SM-302-2019

Security requirements for procuring data concentrators

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	Update shared with members in ENCS member projects on procuring secure equipment
11 November 2019	2.5	Update after ENCS internal review. Hardware security requirements added
30 December 2019	2.6	Final version from ENCS member project on procuring secure equipment

ENCS

Table of Contents

1 Introduction

This document contains security requirements for procuring data concentrators. 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 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 against from cyber-attacks aimed to disrupt the electricity grid, for instance by sending mass switch-off commands.

The data concentrator is an aggregator of the information retrieved and received from the smart meters that are in the same local network (e.g., a PLC network), which is typically used when those smart meters don't have the capability to communicate directly with the central systems or there is a use case for also using the metering information in a field installation (e.g., in a secondary substation to use with DA information) without depending on the central systems.

Secure devices for smart metering 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. Public tendering rules 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 devices, 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 fifteen data concentrators 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 data concentrators and gives requirements for secure development processes at the vendor. A separate document is available for procuring smart meters [1].

The requirements cover secure communication from the data concentrator to smart meters and to the central system. They do not cover the security of the central systems themselves.

The measures cover the following sections from ISO 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 data concentrators, not for legacy systems, although grid operator may analyze which systems can be upgraded to meet them.

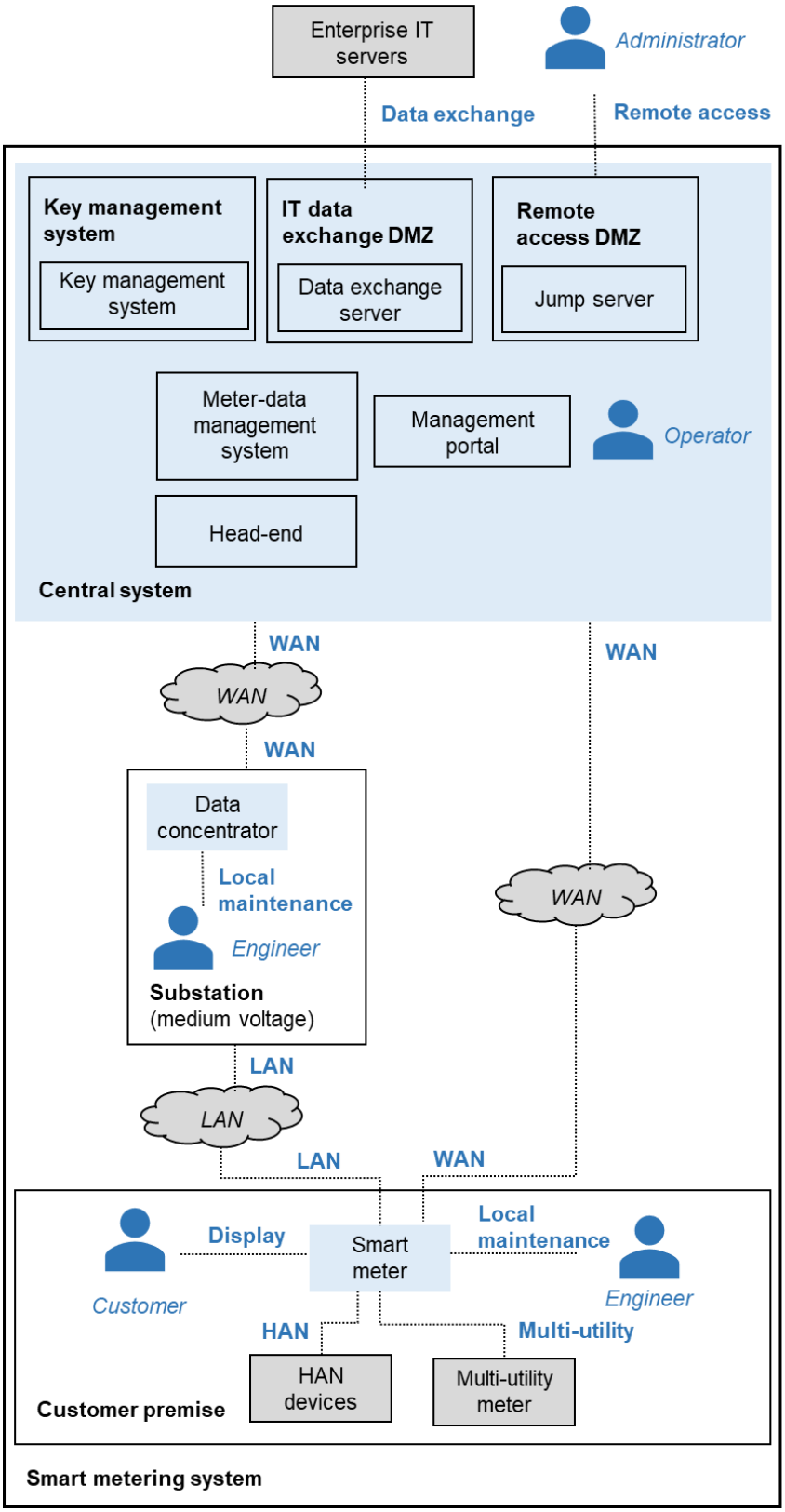

Figure 1: Reference architecture for the smart metering system, showing its users and interface.

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 data concentrators. Requirements for smart meters 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 27001 [6]. To support this, the architecture is organized by the security objectives in ISO 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 data concentrator 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 data concentrators.

User	Required access	Interface
Engineer	• Installation • Maintenance • Testing • Firmware updates	Local maintenance
Central system	• Reading out meter readings • Maintenance • Firmware updates	WAN

2.1 User access management [A.9.2]

The data concentrator manages access rights in such a way that the grid operator can implement the principle of least privileges. For engineers, it uses centrally managed role-based access control to allow the grid operator to keep up with personnel changes and give engineers only the privileges they need.

AC8-DC: Centrally managed, role-based access control for engineers

The data concentrator shall support role-based access control for local engineers with centrally managed accounts. The data concentrator shall be able to:

- allow engineers to log in with individual accounts;
- check the engineer's role in a central access control server;
