DA/SA-301-2022

Security requirements for procuring RTUs and gateways

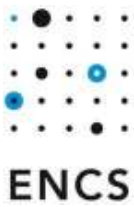
Version 2022v0.8

20 July 2022

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):

This document is shared under the Traffic Light Protocol classification:

TLP White – public



The European Network for Cyber Security (ENCS) is a non-profit membership 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
January 2016	1.0 (2016v1.0)	First release produced in ENCS member project on distribution automation
20 December 2019	2.0 (2019v1.0)	Final version from the 2019 member project on procuring secure equipment.
2 December 2020	2021v0.1	First draft of updated requirements shared with members
18 February 2021	2021v0.2	Updated draft based on test results on various RTUs
22 February 2021	2021v0.3	Version for ENCS internal review
26 February 2021	2021v0.4	Minor edits
11 March 2021	2021v0.5	Integrated optional requirements. Updated based on feedback from tenders.
15 February 2022	2022v0.6 (prev 2022v0.1)	First draft with updated requirements
25 March 2022	2022v0.7	Minor fixes
20 July 2022	2022v0.8	New format with external threat assessment and IEC 62443 requirements

Table of Contents

1 Introduction

This document gives security requirements that grid operators can use in their procurement documents for new remote terminal units (RTUs) and gateways for distribution automation or substation automation.

Grid operators are increasingly automating their medium voltage substations and lines with distribution automation and high voltage substation with substation automation. They use these systems to get power measurements to reliably integrate renewables and electric vehicles, and to remotely control the grid to recover from power outages more quickly.

The automation increases the possible impact of cyber-attacks. Many grid operators already have thousands of substations and lines automated. If attackers succeed in switching off the power in a large part of those, it can take a lot of time to recover.

Making sure the distribution and substation automation systems are secure is hence critical. Grid operators need to set good security requirements when procuring RTUs and gateways. The requirements should not lead to excessive cost when procuring thousands of RTUs, while still ensuring all security risks can be mitigated.

This document provides a harmonized set of security requirements that grid operators use directly in their procurement documents. The requirements have been thoroughly reviewed by both grid operators and vendors. They are designed to fit into the processes and procedures already in place in the organizations and to find a good balance between security and the operational impact.

Harmonizing the requirements allows grid operators to get secure automation equipment more cost-effectively. It saves time and effort in developing requirements, as they are already freely available. It ensures the requirements are feasible, as they have been tested in a market survey, and previous tenders by other operators. And it saves on implementation costs, as vendors get a common baseline to aim at. Grid operators are therefore encouraged to use these requirements when procuring new RTUs or gateways.

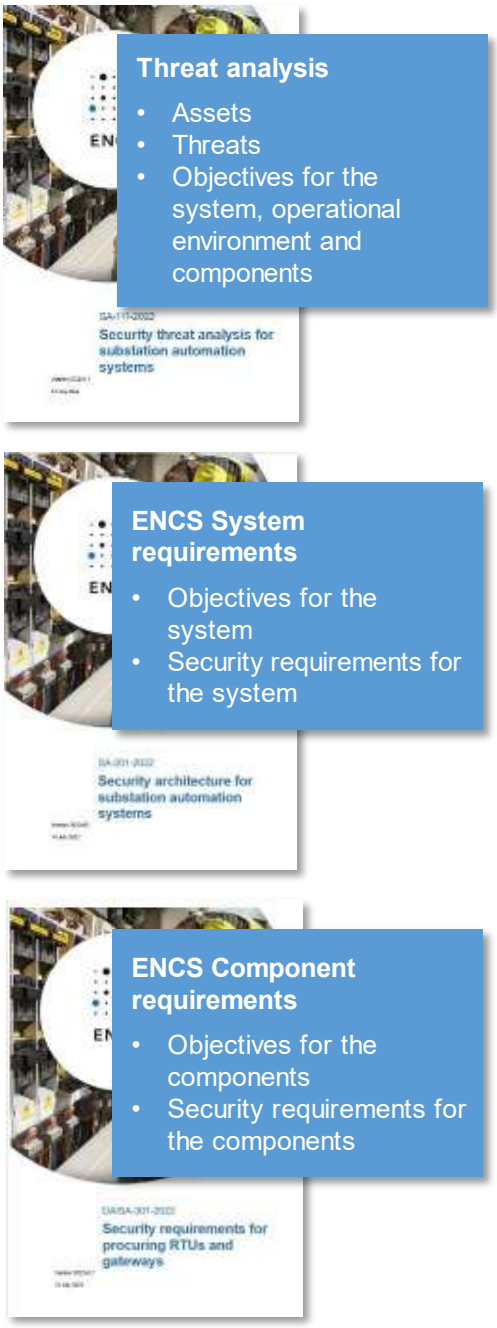


Figure 1: Relation between the different documents on substation automation security.

1.1 Relation to other documents

This document is part of two larger series of documents on substation automation and distribution automation security, as shown in Figure 1.

Both series start with a threat analysis [1] that determines security objectives to counter the threats posed to the assets in a typical substation or distribution automation system. The objectives are split into objectives for the system and operational environment. The objectives for the system are the basis for the security requirements for the system in [2].

The objectives for the operational environment should be implemented by grid operators outside of the system to operate it securely. They include objectives on organizational processes and physical security. Many grid operators will meet these security objectives through their information security management system. Hence, the objectives are linked to controls from the ISO/IEC 27002 standard.

From the security objectives for the system, the threat analysis also derives security objectives for gateways and RTUs. The objectives are chosen so that a gateway meeting the component objectives can be easily integrated into a system meeting the system objectives. The security objectives are the basis for the requirements for gateways and RTUs in this document.

The same objectives are chosen for gateways and RTUs in substation and distribution automation systems, because often vendors are offering the same devices or platforms for both types of systems. By setting the same objectives and requirements, it will be easier for vendors to define their security roadmap and for grid operators to procure devices that meet the requirements.

1.2 Intended use of the device

This document gives requirements for procuring secure RTUs and gateways for distribution automation and substation automation systems. The RTUs and gateways can be used in:

- medium to low voltage transformer substations
- medium voltage transport substations
- automatic circuit recloser controllers applied to overhead distribution lines
- high to medium voltage transformer substations
- high voltage transport substations

Grid operators use RTUs and gateways to monitor and control the medium and high voltage electricity grid from the SCADA systems at their control centers. The RTU or gateway is the device at a substation with which the SCADA system communicates. From the RTU or gateway, the SCADA system gets measurements on the state of the grids, and alarms from, for instance, short circuit indicators from the RTU or gateway, and it sends commands to control the grid, for instance by switching circuit breakers, to the RTU or gateway.

