Security architecture program

Security requirements for procuring smart meters and data concentrators

Version 2.3

22 July 2019

This document was produced in the ENCS program on Security Architectures. This program concerns technical measures systems secure. The ENCS security architectures program is meant to:

- Facilitate information and knowledge sharing on security architectures between ENCS members
- Develop new ENCS services in the area of security architectures based on member needs

The document is part of a series of procurement requirements, including:

- Security requirements for procuring distribution automation RTUs
- Security requirements for procuring substation gateways
- Security requirements for procuring substation IEDs
- Security requirements for procuring substation HMI software
- Security requirements for procuring electric vehicle charge stations

The documents are available through the ENCS port (https://encs.eu/documents).

This document is shared under the Traffic Light Protocol classification:

TLP White - public

The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training.

Version History

Date	Version	Description	Authors
16 February 2015	1.0	Initial release to members	Christiane Peters
8 October 2018	2.0	Updated version based on testing experiences since release 1.0	Maarten Hoeve
22 July 2019	2.3	Version updated with feedback from EDSO cyber-security task force	Maarten Hoeve

ENCS

Table of Contents

1 Introduction

This document contains security requirements for procuring Smart Meters and Data Concentrators. They are intended as a common baseline that can be used by grid operators when they procure new equipment.

Grid operators throughout Europe are deploying Smart Meters to enable the smart grid. Security is a major success factor in the deployment. Security is needed to protect the private data of citizens and to protect against from cyber-attacks aimed to disrupt the electricity grid, for instance by sending mass switch-off commands.

Secure devices are now available in the market. Smart meter communication standards all have security features. Several manufacturers have implemented these features and are offering secure and well-tested devices.

But procuring secure devices remains challenging for grid operators. Cost is a major concern when deploying hundreds of thousands or millions of smart meters. Even a price increase of a few euro due to security can turn the business case negative.

Public tendering rules moreover require security requirements to be defined up front. Mistakes in them can be costly. Leaving out requirements, setting too strict requirements, or including unclear requirements may lead to unsecure or expensive meters, and can delay the rollout.

This document aims to help grid operators to set procurement requirements. It includes requirements that ENCS has developed for members in Austria, Czech Republic, the Netherlands, and Portugal. The requirements have been used in many different tenders. They are set up to allow independent testing, and more than thirty smart meters have already been successfully tested against them. By using these requirements in their tender process, grid operators can start from a mature requirements set.

Harmonizing requirements between grid operators can moreover lead to major cost saving for all. Vendors get a common baseline to aim at. They only need to implement the security requirements once to qualify for all grid operators that use them.

1.1 Scope

This document gives functional and quality requirements for the security of Smart Meters and Data Concentrators, and gives requirements for secure development processes at the vendor. The requirements are meant for procuring new Smart Meters and Data concentrators. They are not requirements to legacy systems.

The requirements cover secure communication from Smart Meters and Data Concentrators to central systems, such as head-ends. They do not cover the security of the central systems themselves.

1.2 How to use the requirements

The requirements can be used to procure Smart Meters and Data Concentrators (implementing for instance control A.14.1.1 in ISO 27001:2013). The requirements can be included directly in procurement documents. But for the best results, it is recommended that grid operators take the following steps:

1. **Check that the requirements mitigate the security risks.** The requirements are based on risk assessments at several grid operators. But different grid operators face different risks. It is recommended that grid operators perform a risk assessment of their own situation. Based on this assessment, requirements may be added or left out.
2. **Add interoperability requirements where needed.** The requirements are technology-independent. They make no assumptions on the communication technologies used. Grid operators may need to add interoperability requirements to makes sure the procured devices integrate into their larger systems, for instance adding requirements to enable supervision of the meters by a central SIEM (Security Information Events Manager).
3. **Evaluate the devices against the requirements.** The procurement process should include checks, including testing, to assure that the devices procured meet the requirements. It is recommended to have them evaluated by an independent party. Recommendations on how to evaluate are included in the requirements.
4. **Define and implement security processes and procedures.** The requirements only ensure that vendors deliver secure devices. It is up to the grid operators to make sure they are also used securely. Processes and procedures should be set up to for instance configure the devices securely and to manage the keys. These are outside the scope of this document. Grid operators may consider setting up an information security management system to ensure the quality of processes and procedures.

1.3 How to read the Requirements

The component requirements in Section 3 use “device” as a generic term for Smart Meters, Data Concentrators, and Gateways. The requirements apply to all these devices, except for requirement SRR.01.SM, which only applies to Smart Meters.

The product lifecycle and governance requirements in Section 3.8, use the term “Vendor” for the party selling the device, and “Purchaser” for the party buying them. The

assumption is that even if they use subcontractors, the Vendor takes full responsibility for meeting the security requirements, not only for the device, but also for the development, production, and delivery.

