SM-301-2019

Security requirements for procuring smart meters

Version 2.6

30 December 2019

This document was produced in the ENCS program on Security Architectures. This program support ENCS members in selecting and implementing technical security measures for systems and their components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

Smart metering	DA-301-2019: Security requirements for procuring smart meters and data concentrators
Distribution automation	DA-101-2019: Security risk assessment for distribution automation systems DA-201-2019: Security architecture for distribution automation systems DA-301-2019: Security requirements for procuring distribution automation RTUs DA-390-2019: Market survey on distribution automation RTU security DA-401-2019: Security test plan for distribution automation RTUs
Substation automation	DA-101-2019: Security risk assessment for substation automation systems DA-201-2019: Security architecture for substation automation systems DA-301-2019: Security requirements for procuring substation gateways DA-302-2019: Security requirements for procuring IEDs DA-303-2019: Security requirements for procuring HMI software
Electric vehicles	EV-101-2019: Security risk assessment for EC charging infrastructure EV-201-2019: Security architecture for EV charging infrastructure EV-301-2019: Security requirements for procuring EV charging stations EV-401-2019: Security test plan for EV charging stations

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

Version History

Date	Version	Description
16 February 2015	1.0	Initial release to members
8 October 2018	2.0	Updated version based on testing experiences since release 1.0
22 July 2019	2.3	Version updated with feedback from EDSO cyber-security task force
9 September 2019	2.4	Updated version for ENCS member project on procuring secure equipment
11 November 2019	2.5	Updated version after ENCS internal review
30 December 2019	2.6	Final version in member project on procuring secure equipment

ENCS

Table of Contents

1 Introduction

This document contains security requirements for procuring smart meters. The requirements can be used directly in procurement documents. 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 increase the efficiency of the smart grid processes and allow the implementation of new use cases such as, load balancing related). Security is a major success factor in this process to protect the private data of citizens and to protect against cyber-attacks aimed to disrupt the electricity grid, for instance by sending mass switch-off commands.

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

Yet, procuring secure devices remains a challenge for grid operators. Cost is a major concern when deploying hundreds of thousands or even millions of smart meters. Even a price increase of a few euros due to new security features can turn the business case negative. Moreover, public tendering rules require security requirements to be defined up front. Mistakes in them can be costly: incomplete, unclear or too strict requirements may lead to insecure or expensive meters, which 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 a 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 gives requirements for secure development processes at the vendor. A separate set of requirements is available for procuring data concentrators [1].

The requirements cover secure communication from the smart meters to the data concentrators or central system (see Figure 1). They do not cover the security of the central systems themselves.

The measures cover the following sections from ISO/IEC 27001:2013 Annex A:

- Access control (A.9)
- Cryptography (A.1)
- Physical and environmental security (A.11)
- Operations security (A.12)
- Communication security (A.13)
- System acquisition, development and maintenance (A.14)
- Supplier relationships (A15)
- Information security aspects of business continuity (A.17)

The requirements are meant for procuring new smart meters, not for legacy systems, although grid operator may analyze which systems can be upgraded to meet them.

