Annex No. 6 – Security Requirements for Remote Reading Meters

1. Security in the Smart Meter Life Cycle

SLC-1.1	Certified Security Management System
Description	The Manufacturer must possess and maintain an Information Security Management System certified for compliance with the ISO/IEC 27001 standard. The scope of certification must explicitly cover the processes of design, software development, production, initialization (secure provisioning), and maintenance of the devices.
Rationale	The ISO/IEC 27001 certificate is formal, internationally recognized proof that the manufacturer applies best practices in information security management. This requirement ensures that security is an integral part of the entire organization and all processes related to the product, not just a feature of the device itself. By covering the entire life cycle, from design to maintenance, the risk of vulnerabilities occurring at any stage is minimized.
Fit criterion	The Manufacturer will present a valid ISO/IEC 27001 certificate issued by an accredited certification body. The scope of certification (Statement of Applicability) must unambiguously confirm coverage of all listed processes: design, development, production, and maintenance of AMI devices.

SLC-1.2	Documented and Verifiable Secure Software Development Life Cycle
Description	The Manufacturer must possess and apply a documented, Secure Software Development Life Cycle (SDLC). This process must include at least: static and dynamic code analysis, software component management (e.g., via Software Bill of Materials - SBOM), and a formal vulnerability management process. All documentation must be available for verification. Each version of software and firmware must be uniquely identifiable (e.g., by version number and release date), and each software image should possess a unique cryptographic hash value.
Rationale	Security "by design" is a fundamental principle of modern cybersecurity. The requirement to possess and apply an SDLC shifts the responsibility for security to the earliest stage—the design and creation of software. This ensures that security gaps are identified and eliminated before the product reaches the

	market, rather than only during the operational phase.
Fit criterion	The Manufacturer will present documentation describing the SDLC process. The documentation will contain a description of the tools used (SAST, DAST), dependency management procedures (SBOM), the vulnerability response policy, and the method of identification and versioning of components (along with examples of version markings and hashes). Reports from SAST/DAST tools and the SBOM document for the delivered software will be presented.

SLC-1.3	**Secure Software Engineering Practices**
Description	The software development process must be based on recognized secure coding standards (e.g., CERT C, MISRA C 2023). The Manufacturer must use tools for static (SAST) and dynamic (DAST) code analysis to eliminate vulnerabilities and maintain a secure configuration management and software versioning system.
Rationale	Security "by design" is a fundamental principle of modern cybersecurity, required by EU regulations such as the Cyber Resilience Act. The use of SAST and DAST tools allows for the automatic detection of common programming errors and vulnerabilities at an early stage of development, significantly reducing the costs of fixing them and the risk of their exploitation in a production environment. Secure version management is key to ensuring software integrity and traceability.
Fit criterion	The Manufacturer will present documentation describing the secure software development process (SDLC). The documentation will contain a description of the applied coding standards, tools (SAST, DAST), and configuration management procedures. Anonymized reports from SAST/DAST tools confirming their practical application will be presented.

SLC-1.4	**Component Supply Chain Management**
Description	The Manufacturer must apply a documented process for the assessment and qualification of external components (hardware and software). Components may be used only if their origin and integrity are confirmed (e.g., digital signature, supplier certificate, verified repository, traceability of hardware components).

Rationale	Modern devices consist of many components from different suppliers, creating a complex supply chain. An attack on this chain is one of the most serious threats. This requirement, emphasized in the NIS2 Directive, forces the manufacturer to take responsibility for the security of the entire product, not just the parts they produced themselves. The use of, for example, a Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) is a good practice in this regard.
Fit criterion	The Manufacturer will present a documented procedure for the assessment and qualification of suppliers and third-party components (software and hardware). The procedure must describe the method of verifying integrity (e.g., checking checksums, digital signatures, supplier certificates, traceability of hardware components) and authenticity of components. Upon request, the manufacturer will make available a list of third-party components (SBOM and HBOM) along with evidence of their verification.