Each requirement is labelled with an identifier, such as SFR.01 or SMR.03, and a title, followed by two items:

- **Requirement:** a need that the device or Vendor must perform.
- **Recommended Evaluation:** activities that are recommended for the Purchaser to make sure that the requirement is indeed met.

After these two items, recommendations are sometimes given on implementing the requirement.

For the evaluation, three types of activities can be recommended:

1. **Documentation review:** The Vendor supplies information on the topics listed. The Purchaser evaluates the information against the requirements.
2. **Functional tests:** The Vendor or Purchaser tests if the functionality in the requirement is indeed implemented on the device.
3. **Penetration tests:** The Vendor or Purchaser performs tests that simulate attacker activities to discover vulnerabilities on the device.

Both the Vendor and Purchaser can choose to let some activities be performed by a third party. If the Vendor performs tests, they should share both the test method and results with the Purchaser (see Requirement SDR.05).

2 Security Architecture

The requirements support three architectures, shown in Figure 1, and described further below. The requirements cover the gray-colored components. The requirements concerning secure communications distinguish between the interfaces shown.

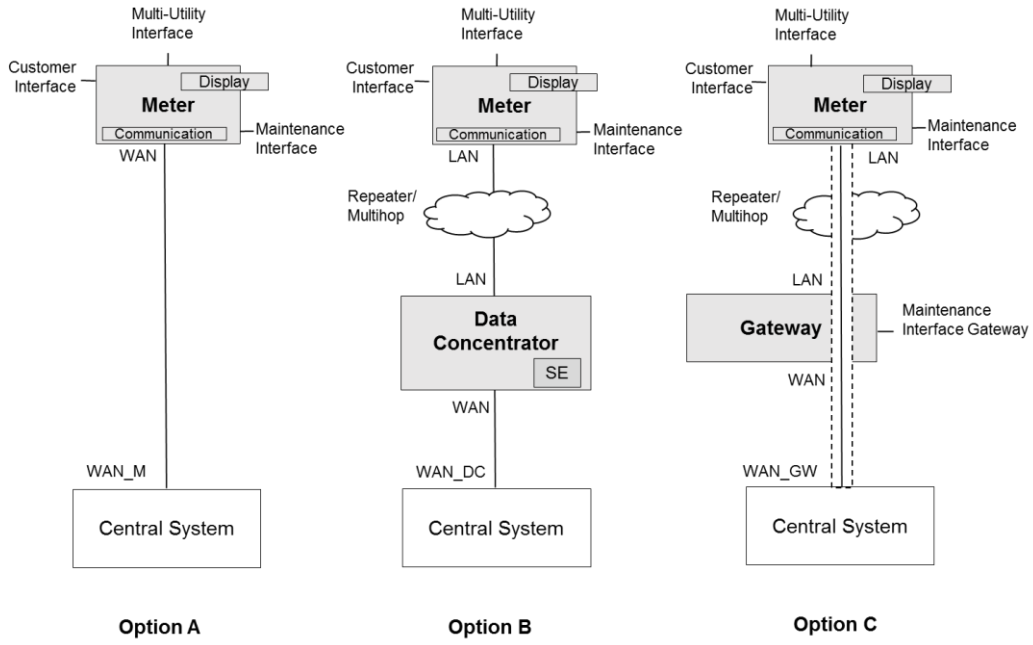

Figure 1: Smart Meter architecture possibilities.

The Local Area Network (LAN) usually uses Power Line Communication (PLC) or wireless mesh technology. The Wide Area Network usually uses a mobile telecommunications network, such as GPRS, CDMA or LTE. This document however does not make any assumptions on the underlying networking technology.

Option A: Directly connected Smart Meter system

In architecture option A, Smart Meters communicate directly with the Head-End System over the WAN. The WAN network is assumed to be maintained by party other than the grid operator. The requirements do not cover this network, but are set up to provide end-to-end security: the Smart Meter and Central System can ensure the integrity and confidentiality of data sent over the WAN, without depending on any network components in the WAN. Of course, availability will depend on the WAN.

In Option A, there is an additional threat that the Central System is compromised from a compromised Smart Meter. The Smart Meter could for instance be used to perform a denial-of-service or remote-code execution attack. Measures should be taken to mitigate this risk, such as performing penetration tests on the Central System from the WAN

interface, or including a secure element on the Smart Meter using the requirements in Section 5.

Option B: Smart Meters and Data Concentrators

In architecture option B, Smart Meters communicate over the LAN with a Data Concentrator. The Data Concentrator collects data from several Smart Meters, and sends it to the Central System over the WAN. The Data Concentrator is maintained by the grid operator.

In Option B, there is an additional threat that keys, credentials, or meter readings are compromised at the Data Concentrator. If a Data Concentrator is compromised, all attached meters are compromised. This could lead to a leak of their private data, manipulation of their meter readings, or even the opening of their breakers.

A Secure Element may be used on the Data Concentrator to mitigate the additional threat. For this reason, requirements for Secure Elements are included in Section 5.