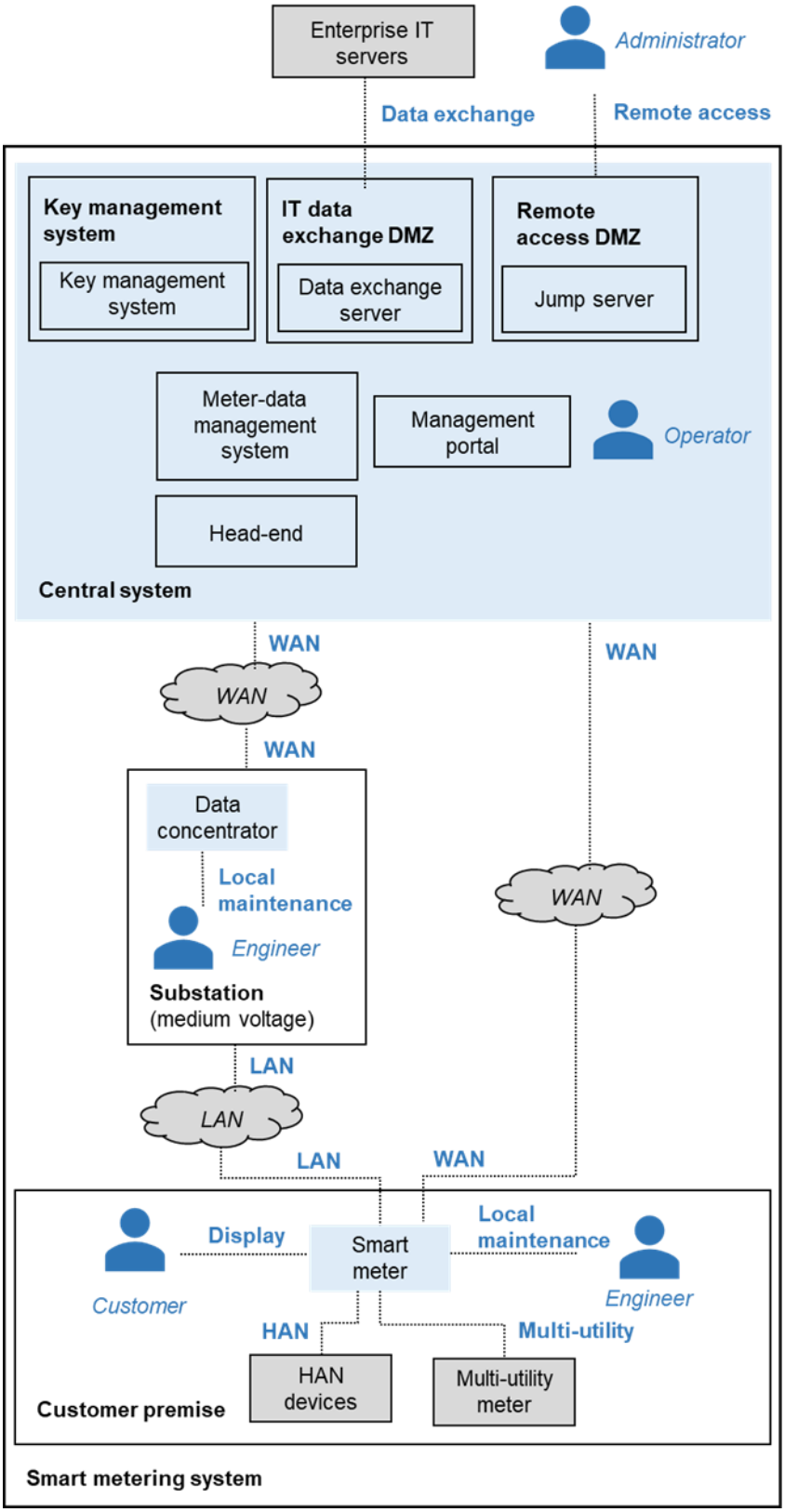

Figure 1: Reference architecture for the smart metering system, showing its users and interface.

Using the requirements

The security requirements are part of a larger approach to creating secure systems, both when building new systems or updating existing systems. It consists of the following steps:

1. Perform a **security risk assessment** to understand the threats to the system and the impact these can have. A risk assessment for a typical smart metering system is available in [2].
2. Design a **security architecture** that selects technical security measures to mitigate the risks. Measures are chosen for the whole system, as this is usually more effective than choosing measures per component. The architecture can act as a blueprint for system integrators and the departments maintain the system. A recommended security architecture for smart metering systems is available in [3].
3. Derive **security requirements for components** from the security architecture that can be used to develop or procure the components. This document gives security requirements for smart meters. Requirements for data concentrators are available in [1].
4. **Test the components** to check that they meet the security requirements. In a procurement process, such tests should be part of the selection phase. Test plans are available for smart meters [4] and data concentrators [5].
5. **Test the system** once it is deployed to check that it is implemented according to the architecture and mitigates the risks. The device and network configuration can be checked using a technical audit. Mitigation of the risks can be checked using penetration and red team tests simulating the threats.

These steps ensure that a secure system is delivered. But after that it still needs to be operated securely. Processes and procedures should be set up to for instance securely maintain the system, manage keys and passwords, and respond to incidents.