We will use the name '**RTU**' for devices that are connected to sensors and actuators primarily through digital and analog input and output (Figure 2), and '**gateway**' for devices

connected primarily through network communication (Figure 3). RTUs are more commonly used in distribution automation (medium voltage substations), gateways more commonly in substation automation (high-voltage substations). But the distinction between RTUs and gateways is often not clear. Many devices on the markets can be used in either role, depending on their configuration. Hence, the security requirements are designed to apply to both RTUs and gateways.

In this document, the term **"device"** will be used for both **RTUs** and **gateways**.

1.3 Intended operational environment

Figure 2 and Figure 3 show the reference architecture for distribution and substation automation systems used in this document. The reference architectures give a simplified view of the intended operational environment for the RTUs and gateways. Security objectives for the operational environment are given in the Security threat analysis for substation automation systems [1].

The RTU or gateway is connected to the SCADA system over a wide-area network (WAN). For distribution automation, this is usually a wireless mobile network, such as a GPRS, CDMA, or LTE network. For substation automation, it is usually a glass fiber network. Grid operators often use the networks of external telecom providers, especially for distribution automation. Network segregation measures such as private APNs are commonly used. But the WAN network is usually not considered trusted for the type of grid control that RTUs and gateways are used for.

The SCADA systems communicate with the RTU or gateway using specialized protocols. Currently, IEC 60870-5-104 is most commonly used. In the future, it is expected that MMS will be increasingly used according to the IEC 61850 standard. For communication with sensors and actuators in the substation, gateways often also use MMS following IEC 61850.

The RTU or gateway is maintained by engineers from the grid operator or its contractors. They can maintain the RTU or gateway locally or remotely. Local maintenance is done at the field location with an engineering laptop. The laptop connects to a local maintenance interface on the RTU or gateway, which can for instance be an Ethernet, USB, or serial port. The engineer then uses specialized engineering software or a web interface on the RTU or gateway to configure it and troubleshoot problems.

Remote maintenance is done from the grid operator's offices, usually from secure locations close to the control centers. Remote maintenance can be done with the same tools as local maintenance. Alternatively, specialized maintenance servers are used to monitor and configure large numbers of RTUs or gateways, and to apply batch firmware

updates. Such servers are more commonly use in distribution automation, as this involves many more devices than substation automation.

Physically, the RTUs and gateways are deployed in substations and other field locations. These locations are unattended most of the time. Engineers only visit them when there are problems or there is scheduled maintenance. Some locations may not be visited for years.

Physical security differs greatly between locations. Large high-voltage substations may be protected by advanced alarm and camera systems, monitored by physical security companies. Distribution automation substations usually are in separate buildings or rooms that are locked. Sometimes there is a sensor to detect door openings. But reacting to the alarms from such sensors make take considerable time. RTUs on overhead distribution lines are, at most, protected by a locked cabinet.

The security requirements assume that motivated attackers can physically reach the RTU. They may also steal an RTU to prepare physical attacks. The goal is to allow grid operators to limit the impact of such physical attacks.

1.4 Checklist for additional requirements

The baseline requirements in Section 3 cover the functions needed to securely operate RTUs or gateways. They can be used directly in procurement documents. It is recommended not to change them, as vendors may read over the changes if they know the requirements from other tenders.

In some cases, grid operators may want to add additional requirements to extend or specify some requirements. Section 4 provides standard sets for optional security requirements that grid operators can add to the baseline. Additionally, grid operators are recommended to check if they want to extend the following requirements to ensure the RTUs or gateways work with their existing system:

- **C.9.4.1, C.13.1.1:** consider specifying the method the device uses to authenticate and secure communication with the SCADA system such as TLS, IPsec, or OpenVPN.
- **C.12.5.4:** consider specifying a method to allow integration into existing tools, or including the tools needed for firmware updates in the tender scope.

Which technologies vendors support, are described in the market survey on DA RTUs [3].

Grid operators are also recommended to check if they want to further specify some of the terms in the following requirements to make them more precise:

- **C.10.1.1:** consider specifying the regulations on cryptography the device needs to comply with, for instance, to meet national legislation.

- **C.12.1.1, C.14.2.6:** consider specifying the expected lifetime of the device.
- **C.12.1.1:** consider specifying the computing power or memory reserves the RTU should have to be future proof.
- **C.12.4.4:** consider specifying the minimum amount of log events to be stored.

The above specifications depend on the situation at the grid operators and are therefore not included in this document.