Option C: End-to-End Secure Smart Meter system

In architecture option C, the Data Concentrator is replaced by a Gateway that only passes on data. It does not hold any keys and credentials, and cannot read or modify the data that passes through it.

The requirements for option C are set up so that the communication between Smart Meters and the Central Systems is end-to-end secure. In that sense, option C is like Option A. The difference is that while in Option A all network components are managed by another party, in option C the gateway is managed by the grid operator. Hence, the grid operator must take measures to secure it. Requirements are therefore included for the Gateway.

In Option C, the Gateway cannot be used to compromise Smart Meters. It usually does not require a Secure Element to this risk.

But, as in Option A, there is an additional threat that the Central System is compromised from a comrpomised Smart Meter. Measures should be taken to mitigate this risk, such as performing penetration tests on the Central System from the WAN interface, or including a secure element on the Smart Meter using the requirements in Section 5.

Hybrid Approach: Combine Options B and C

It is possible to combine options B and C: The Data Concentrator can read out measurement data from Smart Meters, but critical commands (such as opening the

breaker, changing keys, or updating the firmware) are sent from the Central Systems to the Smart Meter over and end-to-end secure connection.

Such a hybrid approach can be implemented by separating roles on the Smart Meter. By the requirements in this document, the Smart Meter must allow different roles, and allow different privileges and keys and credentials for each role. The grid operator can define a role for the Data Concentrator that is only allowed read out power measurements. The Data Concentrator then only needs the keys and credentials for this role.

By carefully defining roles and their privileges, the grid operator can reduce the impact that the compromise of a Data Concentrator or meter has, also reducing the need for a Secure Element in smart meters.

2.1 Components and interfaces

This section provides details on the components and their interfaces. A mapping to the CEN-CENELEC-ETSI reference architecture [1] is given in Appendix A.

2.1.1 Smart Meter

The Smart Meter is an electricity meter that can communicate either with the Central Systems through a WAN interface or a Data Concentrator through a LAN interface.

Table 1: Communication interfaces on Smart Meters.

Interface	Description
Display	Physical display on the Smart Meter that shows information to customers. This interface is assumed to be read-only.
Customer interface	Communication port that can send customers information, for instance to use on an in-home display. This interface is assumed to be read-only.
Multi-Utility interface	Optional interface to connect gas, water, or heat meters.
Maintenance interface	Interface that service engineers can use to locally access the Smart Meter, usually an optical port.
LAN interface	Connection to the Gateway or Data Concentrator, usually through a PLC or wireless mesh network.

WAN interface	Connection to the Central System, usually through a mobile telecommunications network (such as GPRS, LTE or CDMA).

If the customer interface supports more advanced use cases, such as the management of DER devices, the risks should be assessed. Additional requirements may be needed on the interface.

2.1.2 Data Concentrator

The Data Concentrator collects and aggregates information from the meters which it sends in batches to the Central System.

Table 2: Communication interfaces on Data Concentrators.

Interface	**Description**
Maintenance interface	Interface that service engineers can use to locally access the Data Concentrator. It can be an Ethernet, serial, or USB port, or combination of these.
LAN interface	Connection to the Smart Meter, usually through a PLC or wireless mesh network.
WAN interface	Connection to the Central System, usually through a mobile telecommunications network (such as GPRS, LTE or CDMA).

2.1.3 Gateway

The Gateway passes information between the Central System and the Smart Meter. A gateway has the same communication interfaces as a Data Concentrator (Table 2).

3 Component Requirements

This section contains the technical requirements applicable to all devices in the systems: Smart Meters, Data Concentrators, and Gateways.

In the requirements below, **security functionality** means any functionality on the device that is needed to implement the requirements in this document.

Application layer data is the payload of any application layer protocol used to transport smart meter data. Application layer data includes at least electricity measurements, timestamps, commands to switch the breakers, configuration changes, and firmware updates.

3.1 Interface Minimization

SMR.01 Minimizing Protocols and Services

Requirements	1. The device shall support only the communication protocols and network services that it needs to meet its functional requirements. 2. The device shall not use services or applications for security functions if there are vulnerabilities known for them.
Recommended Evaluation	Documentation review on the list of protocols and services supported. Penetration tests that include scans to verify that no unneeded protocols or services are supported, and that services and applications contain no known vulnerabilities.

The penetration tests should at least test the devices against vulnerabilities in public databases, such as the Common Vulnerabilities and Exposures (CVE) database.

SMR.02 Minimizing Hardware Ports

Requirements	1. The device shall expose on the outside only the hardware ports that it needs to meet its functional requirements. 2. The device shall have all debug ports on its circuit board (such as JTAG) disabled, so that they cannot be used to read from or write to memory.

Recommended Evaluation	Documentation review on the list of hardware and debug ports. Penetration tests to verify that no debug ports or unneeded hardware ports can be used.