To ensure the quality of the processes and procedures, it is recommended to use an information security management system, for instance based on the ISO/IEC 27001 [6]. To support this, the architecture is organized by the security objectives in ISO/IEC 27001 [6] Annex A.

2 Access control

Access control requirements concern how access rights are managed, and how strong their authentication needs to be for different user groups. The smart meter enforces access control for the user groups in Table 1. Both human users and other systems accessing the charging station are considered users.

Table 1: User groups on the smart meter.

User	Required access	Interface
Engineers	• Installation • Maintenance • Testing and calibration • Firmware updates	Local maintenance
Central system or data concentrator	• Reading out meter readings • Maintenance • Firmware updates	WAN or LAN
Customer	• Reading out meter readings	Customer
Multi-utility meters (gas, water, heat)	• Send meter readings	Multi-utility interface
Load controlled devices	• Load control, by getting current electricity usage or tariffs, or through switching commands	Load control interface

2.1 User access management [A.9.2]

The smart meter enforces access rights in such a way that the grid operator can implement the principle of least privileges. For engineers and the central system or data concentrator, roles are separated. Customers have read-only access.

AC12-SM: Least privileges with separate roles for engineers, the central system, and data concentrators

The smart meter shall restrict the access privileges of the engineers, the central system, and data concentrator, so that they can access only the functions and data they need. The smart meter shall separate different roles by:

- having different accounts for each role;
- having unique passwords and keys per role;
- identifying and authenticating a user's role when they log in;
- enforcing the access rights of the role.

Remark: There are no requirements on how the privileges are managed. They may be static and only be changeable through software updates.

Full role-based access control can be implemented through the central system for operators and for engineers through the workforce management system.

For the DLMS protocol, different roles can be implemented as different clients. The DLMS public client is excluded from the requirement for unique passwords or keys.

AC13-SM: Least privileges for multi-utility meters and load controlled devices

The smart meter shall restrict the access privileges of multi-utility meters and load controlled devices, so that they can access only the functions and data they need.

AC14-SM: Read-only access for customers

The smart meter shall enforce that customers have read-only access.

2.2 System and application access control [A.9.3]

The smart meter uses machine-to-machine authentication for all users except customers.

AC15-SM: Machine-to-machine authentication for all users, except customers

The smart meter shall support mutual authentication with passwords or keys for all users except customers.

Remark: No authentication is required for customers, as they have read-only access from within their own house.

3 Cryptography

The smart meter uses cryptography for several functions:

- Machine-to-machine authentication for various users (Section 2.2);
- Digitally signing the firmware (Section 5.3);
- Protecting the confidentiality and integrity of communication (Section 6).

Measures need to be taken to make these cryptographic techniques effective.

3.1 Cryptographic controls [A.10.1]

The smart meter uses strong cryptographic keys and algorithms to protect against attacks on the cryptography itself. The smart meter supports remote keys updates from the central systems to allow keys to be updated on thousands of smart meters.

CR1-SM: Strong cryptographic keys and algorithms

For security functions, the smart meter shall use cryptography according to regulations and modern guidelines without any modifications:

- It only uses the cryptographic algorithms that the ECRYPT – Algorithms, Key Size, and Protocols Report [7] recommends as suitable for new or future systems;
- It uses keys at least as long as the ECRYPT report recommends for near term use (section 4.6 in [7]);
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [7] Section 3.2.3 to generate random numbers for security functions;
- If it uses certificates for authentication, it validates them by checking the signature, the certificate-chain, the revocation status, and the identity of the user or role through the subject name, common name or distinguished name.

CR2-SM: Automated key management

The smart meter shall support automated key management by.

- being delivered with unique initial keys installed during manufacturing;
- allowing all keys to be updated in such a way that their confidentiality and integrity is cryptographically protected during transport.

If asymmetric cryptography is used to protect communication, the smart meter shall be able to use certificates given out by the grid operator’s public key infrastructure (PKI).

The smart meter shall support remotely changing all passwords in a way that protects their confidentiality and integrity.

Remarks: It is allowed that some passwords or keys used for internal purposes cannot be updated remotely. But as soon as they are used to implement any of the requirements in this document, the requirement applies.