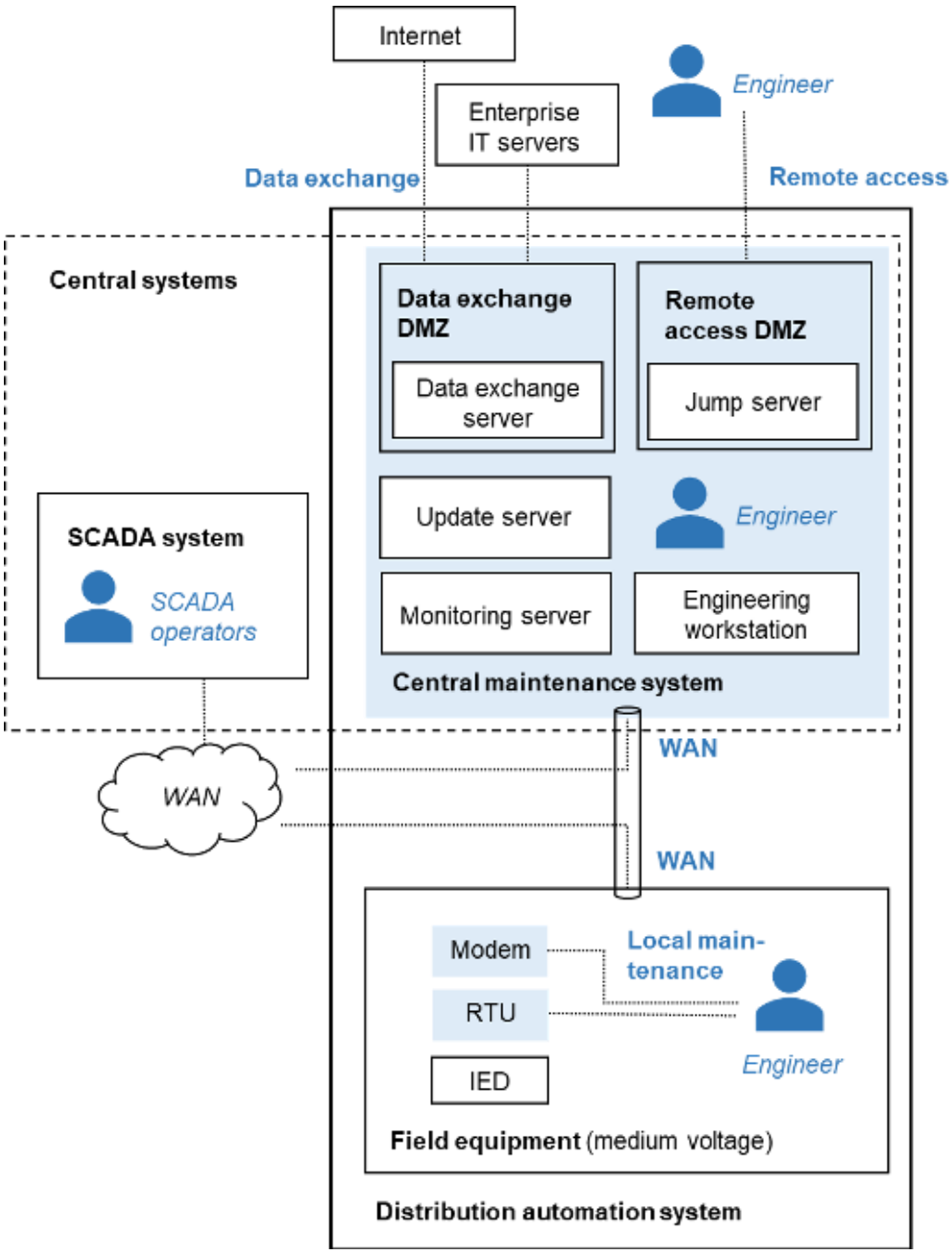


Figure 2: Reference architecture for distribution automation systems, showing its users and interfaces. The requirements in this document concern the RTU.

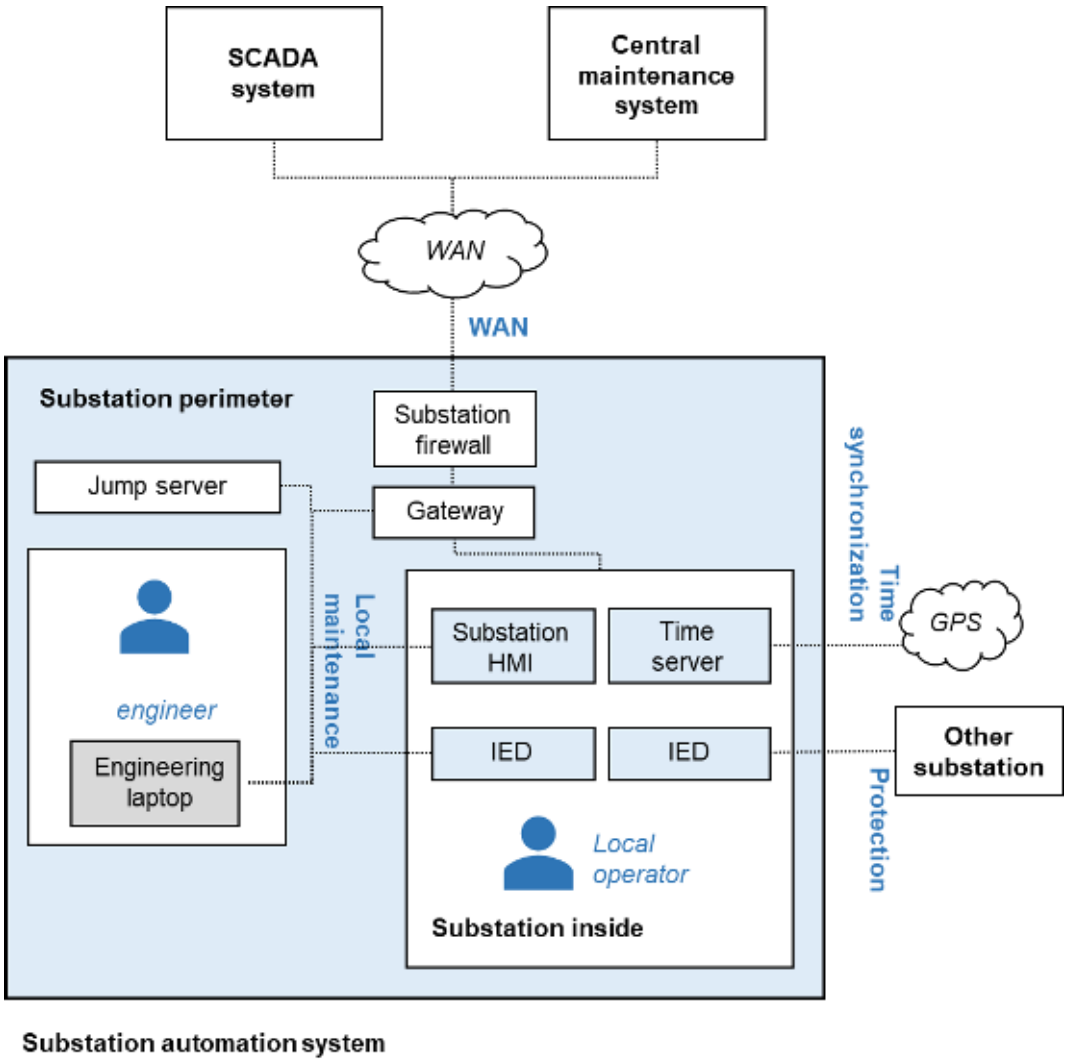


Figure 3: Reference architecture for the substation automation system, showing its users and interfaces. The requirements in this document concern the gateway.

2 Security objectives

This section describes the security objectives for the gateways and RTUs based on which the requirements are selected in Section 3. The rationale for the security objectives is given in the threat analysis for substation automation [1]. This section also describes the access control policy to which the access control objectives refer.

2.1 Access control policy

Table 1 lists the users that are authorized to access the RTU and gateway and the access they require. See Figure 2 and Figure 3 for the interfaces. The access control policy should be designed to implement the principle of least privileges, so that each user group can only access the functions it requires.

Table 1: User groups on the device.

User group	Required access	Interface
SCADA system	• Collect measurements of electrical variables • Send control commands	WAN
Central maintenance system	• Configure the device • Recover the device from a backed-up configuration • Update the device firmware • Monitor the operational logs • Collect additional measurements of electrical variables	WAN
Engineers	• Configure the device • Recover the device from a backed-up configuration • Update the device firmware • Analyze the operational logs	Local maintenance

On the WAN there are two user groups accessing the device: the SCADA system and the central maintenance system. These user groups have different access requirements. The SCADA system only requires access to grid related assets. It should be able to collect the measurements of electrical variables and send control commands.