SMR.03 Account Hardening

Requirements	1. The device shall only contain user accounts that it needs to meet its functional requirements.
Recommended Evaluation	Documentation review on the list of accounts supported by the device. Penetration tests that include a scan of all accounts supported.

A public client account is allowed, if it is required by the communication protocols used.

3.2 Cryptographic Algorithms

SPR.01 Cryptographic Algorithms

Requirements	1. The device shall use for security functionality only cryptographic algorithms and parameters that are according to recommended practices and national regulation. 2. The device shall not use proprietary cryptographic algorithms.
Recommended Evaluation	Documentation review on list the cryptographic algorithms and parameters used to implement the security functions. Functional tests to verify that the algorithms are implemented correctly, for instance using the NIST CAVP test suite [2].

Recommended practices can be found in ENISA's Algorithms, Key Sizes and Parameters Report [3], recently updated in the ECRYPT project [4], and in NIST SP 800-57 Part 1 [5]. National guidelines are provided by the BSI in TR-03116, Part 3 [6] and by ANSSI [7].

SPR.02 Cryptographic Random Number Generation

Requirements	1. The device shall only use a cryptographic random number generators from AIS 20 [8], AIS 31 [9], or FIPS 140-2 (Annex

	C) [10] when generating random numbers for security functionality.
Recommended Evaluation	Documentation review on the list of algorithms used for generating cryptographic random numbers. Functional tests to verify that the random data generated by the device does not show any patterns that make it predictable, for instance the NIST SP 800-22 test suite [11].

Random values are used for security functionality for instance when they are used in authentication protocols, or to create digital signatures or cryptographic keys.

3.3 Data Integrity

SIR.01 Message Authenticity

Requirements	1. The device shall cryptographically verify the authenticity of all application layer data it receives on the interfaces below, except for data that cannot be sent authenticated, and has been explicitly accepted as an exception by the Purchaser. 2. If the device cannot verify the authenticity of data, it shall reject or drop it. 3. The device shall authenticate all application layer data it sends on the interfaces below, except for data for which authentication is not possible, and which has been explicitly accepted as an exception by the Purchaser.
Interfaces Smart Meters	For a smart meter, this requirement applies to the interfaces: • LAN (C) between electricity meter and Data Concentrator or Gateway, • WAN (G1) between electricity meter and Central System, • Maintenance interface, • Multi-utility interface (M) between electricity meter and other utility meters.
Interfaces Data Concentrators	For Data Concentrators, this requirement applies to the interfaces: • WAN (G2) interface to the Central System, • LAN (C) interface to the meter,

	• Maintenance interface.
Interfaces Data Concentrators	For Gateways, this requirement applies to the interfaces: • WAN (G2) interface to the Central System if the message is addressed to the gateway (not the meter), • Maintenance interface.
Recommended Evaluation	Documentation review on measures for message authenticity. Functional tests to verify that the message authentication measures are implemented correctly, and that it is not possible to bypass these measures by downgrading to weaker security settings.

The requirement is usually implemented by verifying a message authentication code (MAC) of each received message, and attaching a MAC to each sent message. For DLMS, this can be done by setting the transport security policy for all clients except the public client to require authentication.

DLMS does not allow authentication for the public client, for message headers, and for parts of the AARQ, AARE, RLRQ, and RLRE messages. Not authenticating this data would normally be an acceptable exception.

The requirement allows message headers or messages without an application layer payload to be unauthenticated.

Data Concentrators may use TLS or a VPN connection to protect message authenticity.

SIR.02 Input Validation

Requirements	1. The device shall apply input validation to all data it receives.
Recommended Evaluation	Penetration tests, which include fuzzing tests to see how the device reacts to malformed messages.

The requirement applies to all layers in the OSI model.

SIR.03 Firmware Signing

Requirements	1. The device shall verify the digital signature of a firmware update (see SDR.03) before applying it.

	2. The device shall reject the firmware if it detects it has been modified, or if it cannot verify the digital signature. 3. The device shall reject the firmware if its version number is lower than that of the currently installed firmware.
Recommended Evaluation	Documentation review on the firmware update process, and the algorithms used for firmware signing. Functional tests to verify that firmware with a valid signature and a higher version number is installed, and firmware with an invalid signature or lower version number is rejected.

The Vendor must follow the guidelines in SPR.01 when implementing digital signatures.

Digitally signed firmware updates can be broadcasted to a group of meters, so that less bandwidth is used. This is useful in powerline communication networks.

The device can still support the downgrade to an older firmware version, if the firmware is sent with a new version number.

SIR.04 Replay Protection

Requirements	1. The device shall detect and reject replayed application layer messages for all messages for which it checks the authenticity (see SIR.01).
Recommended Evaluation	Documentation review on the replay protection measures. Functional tests to verify that the device detects and rejects replayed messages.

The requirement is usually implemented by using a counter that increases for each message (such as the frame counter for DLMS). It is important that no two messages encrypted with the same key, and sent in the same direction have the same counter. So, if the device does not use session keys, the counter must be increased between sessions.