The public key or certificate used to verify firmware signatures may come from an external PKI used by the vendor. It is not required that the smart meter can use certificates from the grid operator's PKI for this purpose.

4 Physical and environmental security

4.1 Equipment [A.11.2]

The smart meter is protected against tampering by its cover to counter fraud.

PH5-SM: Tamper detection

The smart meter shall allow physical tampering to be detected by:

- having a cover that protects against physical manipulation, so that attackers without specialist tools cannot reach its internals without leaving visible traces;
- creating a log event and sending an alert whenever any part of its cover is opened.

5 Operations security

The smart meter shall support the operational processes and procedures needed to keep it secure throughout its lifetime.

5.1 Operational procedures and responsibilities [A.12.1]

To support capacity management, the smart meter needs to have enough computing reserves for future updates.

OP1-SM: Future-proof design

The smart meter shall have enough memory (RAM and flash) and computation power to allow security updates needed during its lifetime, under the following assumptions:

- cryptographic measures are updated following the standards in CR1-SM, in particular the smart meter supports the key sizes recommended for long term use in Section 4.6 of the ECRYPT report [7];
- roles and security event types will grow incrementally up to 50%.

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

Compliance to the requirement can be shown through performance tests. Tests with current firmware under operational workloads should show that there are enough reserves to extend security functions. Tests with algorithms and key sizes recommended for long-term use in [7] should show that the smart meter can run them without affecting operations.

5.2 Logging and monitoring [A.12.4]

To detect and respond to security incidents, the smart meter needs to log relevant security events and allow them to be gathered for analysis. As the logs are important to security, they also need to be protected themselves.

OP5-SM: Security events

The smart meter shall be able to log security events for the following in a local log:

1. Firmware updates
2. Failed authentication attempts
3. Changing the system time
4. Booting the device
5. Changing the security log

6. Changing security parameters
7. Memory exhaustion
8. Attempted replay attacks
9. Attempts to physically tamper with the device
10. Invalid firmware signatures
11. Invalid certificates

The log entries for security events shall include a timestamp, an event description, and the role causing the event.

OP6-SM: Collecting security events

The smart meter shall allow security logs to be read out locally using the normal maintenance tools, and remotely by the central system or data concentrator.

The smart meter shall provide the capability to create timestamps that are synchronized with a system wide time source.

Remarks: 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. Use cases should be defined based on risks to detect security incidents.

OP7-SM: Protecting security logs

The smart meter shall protect security logs by:

- restricting access to authorized users;
- having enough storage capacity to store the security logs;
- implementing a rolling security log, in which the oldest entries are discarded first if log storage is full.

5.3 Control of operational software [A.12.5]

The smart meter implements an efficient update process, so that it can be kept fully patched. The authenticity of firmware is verified using a digital signature.

OP9-SM: Remote firmware updates

The smart meter shall allow remote updates from the central system for all security functionality for which updates are expected to be needed. In particular, the device shall allow to remotely:

- update all cryptographic algorithms and protocols (see CR1-SM);
- update the cryptographic random number generator (see CR1-SM);

- add more roles (AC13-SM);
- change the authorization of roles (see AC13-SM).

OP10-SM: Verification of firmware signatures before installation

The smart meter shall be able to verify the integrity and source of firmware updates before installing the firmware using digital signatures.

5.4 Technical vulnerability management [A.12.6]

Besides through security patches (Section 5.3), technical vulnerabilities are managed through hardening, avoiding known vulnerabilities, and applying input validation vulnerabilities.

OP11-SM: Hardening

The smart meter shall support hardening by disabling unneeded functions, in particular, the smart meter shall be delivered with:

- unused user accounts removed;
- unused network services disabled;
- unused communication protocols disabled;
- unused hardware interfaces disabled;
- debug ports on its circuit board (such as JTAG) disabled.

OP12-SM: Known vulnerabilities

The smart meter shall only use applications, libraries and communication protocols without known security vulnerabilities.

OP13-SM: Input validation

The smart meter shall apply input validation to all data it receives.

Remarks: The smart meter developer should make sure their code checks the validity of all received data They should regularly check that there are no input validations vulnerabilities in third-party libraries and applications. They should use code reviews and robustness tests for code they develop in-house, such as domain-specific protocols such as DLMS.