The central maintenance system should normally only access the configuration and the firmware. In some cases, the central maintenance system may however collect additional measurements of electrical variables, such as high frequency measurements related to faults.

The device should be able to distinguish between the two user groups on the WAN to limit the impact if one of the groups is compromised. Each user group should separately authenticate to the device. The device should ensure that each system can only access the required functions.

On the local maintenance interface, the only user group are engineers from the grid operator or its contractors. These should be able to change the configuration and update the firmware. In case of problems, they should be able to configure the device from a backup configuration. Grid operators may define roles within the group of engineers to apply more fine-grained access rights.

The access control model assumes that engineers do not access the device directly over the WAN. They always work through the central maintenance system.

2.2 Security objectives

To ensure the threats in [1] and [4] are mitigated and the access control policy in Section 2.1 can be followed, the substation perimeter should meet the following security objectives. The rationale for these objectives is described in the threat analyses for substation automation systems [1] and distribution automation systems [4].

AC3 Network-based access control for the SCADA system	The device can enforce access control for the SCADA system based on their network location. The device can verify that the SCADA system is on a trusted network, while allowing SCADA system users to verify its unique identity. The device then enforces that SCADA system users can only access the functions they need.
AC4 Role separation for the central maintenance system	The device can enforce access control with separate roles for the central maintenance system, so that each user can only access the functions they need for their role. The central maintenance system identifies to the device with information that allows the device to determine its role. The device authenticates the user's role and assigns them access rights based on the role. The device uniquely identifies itself to the central

	maintenance system and allows the system to authenticate it.
AC5 Centrally managed, role-based access control for engineers	The device can enforce role-based access control with individual user accounts managed on a central server. The device can enforce mutual authentication for engineers using individual passwords or keys with a login procedure that is protected against known attacks.
MA2 Remote management	The device can be managed remotely. Through remote access it is possible to: • update passwords and keys • update the software or firmware • restore the device from a backed-up configuration The device allows the confidentiality and integrity of the passwords, keys, software, firmware, and back-ups to be protected cryptographically during transport. The device checks the authenticity of firmware or software through digital signatures. The device allows to disable unneeded functions to reduce the likelihood of vulnerabilities. It allows to enable security functions available on the hardware and software platforms to reduce their possible impact.
MO3 Integration with SIEM system	The device shall log security events, such as access control events, and changes to the configuration and firmware. The device can store the logs locally and send them directly to a Security Information and Event Management (SIEM) system in a commonly supported format. The device supports time synchronization to have reliable timestamps for events.
CM1 Cryptographic protection of communication confidentiality and integrity on WAN	The device cryptographically protects the integrity and confidentiality of communication on the WAN interface. The measures shall allow to verify the source of messages and protect against replay and man-in-the-middle attacks.

3 Baseline security requirements

This section contains a set of baseline security requirements that an RTU or gateway should comply with to meet the security objectives in Section 2.2. The baseline covers security measures that most RTU and gateway vendors have implemented and that mitigate the risk that most grid operators have in their substation and distribution automation systems. Sets of optional requirements for additional features are given in Section 4.

3.1 Access control

Access control requirements concern how access rights are managed and how strong their authentication needs to be for different user groups. The device enforces access control for the user groups in Table 1 in Section 2.1.

3.1.1 User access management [A.9.2]

The device 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, so that the grid operator can keep up with personnel changes and give engineers only the privileges they need.

C.9.2.3 Least privileges with separate roles for Central maintenance system

The device shall allow to enforce access control with separate roles for central maintenance system, so that they can access only the functions and data they need for their role.

Remarks: The requirement can be met by having a different user account for each role. Each account should then have its own password or keys for authentication.

The requirement can also be met by full role-based access control.

C.9.2.4 Centrally managed, role-based access control for engineers

The device shall support role-based access control for engineers with centrally managed accounts. The device 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 device shall provide a way for engineers to access it when the device cannot reach the central server.

Remarks: The engineer's role can be checked through different methods. See Section 4.3 for recommended methods. It is recommended to by default support the roles and privileges defined in IEC 62351-8 [5].

To provide access when it cannot reach the central authentication server, the device can for instance use local accounts. Strong passwords should be used also for the local accounts (used when the central server cannot be reached) to ensure they cannot be used to bypass authentication. Preferably, unique passwords are used in each substation, and these are only given to engineers when needed.

3.1.2 System and application access control [A.9.3]

The device supports authentication for all users. It uses individual passwords for engineers.

C.9.4.1 Authentication based on network location for SCADA system

The device shall support authentication for the SCADA system through one of the following options:

A. Based on their network location through a VPN terminating at the device. Mutual authentication shall be used between the device and a network device (e.g., firewall or concentrator) at the central system during the setup of the VPN. Unique passwords or keys can be used for each device.
B. Using unique mutual authentication, so that the SCADA system can check that a connection comes from a unique device, and the device can check that a connection comes from the SCADA system.

Remarks: This measure is usually implemented together with the cryptographic communication security measure C.13.1.1. Passwords and keys are updated according to measure C.10.1.3. Option B can be implemented using transport layer security (TLS) with client-side certificates. The authentication mechanism needs to comply with requirement C.10.1.1 (including the validation of certificates).

C.9.4.2 Authentication by role for central maintenance system

The device shall support mutual authentication for the central maintenance system with passwords or keys that may be shared between users in the same role, so that:

- the central maintenance system can check connections are coming from a unique device, and
- the device can check that maintenance connections are coming from the maintenance application.

Remarks: Passwords and keys are updated according to requirement C.10.1.3. The authentication mechanism needs to comply with requirement C.10.1.1 (including the validation of certificates).

C.9.4.4 Authentication using individual passwords for engineers

The device shall support password-based authentication for engineers. The device shall secure the logon procedure for engineers, for instance 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 a session when it has been inactive for a certain time

The device shall store passwords salted and hashed.

Remark: The inactive time after which a session is closed should be configurable. It is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2.

3.2 Cryptography

3.2.1 Cryptographic controls [A.10.1]

The device uses strong cryptographic keys and algorithms to protect against attacks to the cryptography itself. The device supports remote key updates from the central systems to update keys on possibly thousands of substations.