3.4 Confidentiality

SCR.01 Message Confidentiality

Requirements	1. The device shall encrypt all application layer data that it sends on the interfaces below, except for data that cannot be sent encrypted, and has been explicitly accepted as an exception by the Purchaser. 2. The device shall enforce that all application layer data that it receives on the interface below is encrypted, except for data that cannot be sent encrypted, and has been explicitly accepted as an exception by the Purchaser.
Interfaces Smart Meters	For a smart meter, this requirement applies to the interfaces: • LAN (C) between electricity meter and Data Concentrator or Gateway, • WAN (G1) between electricity meter and Central System, • Multi-utility interface (M) between electricity meter and other utility meters.
Interfaces Data Concentrators	For Data Concentrators, this requirement applies to the interfaces: • WAN (G2) interface to the Central System, • LAN (C) interface to the meter, • Maintenance interface.
Interfaces Gateways	For Gateways, this requirement applies to the interfaces: • WAN (G2) interface to the Central System if the message is addressed to the gateway (not the meter), • Maintenance interface.
Recommended Evaluation	Documentation review on the measures for encryption. Functional tests to verify that the encryption measures are implemented correctly, and that it is not possible to bypass these measures by downgrading to weaker security modes defined for the communication protocols used.

For DLMS, this requirement can be fulfilled by setting the transport security policy for all clients expect the public client to require encryption. DLMS does not allow authentication

for the public client, for message headers, and for parts of the AARQ, AARE, RLRQ, and RLRE messages. Not authenticating this data would normally be an acceptable exception.

Data Concentrators may use TLS or a VPN connection to protect confidentiality.

If data that should be encrypted is not encrypted the device should drop or reject it.

3.5 Resilience

SRR.01.SM Separation of Measurement from Communication

Requirements	1. The Smart Meter shall separate measurement functionality from communication functionality, so that it keeps measuring electricity correctly under denial-of-service attacks.
Recommended Evaluation	Documentation review on the measures to separate measurement from communication. Penetration tests that include testing if the device keeps measuring electricity when it is flooded with messages, or when it receives malformed messages.

This requirement only applies to Smart Meters, not Data Concentrators or Gateways, as these normally do not have measurement functionality.

SRR.02 Fail-Secure Operation

Requirements	1. The device shall not disclose confidential information, such as keys or credentials, during a failure. 2. The device shall protect the integrity of security critical data during failures. 3. The device shall not allow access controls to be bypassed remotely during failures. 4. The device shall restore availability after software failures as soon as possible.
Recommended Evaluation	Documentation review on a specification of how the device behaves under the following failures: • Voltage drops

	• Integrity errors of configurations files; • Failures during execution of cryptographic functions; • Failures during validation of login credentials; • Failures when entering data (wrong data format, wrong data length, invalid commands etc.); Functional tests to verify that the device behaves as specified.

SRR.03 Tamper Detection

Requirements	1. The device shall be protected against physical manipulation, so that attackers without specialist tools cannot reach its internals without leaving clearly visible traces. 2. The device shall create a log event whenever any part of its cover is opened.
Recommended Evaluation	Penetration tests that include physical tests in which the penetration tester tries to reach the device internals without leaving traces. Functional tests to verify that the device creates a log event when the cover is opened.

Grid operators could restrict the requirement to Smart Meters and exclude data concentrators. Since the requirement creates extra costs, grid operators should include it only when a risk assessment show that the risks of physical attacks are not acceptable otherwise. These risks depend on the country and grid operator.

Grid operators should also consider the risk that devices are tampered with during a power outage. Additional requirements may be needed to mitigate this risk.

Specialist tools are any tools that are out of reach for threat actors interested in fraud. Such actors are assumed to have access to any commercially available tools that can be purchase for a few hundred or few thousand euros. They are not assumed to have access to more expensive industrial or scientific equipment.

3.6 Access Control

SAR.01 Separation of Roles

Requirements	1. The device shall support separating roles by having different accounts for each role. 2. The device shall allow to assign each role individual credentials or keys, so that it is not possible for on role to authenticate as another role or to eavesdrop on the communication of another role. 3. The device shall allow to bind roles to interfaces. 4. The device shall prevent privilege escalation attacks.
Recommended Evaluation	Documentation review on the implementation of roles.

Adding roles may be done through firmware updates. For the DLMS protocol, different roles can be implemented as different clients.

In point 2, public client roles are excluded.

SAR.02 User Authentication

Requirements	1. The device shall identify users' roles. 2. The device shall authenticate user's roles, except when they identify as a public client.
Recommended Evaluation	Documentation review on the user authentication measures. Functional tests to verify the measures are implemented correctly.

Users in this requirement can be either human users or communication processes. As in SAR.01, different roles can be implemented as different clients.

SAR.03 Authorization

Requirements	1. The device shall allow to set access control authorizations per role.