SLC-1.5	**Auditability of Manufacturer Security Processes**
Description	The device Manufacturer agrees to a periodic audit of their organization's security processes.
Rationale	Ensuring the security of AMI infrastructure is a shared responsibility of the manufacturer and the operator. For the DSO to effectively manage risk throughout the system life cycle, they must have the ability to verify whether the security processes declared by the manufacturer are actually and consistently applied. This requirement formalizes the DSO's right to conduct audits, which is standard practice in supply chain security management for critical infrastructure.
Fit criterion	Within the contract, the Manufacturer will guarantee the DSO (or an authorized third party designated by them) the right to conduct periodic audits of the security processes listed in requirements SLC-1.1, SLC-1.2, SLC-1.3, SLC-1.4, and SLC-5.1. The scope and frequency of audits will be defined in the contract, and their purpose will be to verify the compliance of actually applied practices with the presented documentation.

SLC-2.1	**Trusted Hardware Module and Secure Boot**
Description	The device must be equipped with a secure boot mechanism that prevents the

	system from starting with unauthorized software. Verification of software integrity and authenticity must take place using a built-in, trusted hardware element storing the manufacturer's key.
Rationale	Software modification is one of the most serious attack vectors. Secure boot implemented in hardware guarantees that only authentic software signed by the manufacturer is run on the device. This protects against the installation of malicious code that could manipulate measurement data or disrupt network operation.
Fit criterion	The device boot process will fail (e.g., the device enters an error state and does not launch the main application) if any part of the software (firmware, bootloader, operating system, application) does not successfully pass digital signature verification. An attempt to run an unsigned software image must be blocked. The event of a failed boot will be recorded in the event log (e.g., using the bootloader mechanism).

SLC-3.1	**Authentication and Verification of Update Integrity**
Description	Every update package (firmware) must be digitally signed by the manufacturer. The device must strictly verify this signature before beginning installation. Updates without a valid digital signature must be rejected. The device firmware update process may be initiated only by an authenticated account assigned a role with administrative privileges (e.g., management association).
Rationale	The remote update process, while necessary to maintain security, creates a risk of uploading malicious software. The requirement for digital signature verification guarantees that the device accepts updates originating exclusively from an authorized source (the manufacturer). At the same time, limiting the ability to initiate updates to the administrator role (e.g., management association) prevents unauthorized attempts to upload software, even if an attacker manages to bypass other defenses.
Fit criterion	The device will reject and not install an update package whose digital signature is invalid, damaged, or comes from an untrusted digital signature issuer. The event of failed verification will be recorded in the security event log. Initiating an update will be possible only from an account with a role possessing administrative privileges (e.g., management association).

SLC-3.2	Protection against Version Rollback
Description	The device must implement a mechanism preventing the installation of a software version older than the one currently installed.
Rationale	Attackers may attempt to install an older software version containing a known and already patched vulnerability in order to exploit it. The anti-rollback protection mechanism blocks this attack vector, ensuring that the software version running on the device is always at least as secure as the previous one.
Fit criterion	An attempt to install an update package with a version number lower than the version currently running on the device will be rejected. The device will record this event in the security event log.

SLC-3.3	Safe Fallback after Failed Update
Description	In the event of a failed software update (e.g., due to transmission error, power loss), the device must be able to automatically return to the last known, stable software version.
Rationale	The update process is a critical operation. An error during this process cannot lead to permanent damage to the device. The safe return mechanism (so-called "fallback" or "rollback") ensures business continuity and system resilience to unforeseen problems, which is key in infrastructure with a long life cycle.
Fit criterion	Simulation of a failed update (e.g., by interrupting power during it) must cause the device, upon restart, to automatically restore the previous software version, report an update error, and continue normal operation. The device will record this event in the event log.

SLC-3.4	Scope of Software Updates
Description	The device must have the assured capability to update key software components, both locally and remotely.
Rationale	Ensuring the ability to update key software components is the foundation of long-term security. It enables responding to newly discovered vulnerabilities and adapting to changing standards (e.g., cryptographic). This requirement specifies which elements must strictly be updatable to avoid a situation where a critical

	security gap cannot be patched remotely.
Fit criterion	The Manufacturer must ensure the capability for remote updates of all key device firmware components, including at least: the operating system, cryptographic libraries, communication stack, and application logic responsible for security functions. The software architecture documentation must unambiguously indicate a modular structure enabling the replacement of these components.