C.10.1.1 Strong cryptographic keys and algorithms

For security functions, the device shall use cryptography according to regulations and modern guidelines without any modifications. In particular:

- It only uses the cryptographic algorithms that the ECRYPT – Algorithms, Key Size, and Protocols Report [6] recommends as suitable for new or future systems.
- It uses keys as least as long as the ECRYPT report recommends for near term use (section 4.6 in [6]).
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [6] 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 or role of the user.

Remark: The requirement applies for instance for the cryptography used in:

- machine-to-machine authentication for the SCADA system and central maintenance system (C.9.4.1 and C.9.4.2)
- hashing passwords used by human users (C.9.4.4)
- digitally signing the firmware (C.12.5.3)
- protecting the confidentiality and integrity of communication (C.13.1.1)

When validating a certificate, the identity of the user can be checked through the subject name, common name, or distinguished name. The role can be checked through the roleID field described in IEC 62351-8 [5].

C.10.1.3 Remote update of passwords and keys

The device shall support remotely changing all passwords and keys used to implement these requirements in a way that protects their confidentiality and integrity, except for root certificates with a long validity period.

Where the device uses certificates for authentication or communication security, it shall be able to use certificates issued by the public key infrastructure (PKI) of the grid operator.

Remarks: Keys and credentials may be updated manually using the maintenance tools. When public-key cryptography is used, keys are preferably updated using an automated process, such as the Simple Certificate Enrollment Protocol (SCEP) [7] or Enrollment over Secure Transport (EST) [8] described IEC 62351-9 [9]. (See Section 4.4.)

Key updates should only happen in compliance with the grid operator's update policy. A validation procedure should be defined to ensure proper change management.

It is allowed that keys or credentials cannot be updated if they are only used for device internal purposes, such as encrypting local storage or setting up secure communication between processors on the same device. But, as soon as they are used to implement any of the requirements in this document, they must also comply with this requirement.

The certificate used to verify firmware updates (C.12.5.3) is issued by the vendor. So, for this certificate, the device does not need to be able to use certificates from the grid operator PKI.

3.3 Operations security

The device should support the operational processes and procedures needed to keep it secure throughout its lifetime.

3.3.1 Operational procedures and responsibilities [A.12.1]

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

C.12.1.1 Future-proof design

The device 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 C.10.1.1, in particular, the device supports the key sizes recommended for long term use in Section 4.6 of the ECRYPT report [6];
- Roles and security event types will grow incrementally up to 50%.

Remarks: Compliance with 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 recommended for long-term use in [6] should show that the device can run them without affecting operations. It is acceptable if the device can only support the long-term key sizes for elliptic curve-based algorithms, not for RSA-based algorithms.

3.3.2 Protection from malware [A.12.2]

The device is protected against exploits and malware by using available platform security features.

C.12.2.2 Use of platform security features

The device shall use security features from the underlying hardware and software platform whenever possible.

Remark: It is recommended to use the following hardware features when they are supported:

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

The software running on the device must be compiled to use the hardware features. The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR.

3.3.3 Backup [A.12.3]

To support recovery processes, it should be possible to recover the device from the configuration files used during its installation.

C.12.3.2 Recovery from configuration files

It shall be possible to recover the device from any failure state to its normal operation using a stored configuration, such as a project file.

Remark: One method to allow easy recovery is to store a previous known correct file stored in the device file system, which is safely retrievable and usable by an authorized user executing the least possible number of steps.

3.3.4 Logging and monitoring [A.12.4]

To support detecting and responding to security incidents, the device needs to log relevant security events and allow them to be gathered for analysis. As the security logs are important to security, they also need to be protected themselves.

C.12.4.2 Security events

The device shall be able to store in a local log all events relevant to its security, such as:

- Successful authentications
- Failed authentication attempts
- Firmware uploads
- Successful firmware updates
- Failed firmware updates
- Changing the device configuration
- Changing the system time
- Booting the device
- Shutting down the device
- Changing keys or credentials
- Failed attempt to change keys or credentials
- Changing user accounts
- Changing authorizations

The log entries for security events shall include a timestamp, an event description, and the role causing the event. Events caused by engineers are linked to individual users.

C.12.4.3 Collecting security events over syslog

The device shall allow the security logs to be read out using the normal maintenance tools.

The device shall be able to send all security logs to a central server using, at least, the Syslog communication protocol (RFC 5424 [10]). The logs shall be sent in a commonly used format to avoid the need to develop a dedicated parser.

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

Remark: The logs can be sent directly to a Security Information and Event Management (SIEM) system, or they can be gathered first by a monitoring server in the central maintenance system and then forwarded to the SIEM. The choice depends on where the SIEM system is placed in the grid operator's networks. The device should allow selecting from which severity level it sends log events to the central server.

C.12.4.4 Protecting security logs

The device 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 only the system and root users should be allowed to modify the logs, and only specific user groups should be authorized to read them.

3.3.5 Control of operational software [A.12.5]

The authenticity of firmware updates is verified using a digital signature.

C.12.5.2 Remote firmware updates

The device shall allow remote software or firmware 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
- update the cryptographic random number generator
- add more roles
- change the authorization of role

C.12.5.3 Verification of firmware signatures before installation

The device shall be able to verify the authenticity of firmware updates using digital signatures before installing the firmware. The vendor digitally signs each firmware release.

Remark: Verifying the firmware integrity using only a hash value does not satisfy the requirement. It is recommended to also encrypt the firmware during transport, to make it harder to reverse engineer it and find vulnerabilities.

3.3.6 Technical vulnerability management [A.12.6]

To support effective vulnerability management, the device is hardened by disabling unneeded functions and enabling security features.

C.12.6.1 Hardening

The device shall support hardening by disabling unneeded functions. Specifically, the device shall allow:

- all unused user accounts to be removed
- all unused network services to be disabled
- all unused hardware interfaces to be disabled

Remark: If a VPN tunnel is used, the device must allow closing all services not used outside of the tunnel.

3.4 Communication security

3.4.1 Network security management [A.13.1]

The device needs to support securing communications on the WAN network.

C.13.1.1 Confidentiality and integrity of network communication

The device shall be able to cryptographically protect the integrity and confidentiality of communication on the WAN interface. The measures shall allow to verify the source of messages and protect against replay and man-in-the-middle attacks.

Remarks: Confidentiality and integrity of the communication can be protected by setting up a VPN tunnel or by using TLS (as specified in IEC 62351-3 [11] and IEC 60870-5-7 [12]).

If end-to-end secure protocols are used for the SCADA traffic, it is recommended that the device allows to turn off encryption and use only message authentication, so that it is possible to apply deep-packet inspection. With TLS this can be achieved by using the NULL cipher (although this is not allowed by IEC 62351-3 [11]).