	2. The device shall enforce these authorizations.
Recommended Evaluation	Documentation review on the user authorization measures. Functional tests to verify the measures are implemented correctly.

For the DLMS protocol, this requirement can be implemented by allowing the access rights of each attribute and method to be set per client. Changing the authorizations may be done through firmware updates.

3.7 Audits and Logs

SLR.01 Security and Audit Events

Requirements

1. The device shall store in a local log the following security events:
    a) Failed authentication attempts
    b) Failed firmware updates
    c) Changing the system time
    d) Opening the cover (see SRR.03)
    e) Booting the device
    f) Shutting down the device
    g) Failed attempt to change keys or credentials
    h) Attempted replay attacks
    i) Failures in message authenticity verification
2. The device shall store in a local log the following audit events:
    a) Successful authentications
    b) Firmware uploads
    c) Successful firmware updates
    d) Resetting alarm or error registers
    e) Changing keys or credentials
3. The device shall log for each security and audit event:
    a) A timestamp
    b) The event type
4. The device shall allow the log files to be read out remotely.

Recommended Evaluation	Documentation review on the list of security event logged. Functional tests to verify that the events are indeed logged.

Monitoring the security and audit events is key to keeping the smart metering system secure. It is recommended to collect the events centrally for analysis. They can be collected for instance in a log management or Security Information and Event Management (SIEM) system. Additional interoperability requirements may be needed on top of SLR.01.4 to ensure easy collection. Use cases should be defined based on risks to detect security incidents.

Besides the required events, it is recommended to log

1. Attempts to perform unauthorized operations
2. Detection of replayed messages
3. Detection of messages with an invalid authentication tag

Furthermore, it is recommended to log for each event also:

- the user that caused the event causing the event
- the interface on which the event occurred

It is recommended to restrict write access to logs to roles with a security responsibility, such as a maintenance role or a specialized security officer role. The device should allow such restrictions by requirement SAR.03.

SLR.02 Storage Space for Security Events

Requirements	1. The device shall store the latest 100 security and audit events. 2. The device shall not allow audit events to be flushed out by generating many security events.
Recommended Evaluation	Documentation review on the log storage capacity. Functional tests to verify that the device stores 100 security events.

The most straightforward way to ensure that 100 security events can be stored is to have a dedicated security log with space for at least 100 events. If another approach is chosen, the Vendor should show that this approach meets the requirement.

Security events can easily be generated even without keys or credentials, for instance by creating failed login attempts. In this way, it would be possible to mask configuration changes to the device, logged as audit events. This can be prevented for instance by

keeping counters for the number of events per period, or by using separate logs for security and audit events.

3.8 Future Proof Design

SFR.01 Remote Updates

Requirements	1. The device shall allow remote updates for all security functionality for which updates are expected to be needed. In particular, the device shall allow to remotely: a) Update all cryptographic algorithms and protocols (see SPR.01) b) Update the cryptographic random number generator (see SPR.02) c) Add more roles (see SAR.01) d) Change the authorization of roles (see SAR.03) e) Add new security events (see SLR.01)
Recommended Evaluation	Documentation review on the remote update method.

The device may update the functionality through remote firmware updates. To allow updates of cryptographic algorithms and protocols it may be required that the communication protocols used allow to negotiate the protocol version or cryptographic settings used.

SFR.02 Future-Proof Design

Requirements	1. The device shall have sufficient memory (RAM and flash) and computation power to allow the updates in SFR.01 that are needed in the device's lifetime, under the following assumptions: a) Cryptographic algorithms and key sizes are updated following national and international security standards, and the protocol standards used during the lifetime of the devices

	b) Roles and event types will grow incrementally (not more that 50% more than used initially)
Recommended Evaluation	Documentation review on the following topics: • Test results that show the available and used memory of the device under current operational workloads • Test results that show the performance of cryptographic algorithms that are: a) defined in international standards, b) expected to be needed during the device's lifetime according to applicable national or international standards, and c) used in the communication protocols or firmware update process of the device. • Memory expected to be needed for future security functionality under the assumptions in the requirements

DLMS meters are expected to be updated to implement DLMS security suites 1 and 2.

Grid operators can specify the cryptographic standards they follow in the requirement to make it more concrete.

The vendor needs to provide the test results needed for the documentation review.

SFR.03 Key and Credential Updates

Requirements	1. The device shall allow all credentials and keys used for security functionality to be changed remotely.
Recommended Evaluation	Documentation review on the key and credential update methods. Functional tests of the key and credential update methods.

4 Product Lifecycle and Governance

This section contains measures that the Vendors should take to secure the development, production, and delivery of the devices.

SDR.01 Vendor ISMS

Requirements	1. The Vendor shall implement an information security management system (ISMS) whose scope includes the development, manufacturing, and provisioning of the device and related software and tools.

Related software and tools are for instance maintenance software and hand-held terminals.

It is recommended to follow the ISO 27001 standards in implementing the ISMS.

