smart Meters Coordination Group has developed a general set of AMI Use Cases [ref 5].
Implementation guidance	The manufacturer provides design evidence ensuring that the Use Cases are supported. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The evaluator checks the documentation.
Implementation guidance	The manufacturers of the components provide standardized failure statistics, MTBF (mean time between failures) or others.
Assurance guidance	The evaluator checks the failure statistics.

Sub-requirement	**The availability of the system SHALL be monitored.**
Implementation guidance	Supervision of the availability of the AMI components and the communication network is implemented. The communication network operator provides statistics on the reliability of the message exchange in the network.
Assurance guidance	The evaluator checks the output of supervision functions and the network statistics.

Sub-requirement	**The system and its components SHALL start-up and recover from failures in a defined and secure way.**
Implementation guidance	The manufacturer implements and documents error recovery capabilities for the system and its components.
Assurance guidance	The availability and recovery is tested by inducing communication and component failures.

Sub-requirement	**The system SHALL be designed in such a way that if communication failures occur they have only minimal impacts on the system availability.**
Implementation guidance	The effect of communication failures is documented.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**In case of failure, system components SHOULD not compromise their own security or that of other components of the AMI.**
Implementation guidance	Software protection measures are included in the design process (e.g. by applying the MISRA rules).
Assurance guidance	The evaluator checks the software design procedures.

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

Description	Examples of such standards can be found in the NIST recommendations (or NSA suite B).
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**The description of the crypto mechanisms and of the key management SHALL be publically available (based on open standards).**
Implementation guidance	The mechanisms providing encryption and authentication considers NIST recommended (or NSA suite B) cryptography suitable for AMI applications.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**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**
Implementation guidance	Evident.
Assurance guidance	The evaluator checks the documentation.

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

Description	Entities include persons and components. Components are all system parts that support AMI functions. Authorisation determines the access rights of the entity to the AMI component.
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	Every data point and function SHALL have defined access rights.
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	This requirement is verified in a functional security test. The test specifically ensures that each entity has only the defined and necessary privileges.

Sub-requirement	Every entity SHALL be uniquely identifiable.
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	Access SHALL be temporarily denied after a specified number of unsuccessful attempts.
Implementation guidance	The time for denial of access and the number of unsuccessful attempts to trigger the denial is defined and configurable.
Assurance guidance	The evaluator tests the denial of access mechanism.

Sub-requirement	Access rights SHALL expire after a pre-defined time.
Implementation guidance	The expiry time is defined and made configurable.
Assurance guidance	The evaluator changes the clock date/time and tests the denial of access.

F: Data at rest SHALL be protected in all system components

Description	The protection concerns unauthorised disclosure and modification.
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**Different levels of protection SHALL be provided, depending on the application category of the data.** **Categories include:** **- Metrologically certified data (e.g. consumption/generation measurements)** **- Credentials** **- Configuration** **- Firmware**
Implementation guidance	The system components implement different levels of protection in a documented way. All data that has been classified as sensitive (determined via the Risk Analysis) should have highest level of protection.
Assurance guidance	The manufacturer shows that data at rest is protected by showing the application categories and the protection applied.

Sub-requirement	**Obsolete data SHALL be permanently deleted.**
Implementation guidance	A deletion function is implemented.
Assurance guidance	The evaluator checks the deletion function.

Sub-requirement	**Modifications of data in specific application categories SHALL be identified and logged, including initiator details.**
Implementation guidance	Implement a log file for modification of specific data categories.
Assurance guidance	Modifications are made and the log file inspected.

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

Description	This refers to both hardware and software.
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**Security functionality in AMI components SHALL be updatable (bug fixes) and upgradable (additional functionalities).**
Implementation guidance	Update functionality is implemented.
Assurance guidance	The evaluator performs an update (with valid and invalid images), activates and checks the result

Sub-requirement	**AMI components SHALL allow spare capacity (memory and CPU power) for updates and upgrades.**
Implementation guidance	The manufacturer specifies the spare capacities in memory and CPU power.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**Integrity and authenticity of update images SHALL be verified before they are applied or activated.**
Implementation guidance	The verification process is implemented and documented.
Assurance guidance	The evaluator performs an update (with valid and invalid images), activates and checks the result.

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

Description	
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification.
Assurance guidance	The evaluator checks the documentation.

Sub-requirement	**Interfaces that are not used SHALL be disabled.**
Implementation guidance	The function to disable interfaces is implemented.
Assurance guidance	The evaluator disables interfaces and verifies the status of each disabled interface.

Sub-requirement	**Disabled functions of AMI components SHALL not compromise security functions.**
Implementation guidance	The system is designed in such a way that functionality blocks do not interfere with security functions in an unintended way.
Assurance guidance	The evaluator checks the effect on security by disabling functionalities.

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

Description	Disturbances and attacks can be: tampering, EMC, Clock/ Date/ Time change, Denial of Service.
Implementation guidance	The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification. The manufacturer implements protection measures against a sufficient range of attacks, including: - Tampering - EMC - Clock/ Date/ Time - Denial of service
Assurance guidance	The evaluator checks the documentation. The evaluator carries out penetration and other protection testing.

Annex A – List of security events

Event
User Authentication for a particular role: • Successful authentication • Failed authentication
Firmware updates • Successful firmware updates • Failed firmware updates due to invalid digital signatures
Setting the time of the device
Tamper detection
Power-down of the device
Power-up/resume of the device
Reset or reboot of the device
Watchdog triggered reset
Device errors
Reconfiguration of cryptographic parameters • Key changes • Change of access rights • Reset of random number generator
Energy supply connect/disconnect
Load limitation configuration and activation
Security attack attempt