If a VPN is used to implement the first part of the requirement, the deep-packet inspection sensor can be placed after the VPN concentrator in the central systems. So, encryption can be used without limiting visibility.

3.5 System acquisition, development, and maintenance

3.5.1 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 lifetime of the device, they should provide security updates.

C.14.2.1 Secure programming practices

The developer shall set up programming practices for the device firmware. They 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 [13], available for different languages, and the MISRA C software development guidelines for embedded systems [14].

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)

C.14.2.2 Security testing during development

The developer shall test each firmware release to find vulnerabilities and 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

The developer shall make the results of these tests available to the grid operator on request.

Remarks: The test plan for RTUs and gateways [15] includes a list of test cases that vendors can use to check the implementation of the requirements.

The device developer should test that their code checks the validity of all input data, including validating if values are within the permitted value range. They should monitor for input validation vulnerabilities in third-party libraries or applications. They should also use reviews and robustness tests for code they develop in-house, such as web interfaces or the implementation of domain-specific protocols such as IEC 104. For web services, it is recommended to follow the recommendations from the Open Web Application Security Project (OWASP) [16] [17].

C.14.2.3 Support for third party 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 devices 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 as long as it does not prevent proper testing.

C.14.2.4 Secure configuration guidelines

The developer shall provide guidelines on how to securely configure and operate the device, 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

C.14.2.6 Vulnerability handling

The developer shall produce security updates to fix all severe vulnerabilities found during the lifetime of the device. 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 vulnerabilities as soon as possible.

Remark: As vulnerabilities should be considered at least:

- vulnerabilities for third party libraries and applications reported in public databases, such as the Common Vulnerabilities and Exposures (CVE) database
- issues that would allow bypassing the security measures in this document
- input validation issues
- denial-of-service issues that can be exploited remotely
- failures of security measures due to hardware malfunctions, corruption of stored or received data and software crashes

To determine which vulnerabilities are severe, the Common Vulnerability Scoring System (CVSS) can 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.

3.6 Supplier relationships

3.6.1 Information security in supplier relationships [A.15.2]

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

C.15.1.1 Protection of customer assets

The developer shall have an ISO/IEC 27001 certified ISMS that protects the confidentiality, integrity, and availability of any assets that could compromise the security of the device, including:

- detailed security designs
- source code
- the development and build environment
- private keys used for firmware signing
- customer-specific keys and credentials

Remark: The certification scope should cover the development and manufacturing of the device and related tools.

4 Optional security requirements

The requirements in Section 3 provide a baseline of security measures that are present in most RTUs and gateways and that sufficiently mitigate security risks for most grid operators. Some grid operators may want to have additional security features to mitigate additional risks specific to their situation, or to ensure that the RTUs and gateways are interoperable with their existing central systems.

This section contains five sets of optional security requirements that grid operators can use to procure RTUs or gateways with the following additional security features:

- Security for a central maintenance application
- Additional protection against physical attacks
- Centralized access control profiles to integrate with specific technologies
- Automated key management
- Secure direct communication between devices at different location

Grid operators can use these requirements to complement the baseline requirements in Section 3. It is expected that some optional requirements will be integrated in future versions of the baseline when more vendors support them.

As in Section 3, the term “device” is used for both RTUs and gateways.

4.1 Central maintenance application

Grid operators may want to include a central maintenance application in their procurement. This is the application in the central maintenance system that can be used to remotely configure the devices or apply firmware updates. Such applications are particularly useful in distribution automation systems with thousands of RTUs.

This section contains technical security requirements for procuring the central maintenance application. The requirements allow the application to be used in the recommended security architecture described in [18]. In addition to these technical requirements, the scope of the organizational requirements to the vendor in Sections 3.5 and 3.6 should be extended to cover the development of the central maintenance application.

C.9.2.4 Centrally managed, role-based access control for remote engineers

The central maintenance application shall support role-based access control for engineers with centrally managed accounts. It 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 central maintenance application shall allow grid operators to implement their own access control model, for instance by allowing them to create roles with custom privileges.

C.9.4.3 Machine-to-machine authentication for the central maintenance system

The central maintenance application shall support mutual authentication with the devices, so that:

- the central maintenance application can check connections are coming from a unique device, and
- the device can check that maintenance connections are coming from the maintenance application.

C.10.1.1 Strong cryptographic keys and algorithms

For security functions, the central maintenance application shall use cryptography according to regulations and modern guidelines without any modifications. In particular:

- It only uses the cryptographic algorithms that the ECRYPT – Algorithms, Key Size, and Protocols Report [6] recommends as suitable for new or future systems.
- It uses keys as least as long as the ECRYPT report recommends for near term use (section 4.6 in [6]).
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [6] 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 or role of the user.

Remark: When validating a certificate, the identity of the user can be checked through the subject name, common name, or distinguished name. The role could be checked through the roleID field described in IEC 62351-8 [5].

C.12.4.2 Security events

The central maintenance application shall be able to store in a local log all events relevant to security, such as:

- Successful authentications
- Failed authentication attempts
- Firmware uploads to devices
- Successful firmware updates to devices

- Failed firmware updates to devices
- Changing the device configuration
- Changing keys or credentials on devices
- Failed attempt to change keys or credentials on devices
- Changing user accounts on devices
- Changing authorizations on devices
- Changing access control settings on the central maintenance application

The log entries for security events shall include a timestamp, an event description, and the role causing the event. Events caused by engineers are linked to individual users.

C.12.5.4 Batched, remote firmware updates

The central maintenance application shall allow to perform batched, remote firmware updates to the devices. It shall be possible to update all security functions through these updates.

Remark: Allowing batch firmware updates simplifies managing large numbers of RTUs, for instance, making it is easier to roll out security updates.

C.13.1.1 Confidentiality and integrity of network communication

The central maintenance application shall be able to cryptographically protect the integrity and confidentiality of communication on all its interfaces. The measures shall allow to verify the source of messages and protect against replay and man-in-the-middle attacks.

4.2 Additional protection against physical attacks

This section contains requirements to implement the additional measures against physical attacks defined in the whitepaper *Protecting distribution automation systems against physical attacks* [19].

Requirement C.10.1.8 helps to limit the impact of a physical compromise to one device by ensuring that keys and passwords shared between devices are not sent to the device. So, even if an attacker gains full control of the device, they cannot capture keys or passwords that they can use in other parts of the system.

The hardware security requirements C.11.2.6, C.11.2.7, and C.11.2.8 make it harder for attackers to compromise a device and use it as an entry point into the central systems.