- enforce the access right of the engineer's role.

The data concentrator shall allow changing the privileges of a role or adding new roles.

Remarks: The engineer's role can be checked through different methods:

- using an online authentication protocol, such as RADIUS
- using a ticked-based authentication protocol, such as Active Directory (AD) (Kerberos)

- using certificate-based authentication, as defined in IEC 62351-8 [7]

Grid operators may want to specify a method that works with their existing systems.

Roles and privileges may be managed through the data concentrator configuration tools.

AC9-DC: Least privileges for the central system

The data concentrator shall restrict the access privileges of the central system, so that it can access only the functions and data it needs.

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

2.2 System and application access control [A.9.3]

The data concentrator enforces authentication for all users. It uses individual passwords for engineers, and machine-to-machine authentication for the central system.

AC10-DC: Authentication with individual passwords for engineers

The data concentrator shall support password-based authentication for engineers. The data concentrator shall secure the log on procedure for engineers by:

- not displaying the password when it is being entered;
- not indicating if an account exists after a failed login attempt;
- blocking access after several failed login attempts;
- automatically closing as session when it has been inactive for more than an administratively configurable maximum time period.

Passwords are stored salted and hashed.

Remark: It is recommended to use a password hashing function that is resistant against GPU cracking attacks, such as Argon2 or PBKDF2.

AC11-DC: Machine-to-machine authentication for the central system

The data concentrator shall support mutual authentication with passwords or keys for the central system.

Remark: Passwords and keys are updated according to measure CR2.

3 Cryptography

The data concentrator uses cryptography for several functions:

- Machine-to-machine authentication for the central system (Section 2);
- Hashing passwords used by human users (Section 2);
- Hardware security measures (Section 4.1);
- Digitally signing the firmware (Section 5.4);
- Protecting the confidentiality and integrity of communication (Section 6.1).

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

3.1 Cryptographic controls [A.10.1]

The data concentrator uses strong cryptographic keys and algorithms to protect against attacks to the cryptography itself. The data concentrator supports remote key updates from the central systems to allow for automated key management. The data concentrator cryptographically protects keys used to send critical commands to smart meters.

CR1-DC: Strong cryptographic keys and algorithms

For security functions, the data concentrator 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 [8] 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 [8]);
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [8] 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-DC: Automated key management

The data concentrator shall support automated key management by:

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

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

The data concentrator shall support remotely changing all passwords used to implement these requirements in a way that protects their confidentiality and integrity.