SDR.02 Configuration Management

Requirements	1. The Vendor shall use a configuration management system. 2. The Vendor shall identify the author of each change made. 3. The Vendor shall ensure that third-party suppliers of security-relevant functions and products implement comparable processes.

The configuration management should keep track of hardware configurations, source code and firmware, and customer-specific configuration of devices.

SDR.03 Secured Versioning

Requirements	1. The Vendor shall identify each firmware or hardware release with a unique version number. 2. The Vendor shall be able during the product lifecycle to reproduce each release based on the version number. 3. The Vendor shall digitally sign each firmware release.

SDR.04 Vulnerability Management

Requirements	1. The Vendor shall have a documented process to handle vulnerabilities. 2. The Vendor shall monitor information sources on vulnerabilities to determine if it has been affected. 3. The Vendor shall handle vulnerabilities found by themselves, the Purchaser or system integrator, or external security researchers. 4. The Vendor shall notify the Purchaser about any vulnerabilities found as soon as possible.

The vulnerability management process should at least address how the Vendor identifies vulnerabilities, how it prioritizes fixing them, and how it communicates them to the Purchaser.

SDR.05 Security Testing

Requirements	1. The Vendor shall perform tests on each firmware release to verify that all the security requirements in this document have been implemented fully and correctly. 2. The Vendor shall share the test method and results with the Purchaser.

Guidance on the test activities to performed is given in the evaluation recommendations for each requirement.

SDR.06 Production Security and Credential Provisioning

Requirements	1. The Vendor shall securely install the initial keys and credentials on the device. 2. The Vendor shall securely hand over the initial credentials to the grid operator.

To determine what ‘securely’ means in this requirement the Vendor is expected to use the risk management process that is part of the ISMS required by SDR.01. Security measures that should be considered are creating a secure area for installing the initial keys and credentials, and using a secure communication channel to send these to the Purchaser.

5 Requirements for Secure Elements

This section contains requirements for Secure Elements that can protect a device against physical attacks. A Secure Element can be used if a risk assessment shows that the risks of physical attacks are too high, especially for Data Concentrators in architecture option B (see Section 2).

SER.01 Secure Element

Requirements	1. The Secure Element shall be certified by a recognized certification scheme.
Recommended Evaluation	Documentation review on the certificate and the evaluation report from the certification.

Examples of recognized security certification schemes are Common Criteria.

SER.02 Cryptographic Operations

Requirements	1. The Secure Element shall be used to perform all cryptographic operations on the device.
Recommended Evaluation	Documentation review on the functionality of the secure element, and how it is used in the device.

Cryptographic operations that must be done on the secure element include:

- Encrypting data
- Generating and verifying message authentication codes
- Generating and verifying digital signatures
- Generating new keys, including session keys
- Calculating hash values
- Generating cryptographic random numbers

SER.03 Secure Boot Process

Requirements	1. The Secure Element shall ensure a secure boot process of the device that verifies the digital signature of the firmware, and the integrity of all configuration data during boot time.

Recommended Evaluation	Documentation review on the secure boot process. Penetration tests in which testers try to bypass the secure boot process.

SER.04 Encryption of Stored Data

Requirements	1. The secure element shall be used to encrypt all data stored in persistent memory, in such a way that the encryption key never leaves the secure element.
Recommended Evaluation	Documentation review on the secure boot process. Penetration tests in which testers analyze the contents of the device's persistent memory.

Appendix A: Mapping to M/441 Architecture

Following mandate M/441 by the European Commission issued in 2009, the standardization organizations CEN, CENELEC and ETSI issued a reference architecture for smart metering [1] as shown in Figure 2. This paragraph describes the mapping between the smart metering architecture described in this document and the M/441 reference architecture.