6 Communication security

6.1 Network security management [A.13.1]

The smart meter cryptographically protects communication confidentiality and on untrusted networks. The smart meter needs to be protected against denial-of-service attacks, as they can be reached directly from untrusted networks.

CM1-SM: Cryptographic protection of communication confidentiality and integrity

The smart meter shall be able to use cryptographic measures to protect the integrity and confidentiality of communication on the LAN and WAN interfaces. The measures allow to verify the source of messages and protect against replay attacks.

CM2-SM: Cryptographic protection of wireless communication on customer premises

The smart meter shall be able to cryptographically protect the integrity and confidentiality of wireless communication on customer premises on the HAN, multi-utility, and local maintenance interfaces.

CM7-SM: Resilience against denial-of-service attacks

The smart meter shall be resilient against denial-of-service attacks: it does not become unavailable for long times when network interfaces are flooded with data, or when malformed messages are sent on network interfaces.

Remarks: The smart may become slower when flooded or when dealing with malformed packets. But it should not crash or reboot so that it is not reachable for a longer time.

7 System acquisition, development and maintenance

7.1 Security in development and support processes [A.14.2]

The developer should integrate security throughout their development process to ensure that secure firmware is delivered. They should set up secure programming practices and test each firmware release themselves. They should allow the grid operator to verify the security by acceptance testing and provide guidelines on secure configuration and operation. If vulnerabilities are found during the lifecycle of the smart meter, they should provide security updates.

SD1-SM: Secure programming practices

The developer shall set up programming practices to ensure the consistent delivery of secure smart meter. The vendor shall:

- Define secure coding guidelines;
- Provide security training to developers;
- Set up internal code reviews;
- Use an issue tracker to follow the vulnerabilities and other security issues;
- Implement a version control system;
- Enable compiler options to harden binaries as much as possible.

Remark: Examples of secure coding guidelines are the SEI CERT coding standards [10], available for different languages, and the MISRA C software development guidelines for embedded systems [11].

SD2-SM: Security testing during development

The developer shall test each firmware release to check the implementation of the requirements in this document. Testing shall at least include:

- functional testing for all functional requirements;
- robustness testing of custom protocol implementations.

Remark: The test plan for smart meters [4] includes a list of test cases that vendors can use to check the implementation of the requirements.

SD3-SM: Support for independent testing

The developer shall support testing by the grid operator or an independent party by:

- allowing the grid operator or a third party to audit the development process;
- providing documentation on how the requirements have been implemented;
- making available smart meters for testing;
- providing all keys and credentials needed for testing;
- providing access to source code for code reviews.

Remark: The developer may require a non-disclosure agreement when providing sensitive information, if it does not prevent proper testing.

The vendor may additionally provide a test certificate from a third-party laboratory.

SD4-SM: Secure configuration guidelines

The developer shall provide guidelines on how to securely configure and operate the smart meter, covering at least:

- hardening;
- account management;
- setting up security logging.

SD5-SM: Vulnerability handling

The developer shall produce security updates to fix all severe vulnerabilities found during the lifecycle of the smart meter. The developer shall monitor all relevant information sources on vulnerabilities, including:

- public vulnerability databases;
- notifications from developers of libraries used in the firmware;
- penetration test results from customers;
- notifications from vulnerability researchers.

The developer shall inform the grid operator about all vulnerabilities found as soon as possible.

Remark: To determine which vulnerabilities are severe, the Common Vulnerability Scoring System (CVSS) should be used. Vulnerabilities with a score of 7.0 or higher would be considered severe and need to be fixed. The developer may agree with the grid operator to use another method to determine the severity of the vulnerabilities if it can be objectively applied and gives a good indication of the risk.

8 Supplier relationships

8.1 Information security in supplier relationships [A.15.2]

To ensure that the smart meter developer protects information of the grid operator or under his responsibility, it needs to implement an information security management system (ISMS).

SR1-SM: Protection of customer assets

The developer shall have an ISMS to protect any information that could compromise the security of the smart meter, including:

- Detailed security designs;
- Source code;
- Customer-specific keys and credentials.