C.10.1.8 Challenge-response authentication on WAN

The device should be able to only use challenge-response protocols for authentication on the WAN, so that it does not receive passwords or keys.

Remark: This measure protects against physical attacks against the device. If the device would receive passwords or keys after a physical compromise, attackers could use these to compromise other hosts in the system.

C.11.2.6 Secure boot

The device should 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 trust 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 to prevent double fetch issues

An anti-rollback feature should be implemented in hardware so that an attacker cannot downgrade the firmware to a known vulnerable version.

Remarks: The anti-rollback feature can create operational problems if the newly rolled out firmware version has issues. A solution to this is to have the manufacturer sign the previous version of the firmware as if it was the next version. This solution does require that the firmware be linked to the customer, so that other customers cannot be attacked using this downgrade.

C.11.2.7 Protection of all stored data

The device should be able to cryptographically protect the integrity and confidentiality of all stored data. Before using data loaded from storage, the processor should verify that it has not been modified.

The keys used to protect the data should be stored so that they are protected against advanced physical attacks. Unique keys should be used for each device.

Remarks: The keys can be stored in tamper resistant hardware or encrypted and authenticated using another key stored in tamper resistant hardware. Tamper resistant hardware could be a specially protected part of the main processor or a dedicated cryptoprocessor, such as a secure element or trusted platform module.

If the key is stored in a cryptoprocessor, the cryptographic operations on the stored data do not need to be done on the cryptoprocessor, as this may cause performance issues. The unprotected data would anyway be available to attackers when the device is running.

C.11.2.8 Hardware-based authentication

The device should use a cryptoprocessor to protect authentication keys and passwords, so that it is not possible to authenticate as the device without the cryptoprocessor.

- Authentication keys and passwords cannot be accessed on the device unencrypted outside of the cryptoprocessor:
- The cryptographic operations needed to authenticate the device are performed by the cryptoprocessor.
- Keys and passwords are either securely generated inside the cryptoprocessor, or they are sent from an HSM at the central system in such a way that the integrity and confidentiality are protected end-to-end.

Communication between the cryptoprocessor and the main processor should be cryptographically protected to prevent man-in-the-middle attacks.

The cryptoprocessor should be certified through an international scheme to fulfill the above requirements and protect against attacks by advanced attackers, including advanced physical attacks. The vendor should present all the relevant certificates.

Remarks: When keys are generated within the cryptoprocessor, they must be generated using a cryptographic random number generator seeded with enough entropy.

Possible certifications for the cryptoprocessor are:

- Common Criteria (CC) for a secure element. The security target must cover the above requirements and have an assurance level of EAL 3 or higher.
- Trusted Platform Module (TPM).

Relevant certificates would include those for the IC, platform and applets implementing the cryptographic functions.

4.3 Profiles for centralized access control

This section contains specifications for implementing centralized access control on devices in a way that is interoperable between vendors. Two profiles have been selected based on the analysis in the whitepaper *Centralized access control for field devices* [20]. The first profile uses certificate-based authentication following the IEC 62351-8 PUSH method [5]. The second profile uses RADIUS.

4.3.1 Profile 1: Certificate-based authentication

With certificate-based authentication, engineers authenticate to the device with a personal X.509 certificate. The certificate contains information about their role. The advantage is that engineers can also authenticate if the device cannot communicate with

the central systems. The disadvantage is that the grid operators must set up a public key infrastructure (PKI) and a way to hand out certificates to engineers.

C.9.2.6 Centrally managed role-based access control using certificates

The device should support role-based access control for engineers with authentication using certificates following the PUSH model in IEC 62351-8 [5]. The device should support at least access token Profile A (X.509 Public key certificate), as defined in [5] Section 10.5.1.

Remarks: The engineer's certificate can be used as a client-side certificate when setting up a TLS or DTLS connection. In this way, it can be used for web interfaces, MMS access, and most maintenance tools relatively easily.

Profile A in [5] is selected over Profile B because the attribute certificates used in profile B do not seem to be widely supported in TLS libraries.

4.3.2 Profile 2: Authentication using RADIUS

In this profile, the device checks the user's credentials with a central RADIUS server. The server tells the device which role the user has. The advantage over Profile 1 is that there is no need to set up a PKI that hands out certificates to engineers. The disadvantage is that the device needs to be able to communicate with the central RADIUS server.

C.9.2.7 Centrally managed role-based access control using RADIUS

The device should support role-based access control for engineers with authentication using the RADIUS protocol, as follows:

- The engineer enters their password on a maintenance tool on their own device.
- The device sets up a secure connection to the RADIUS server using TLS. The device checks the identity of the RADIUS server.
- The device authenticates the engineer with the RADIUS server. It supports at least the EAP-TTLS authentication method.
- The RADIUS server tells the device the engineer's role using the Profile D: RADIUS token defined in [5], Section 10.5.4.

The device shall provide local accounts from which engineers can log in when the device cannot reach the central server.

Remarks: The EAP-TTLS authentication method is chosen because it does not give the password in cleartext to the device. Even if an attacker fully compromises a device, they cannot get the password.

The identity of the RADIUS server can be checked for instance through the subject name, common name, or distinguished name in the certificate. If the identity is not checked, attackers may spoof the RADIUS server to gain access to the device.

4.4 Automated key management

This section contains specifications for implementing automated key management in a way that is interoperable between vendors. The requirements are designed to ensure that devices can be used in a key management system compliant with IEC 62351-9 [21]. The requirements are aimed at using asymmetric keys in a public key infrastructure. They ensure that the device complies with the requirements for asymmetric key management in Section 8 of IEC 62351-9 [21].

C.10.1.5 Automated enrollment and key renewal

The device should support automatically enrolling into a grid operator's public key infrastructure during commissioning and automatically updating keys when they are within a configurable time before expiration. The device should support using at least one of the following protocols:

- Simple Certificate Enrollment Protocol (SCEP, RFC 8894 [7])
- Enrollment over Secure Transport (EST, RFC 7030 [22])

If the device supports SCEP, it should support the following transactions of that protocol:

- get CA certificate
- certificate enrollment and renewal
- poll for client initial certificate
- get next certificate authority certificate

The device should support signing the SCEP message with an existing CA certificate in case of key renewal (see Section 2.3 in RFC 8894 [7]).