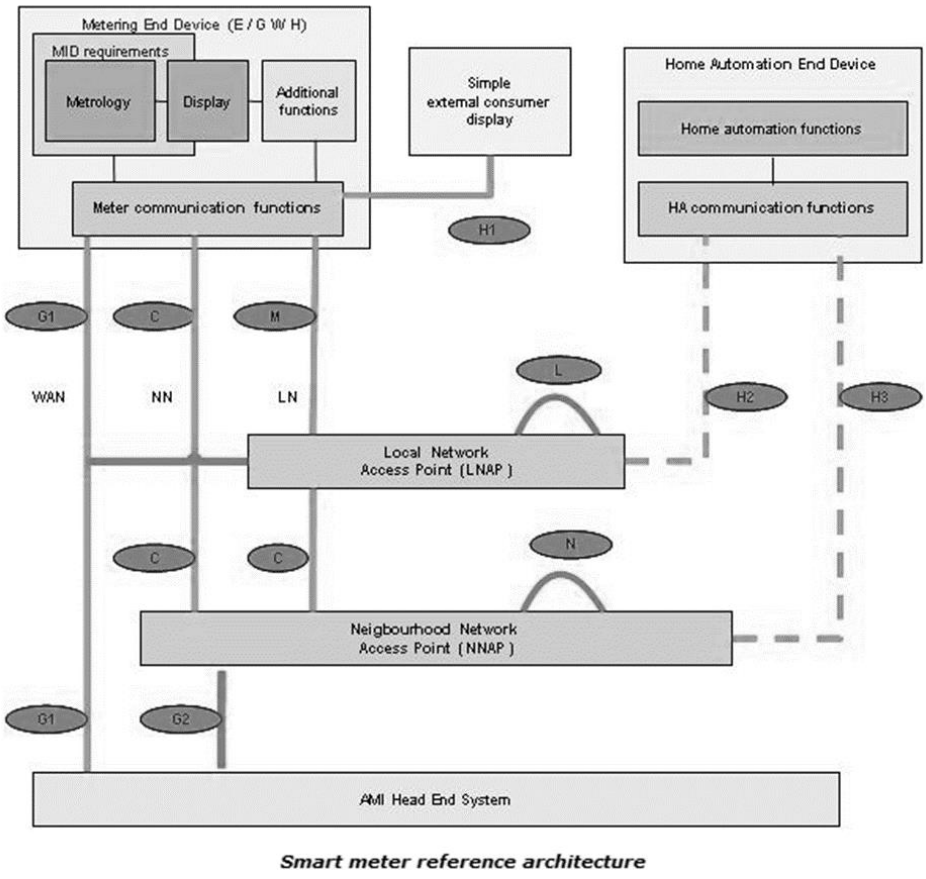

Figure 2: M/441 Reference architecture diagram for smart metering communications.

The communication networks described in the M/441 reference architecture map as follows to the architecture in this document:

Table 3: Mapping of communication networks in M/441 reference architecture

Communication Networks in M/441	Access points of communication networks in M/441	Part of the reference architecture in this document	Comment
WAN	---	Yes	The Wide Area Network connecting meters, data concentrators, and Gateways to the Central System.
NN	NNAP	Yes	The Neighborhood Network (NN) is the segment connecting up to 100 homes in a segment to a data concentrator or Gateway.
LN	LNAP	No	A local network (LN) within the same premises such as local home area network is out of scope.

The interfaces described in the M/441 reference architecture map as follows to the interfaces described in Chapter 2.2 in this document:

Table 4: Mapping of interfaces to M/441 reference architecture.

Interfaces in M/441 CEN-CENELEC-ETSI Reference Architecture	Corresponding interface in this document	Comment
G1	Meter WAN	As in Chapter 2.2
G2	DC/Gateway WAN	As in Chapter 2.2
C	Meter LAN, DC LAN, Gateway LAN	As in Chapter 2.2

M	Multi-Utility Interface	The Metering end device interface (M interface) can be defined with different profiles according to CEN-CENELEC-ETSI. The M interface connects to a metering end device such as a gas/water/heat meter.
H1	Customer Interface	As in Chapter 2.2
H2	---	The LN is out of scope and thus no corresponding interfaces are defined in this document.
L	---	The LN is out of scope and thus no corresponding interfaces are defined in this document.
N	---	The LN is out of scope and thus no corresponding interfaces are defined in this document.
I	---	While the document demands the separation of functional blocks it does not explicitly define meter-internal interfaces.
Not defined	Maintenance Interface	Optical port.

References

[1] CEN, CENELEC, and ETSI, "Functional reference architecture for communications in smart metering systems. Technical Report 50572," 2011.

[2] National Institute for Standards and Technology (NIST), "Cryptographic Algorithm Validation Program," [Online]. Available: http://crsc.nist.gov/groups/STM/cavp/. [Accessed 28 1 2017].

[3] ENISA, "Algorithms, Key Sizes and Parameters Report, 2013 recommendations, version 1.0," 2013.

[4] ECRYPT-CSA, "Algorithms, Key Size and Protocols Report," 2018.

[5] National Institute for Sandards and Technology (NIST), "Special Publication 800-57 Part 1 Rev. 3: Recommendation for Key Management," 2012.

[6] Budensambt für Sicherheit in der Informationsechnik (BSI), "TR-03116, Part 3: Kryptographische Vorgaben für Projekte der Bundesregierung - Intelligente Messsysteme," 2014 (adapted anually).

[7] ANSSI, "Mécanismes cryptographiques - Règles et recommandations, Rev 2.03," 2014.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Andwendungsweise und Interpretationen zum Schema AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für determinischtische Zufallszahlengeneratoren," 2013.

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Andwendungshinweise und Interprtationen zum Schema AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallsgeneratoren, Version 3.0," 2013.

[10] National Institute of Standards and Technology (NIST), "FIPS PUB 140-2, Annex C: Approved Random Number Generators for FIPS PUB 140-2," 2012.

[11] National Institute of Standards and Technology (NIST), "Special Publication 800-22, Revision 1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," 2012.