The ISMS shall be ISO/IEC 27001 certified and the certification scope shall cover the development and manufacturing of the smart meter and related tools.

9 Information security aspects of business continuity management

9.1 Information security continuity [A.17.1]

To ensure that the security of the smart metering system is not compromised during disruptions, the smart meter is designed to fail securely.

BC1-SM: Fail-secure design

The smart meter shall be designed to minimize the impact of a failure on security. During a failure the smart meter shall:

- not leak confidential information, such as keys or credentials;
- protect the integrity of critical data;
- not allow access controls to be bypassed;
- restore availability as soon as possible.

Remarks: Examples of failure are hardware malfunctions, corruption of stored or received data, and software crashes. A watchdog can be used to monitor the smart meter and to automatically initiate steps to restore availability.

Appendix A: Implementing the requirements in DLMS

This appendix explains how many of the requirements can be (partially) met by using security measures in the DLMS protocol. The measures refer to the DLMS Green Book edition 7 [12] and Blue Book edition 10 [13], because these are the most commonly used editions. But they can also be implemented when using later editions.

Requirement	DLMS implementation
AC12-SM: Least privileges with separate roles for engineers, the central system, and data concentrators	Different roles can be implemented as different clients. DLMS supports having different passwords or keys per client.
AC15-SM: Machine-to-machine authentication for all users, except customers	User authentication is usually implemented through data access security. Both Low Level Security (LLS) and High Level Security (HLS) can be used. It is recommended to only use LLS for local access, not for access over a network, as the password is sent in cleartext. Some HLS mechanisms are not allowed by requirement CR1-SM as they use outdated cryptographic algorithms. User authentication can also be implemented using data transport security without data access security by enforcing authentication.
CR2-SM: Automated key management	DLMS support updating keys using the global key transfer function. This function protects the confidentiality and integrity of keys using AES keywrap and meets the requirement (if meters come with unique initial keys installed).
OP6-SM: Collecting security events	If the security events are stored in a DLMS event log object, they can be read out over DLMS by both maintenance tools and the data concentrator or central system.

Requirement	DLMS implementation
OP7-SM: Protecting security logs	Access to log may be restricted through the normal access control mechanism for DLMS objects. Vendors need to ensure that enough room is reserved for the log object and that it is rolling.
OP9-SM: Remote firmware updates	DLMS supports remote firmware updates through the image transfer mechanism.
OP10-SM: Verification of firmware signatures before installation	The DLMS image transfer mechanism has a step to verify the image through the image_verify method on the meter. How the image is verified is however not defined in DLMS and is left by the vendor. If the vendor implements the image_verify method so that it verifies the digital signature of the firmware, the requirement can be met within the DLMS image transfer mechanism.
CM1-SM: Cryptographic protection of communication confidentiality and integrity	DLMS can implement the requirement through data transport security. The security policy for all clients used on the WAN and LAN interfaces (except the public client) should be set so that all messages are authenticated and encrypted.

References

[1] ENCS, "SM-302-2020: Security requirements for procuring data concentrators," 2020.

[2] ENCS, "SM-101-2020: Security risk assessment for smart metering," 2020.

[3] ENCS, "SM-201-2020: Security architecture for smart metering," 2020.

[4] ENCS, "SM-401-2020: Security test plan for smart meters," 2020.

[5] ENCS, "SM-402-2020: Security test plan for data concentrators," 2020.

[6] ISO/IEC, "ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements," 2013.

[7] ECRYPT - CSA, "D5.4 Algorithms, Key Size and Protocols Report," 2018.

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

[9] ISO/IEC, "ISO/IEC 19790:2012: Information technology -- Security techniques -- Security requirements for cryptographic modules," 2012.

[10] Carnegie Mellon University (CMU), "SEI CERT C Coding Standard," [Online]. Available: https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard. [Accessed 10 10 2019].

[11] MISRA, "Guidelines for the Use of the C Language in Critical Systems," 2013.

[12] DLMS User Association, "DLMS/COSEM Architecture and Protocols ("Green Book") - 7th Edition," 2009.

[13] DLMS User Association, "COSEM Identification System and Interface Classes ("Blue Book") - 10th Edition," 2010.