If the device supports EST, it should support the following functions of that protocol:

- distribution of CA certificates
- *SimplePKIRequest* and *SimplePKIResponse* exchange
- re-enrollment
- *getCACert* message
- *csrattrs* message
- CSR attribute request and response handling

Remarks: The requirement applies to asymmetric keys used on the device, including:

- Keys used for authentication and communication security, e.g., in TLS or IPsec
- Public keys and certificates used to verify digital signatures on firmware images

- Root certificates

IEC 62351-9 [21] requires that the Registration Authority (RA) and Certificate Authority (CA) support both SCEP and EST. So, a device that supports one of the protocols should be interoperable with them.

The requirements for the EST protocol are based on those in Section 8.1.7 of IEC 62351-9 [21]. The requirements for the SCEP protocol are chosen to provide similar functionality.

The device should generate its own private keys using a cryptographic (pseudo-)random number generator (see C.10.1.1 in [23]).

To support automated enrollment, the device should be configured to automatically connect to a commissioning server during manufacturing. The device should be able to check the identity of the commissioning server.

C.10.1.6 Initial authentication for enrollment

The device should be configured to use authentication during commissioning. During manufacturing, the vendor should install on the device means to uniquely identify and authenticate itself. The device vendor should send the information needed to check the identification and authentication to the grid operator in a secure way.

Remarks: The device can be uniquely identified through:

- a unique name in the Common Name of an initial certificate from the vendor's CA
- a certificate serial number in an initial certificate from the vendor's CA
- the fingerprint of an initial certificate (self-signed or from the vendor's CA)
- a unique username for EST

With SCEP and EST, the device can authenticate using the following mechanisms:

- through a one-time password (the challenge password for SCEP or a password used in HTTP Basic or Digest authentication for EST)
- by signing the Certificate Signing Request (CSR) with its private key
- through a TLS client-side certificate for EST

All these mechanisms are allowed.

Grid operators should check the identity of a device when it tries to enroll to ensure that certificates are not given to unauthorized parties. They should load the identification and authentication information from the vendor into their RA before devices are installed.

C.10.1.7 Certification revocation lists

The device shall support certificate revocation through one of the following methods:

- Certificate Revocation Lists (CRLs, RFC 5280 [24]) downloaded via SCEP, LDAP(S), or HTTP(S)
- Online Certificate Status Protocol (OCSP, RFC 6960 [25])

Remark: Certificate Revocation Lists are public information whose integrity is protected by a signature from the certificate authority. So, they may be transported over insecure channels such a LDAP or HTTP.

4.5 Communication between devices at different locations

Some grid operators need to allow direct communication between medium voltage RTUs, for instance in use cases involving automatic reclosers or self-restoration of the grid. This section contains security requirements to securely implement such communication.

C.9.2.1 Least privileges between devices at different locations

If the device supports direct communication with other devices, the device shall restrict the privileges of other devices, so that they can access only the functions and data they need.

Remark: Direct communication between devices is needed for instance in use cases involving automatic reclosers or self-restoration of the grid. Only the measurements required for the use case should be shared and only the commands in the scope of the use case should be allowed. If the device only communicates with the central system, the requirement does not apply.

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

C.9.4.3 Machine-to-machine authentication between devices at different locations

If the device supports direct communication with other devices, the devices shall support mutual authentication to access each other.

Remark: If the device only communicates with the central system, the requirement does not apply.

C.13.1.3 Restrict direct communication between devices

If the device supports direct communication with other devices, it shall be able to restrict the communication to what is needed.

Remark: In most cases, direct communication between devices should be blocked, and devices should only communicate with the central systems. But if the distribution automation system supports use cases involving automatic reclosers or self-restoration of

the grid, direct communication between devices may be needed. In those cases, communication should usually be restricted to devices on the same MV line, and the needed protocols and ports.

Appendix A: Mapping to IEC 62351

The table below shows how some of the requirements can be implemented through compliance with the IEC 62351 standard.

Requirement	IEC 62351 part	Implementation
C.9.2.3	IEC 62351-8 [5]	A set of roles and privileges and two methods (PUSH and PULL) to authenticate users through a central server are defined
C.9.4.1	IEC 62351-3 [11] IEC 62351-5 [12]	Authentication using TLS with client-side certificates is specified
C.10.1.3	IEC 62351-9 [9]	Different methods for key management on devices, including the SCEP and EST protocols are specified.
C.13.1.1	IEC 62351-3 [11] IEC 62351-5 [12]	Communication security using TLS and an application layer method is specified. (Using TLS is recommended.)

Glossary

APN	Access Point Name
CVSS	Common Vulnerability Scoring System
EST	Enrollment over Secure Transport
ISMS	Information Security Management System
MV	Medium Voltage
PKI	Public Key Infrastructure
RADIUS	Remote Access Dial-In User Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SIEM	Security Incident and Event Management
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network

References

[1] ENCS, "SA-111-2022: Security threat analysis for substation automation systems," 2022.

[2] ENCS, "SA-201-2022: Security architecture for substation automation systems," 2022.

[3] ENCS, "Market survey for distribution automation systems," 2019.

[4] ENCS, "DA-101-2019: Security risk assessment for distribution automation," 2019.

[5] IEC, "IEC 62351-8: Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control," 2020.

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

[7] Internet Engineering Task Force (IETF), "RFC 8894: Simple Certificate Enrolment Protocol," 2020.

[8] IETF, "RFC 7030: Enrollment over Secure Transport," 2013.

[9] IEC, "IEC 62351-9:2017: Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment," 2017.

[10] IETF, "RFC 5424: The syslog protocol," 2009.

[11] IEC, "IEC 62351-3:2014: Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP," 2014.

[12] IEC, "IEC 62351-5-7:2013: Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)," 2013.

[13] 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].

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

[15] ENCS, "DA/SA-401-2021: Security test plan for RTUs and gateways," 2021.

[16] OWASP Foundation, "OWASP Top Ten," [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed 2 12 2020].

[17] OWASP Foundation, "OWASP Web Security Testing Guide," [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/. [Accessed 2 12 2020].

[18] ENCS, "DA-201-2021: Security architecture for distribution automation systems," 2021.

[19] ENCS, "WP-023-2020: Protecting distribution automation systems against physical attacks," 2020.

[20] ENCS, "WP-032-2020: Centralized access control for field devices," 2020.

[21] IEC, "IEC 62351-9:2917: Power systems management and associated information exchange - Data and Communications security - Part 9: Cyber security key management for power systems equipment," 2017.

[22] Internet Engineering Task Force (IETF), "Enrollment over Secure Transport," 2013.

[23] ENCS, "DA/SA-301-2021: Security requirements for procuring RTUs and gateways," 2021.

[24] Internet Engineering Task Force (IETF), "RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," 2008.

[25] Internet Engineering Task Force (IETF), "RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," 2013.