Remarks: It is allowed that some keys or credentials 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 only exception are (public) keys used as the root of trust for secure boot, which need to be stored in immutable hardware (see PH6-DC).

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 data concentrator can use certificates from the grid operator's PKI for this purpose.

CR3-DC: Protecting keys on the data concentrator

If the data concentrator stores keys used to send critical commands to smart meters, it shall be able to protect the confidentiality and integrity of these keys cryptographically, using a module that does not allow unencrypted keys to be extracted and resists physical attacks as described in PH5b-DC below.

4 Physical and environmental security

Physical security measures on the data concentrator are included to protect key databases.

4.1 Equipment [A.11.2]

If a data concentrator has access to smart meter keys for communication, this creates a risk of keys being stolen through physical attacks. It is therefore recommended to take the following additional hardware security measures on data concentrators.

PH5a-DC: Hardware security for smart meter keys on data concentrators

If the data concentrator stores keys for roles that send critical commands to smart meters, the secure module that stores them shall be implemented on a secure element, satisfying the following requirements:

- The secure element receives keys from the HSM at the central system in such a way that the integrity and confidentiality are protected end-to-end.
- The data concentrator cannot extract long-term keys unencrypted from the secure element, instead the secure element encrypts and authenticates messages provided by the data concentrator.
- Stored keys are protected against advanced software and physical attacks.
- Communication between the data concentrator main processor and the secure element is cryptographically protected to prevent Man-in-the-Middle attacks.

The secure element shall be Common Criteria (CC) Certified against a security target that covers the above requirements and an assurance level of EAL 3 or higher. The vendor shall present all relevant Common Criteria certificates.

Remarks: The second requirement only applies to long-term keys. Session keys may be extracted unencrypted to offload cryptographic operations to the main processor.

Separate Common Criteria certificates may be presented for the IC, Platform and applet.

PH5b-DC: Secure boot for data concentrators

The data concentrator shall have hardware support for secure boot in which the authenticity of all software loaded during the boot sequence is cryptographically verified. The secure boot process:

- has a root of trusted anchored in immutable hardware (ROM or OTP);

- protects the confidentiality and integrity of all parts of the secure boot chain;
- verifies the authenticity of all data cryptographically before use;
- copies all data into volatile memory (SRAM/DRAM) before verification and decryption.

Remarks: Ideally an anti-rollback feature should also be implemented so that an attacker cannot downgrade the firmware to a known vulnerable version. However, this can add operational problems if the newly rolled out firmware version has issues. A solution to this is to have the manufacturer also sign the previous version of the firmware as if it was the next version. However, such a scheme would also mandate that the firmware should contain the customer ID, so that other customers cannot be attacked using this downgrade.

PH5c-DC: Protection of stored data on data concentrators

The data concentrator shall be able to cryptographically protect the integrity and confidentiality of all data is not stored on the same package as the processor. The keys used are stored in hardware that is resistant against advanced physical attacks. Before each use, the processor verifies that data loaded from storage has not been modified since it was written.

5 Operations security

5.1 Operational procedures and responsibilities [A.12.1]

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

OP1-DC: Future-proof design

The data concentrator 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-DC in particular the smart meter supports the key sizes recommended for long term use in Section 4.6 of the ECRYPT report [8];
- Roles and security event types will grow incrementally up to 50%.

Remarks: Data concentrator that use 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 future algorithms specified in CR1-DC should show that the data concentrator can run them without affecting operations.

5.2 Backup [A.12.3]

To support recovery processes, it should be possible to recover the data concentrator from the configuration file used during its installation.

OP4-DC: Recovery from configuration

It shall be possible to recover the data concentrator to its normal operation using a stored configuration, such as a project file.

It shall be possible to manually backup the data concentrator configuration to a remote network location through remote access to the device.

5.3 Logging and monitoring [A.12.4]

To support detecting and responding to security incidents, the data concentrator 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-DC: Security events

The data concentrator 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
12. Invalid settings for cryptographic protocols such as TLS

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

OP6-DC: Collecting security events

The data concentrator shall allow the local security logs to be read out by the normal maintenance tools and the central system.

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

If the data concentrator collects the security logs from the attached smart meters, it shall allow the central system to access them.

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-DC: Protecting security logs

The data concentrator 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.

Remark: Normally on the system and root users should be allowed to modify the logs, and only specific user groups should be authorized to read them.

5.4 Control of operational software [A.12.5]

The data concentrators should support secure software installation procedures by only allowing remote updates that are digitally signed.

OP9-DC: Remote firmware updates

The data concentrator shall allow remote updates for all security functionality for which updates are expected to be needed.

OP10-DC: Verification of firmware signatures before installation

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

Remark: It is additionally recommended to protect the firmware authenticity with secure boot (see requirement PH5b).

5.5 Technical vulnerability management [A.12.6]

Technical vulnerability management is facilitated by the remote firmware updates in Section 5.4. Additionally, the data concentrator should allow hardening to reduce the chance of it having vulnerabilities.

OP11-DC: Hardening

The data concentrator shall support hardening by disabling unneeded functions, in particular, the data concentrator shall allow:

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

OP12-DC: Known vulnerabilities

The data concentrator shall only use applications, libraries and communication protocols without known security vulnerabilities.

OP13-DC: Input validation

The data concentrator shall apply input validation to all data it receives.

Remarks: The data concentrator 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 web interfaces or domain-specific protocols such as DLMS.

OP14-DC: Hardware assisted measures against exploits

The data concentrator shall implement the following hardware features if they are available:

- *No-Execute (NX) / Write-xor-execute (W^R):* If the data concentrator has a Memory Protection Unit (MPU) or Memory Management Unit (MMU), it shall be used to mark code regions as read-only and data sections as non-executable.
- *Address Space Layout Randomization (ASLR):* If the data concentrator has a Memory management Unit (MMU), it shall be used to load data and code at different memory addresses every time an application is run.

The software running on the data concentrator shall be compiled to use the hardware features.

Remark: The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR.

6 Communication security

6.1 Network security management [A.13.1]

The data concentrator needs to support securing communications on the WAN and LAN network. The data concentrator needs to be protected against denial-of-service attacks, as they can be reached directly from untrusted networks.

CM1-DC: Confidentiality and integrity of network communication

The data concentrator 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.

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

The data concentrator 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 data concentrator 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 as well as provide guidelines on secure configuration and operation. If vulnerabilities are found during the lifecycle of the data concentrator, they should provide security updates.

SD1-DC: Secure programming practices

The developer shall set up programming practices to ensure the consistent delivery of secure data concentrator. 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 or use memory-safe languages.

Remark: Examples of secure coding guidelines are the SEI CERT coding standards [11], available for different languages, and the MISRA C software development guidelines for embedded systems [12].

Compiler options that should be enabled include:

- stack cookies or canaries which make it harder to exploit stack-based buffer overflows.
- fortify source which can be used to detect buffer overflow vulnerabilities;
- Control Flow Integrity (CFI) which makes it harder for an attacker to perform code re-use attacks such as return-to-libc or Return Oriented Programming (ROP).

SD2-DC: 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;
- automated web application testing on any web interfaces;
- automated vulnerability scanning.

Remark: The test plan for data concentrators [5] includes a list of test cases that vendors can use to check the implementation of the requirements.

SD3-DC: 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 data concentrators stations 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.

SD4-DC: Secure configuration guidelines

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

- expected security measures in the operating environment;
- hardening;
- account management;
- setting up health and performance monitoring;
- setting up security logging;
- setting up backups.

SD5-DC: Vulnerability handling

The developer shall produce security updates to fix all severe vulnerabilities found during the lifecycle of the data concentrator. 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 data concentrator developer protects information of the grid operator or under his responsibility, it needs to implement an information security management system (ISMS).

SR1-DC: Protection of customer assets

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

- detailed security designs;
- source code;
- customer-specific keys and credentials.

The ISMS shall be ISO 27001 certified and the certification scope shall cover the development and manufacturing of the data concentrator 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 data concentrator is designed to fail securely.

BC1-DC: Fail-secure design

The data concentrator shall be designed to minimize the impact of a failure on security. During a failure the data concentrator 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 data concentrator and to automatically initiate steps to restore availability.

References

[1] ENCS, "SM-301-2020: Security requirements for procuring smart meters," 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] IEC, "IEC TS 62351-8:2011: Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control," 2011.

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

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

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

[11] 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].

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