SLC-4.1	**Documented Vulnerability Management Process**
Description	The Manufacturer must implement and maintain a formal vulnerability management process, compliant with standards such as ISO/IEC 29147 and ISO/IEC 30111, throughout the entire defined technical support period of the device. The process must include proactive monitoring of components for newly discovered flaws, risk assessment, and timely delivery of security patches according to defined timeframes.
Rationale	No software is free of bugs, and new vulnerabilities are discovered continuously. Possessing a formalized proactive response process is key to maintaining security throughout the long life cycle of the meter. This is a fundamental requirement of the EU Cyber Resilience Act (CRA). It ensures that detected gaps will be systematically analyzed and patched within a predictable and contractually guaranteed time.
Fit criterion	The Manufacturer will present a publicly available Vulnerability Disclosure Policy and an internal vulnerability management procedure. The procedure must define timeframes (SLA) for delivering patches depending on the criticality level of the flaw (e.g., based on CVSS).

SLC-5.1	**Secure Production Environment and Initialization**
Description	The device initialization process (provisioning), including the injection of unique cryptographic credentials, must take place in a physically and logically secured, controlled, and auditable production environment.
Rationale	Initialization is the moment when the device is given its unique digital identity (keys, certificates). Compromise of this process could lead to device cloning or

	theft of master keys, undermining the security of the entire system.
Fit criterion	The Manufacturer will present evidence of securing the production environment, e.g., within the framework of ISO/IEC 27001 certification (in accordance with SLC-1.1). The documentation must describe physical and logical access control measures to the production line and audit procedures for the credential injection process. It must be possible to trace what credentials were injected into a given device and when.

SLC-6.1	**Future-Proof Design**
Description	The device must possess sufficient reserves of computing power and memory to enable future updates of cryptographic algorithms and communication protocols to newer, more secure versions without the need for physical hardware replacement.
Rationale	The life cycle of a meter is 15-20 years. During this time, current cryptographic standards may prove insufficient. Ensuring hardware reserves allows for remotely raising the security level in the future and prevents the accumulation of technical debt.
Fit criterion	The technical documentation of the device must demonstrate that: • the device possesses sufficient hardware resources and software architecture enabling the implementation of cryptographic algorithms and communication protocols corresponding to higher security levels in the future (e.g., transition from SL1 – 128-bit, to SL2 – 256-bit), • the software architecture is modular, enabling the replacement of cryptographic libraries and update of algorithms without the need to replace hardware, • the manufacturer provides evidence (e.g., performance tests or declarations) confirming that higher-level algorithms can be supported in the device's normal operating mode.

2. Strong Cryptography

CRY-1.1	**Approved Cryptographic Algorithms**
Description	It is permitted to use only publicly known, proven, and considered secure at the

	time of delivery cryptographic algorithms.
Rationale	The requirement to rely on recognized international standards ensures that the applied mechanisms are resistant to known attacks and have been thoroughly analyzed by the cryptographic community. Minimum requirements: • symmetric encryption – e.g., AES-128 bit, • public key cryptography – e.g., ECC with 256-bit key, • hash functions – e.g., SHA-256.
Fit criterion	Documentation analysis and communication tests will show that for the realization of security functions (encryption, signatures), the device utilizes only algorithms and parameters (key lengths, curves) compliant with the given specification.

CRY-1.2	**Upgradability of Cryptographic Mechanisms**
Description	The software architecture must enable the future update or replacement of cryptographic libraries and algorithms with newer, more secure versions via remote and local software updates.
Rationale	This is an extension of requirement SLC-6.1 ("Future-Proof Design"). In the perspective of 15-20 years of meter operation, currently used cryptographic algorithms may be deemed insecure. The ability to update them remotely and locally is key to maintaining long-term security.
Fit criterion	The software architecture documentation must demonstrate that cryptographic functions are implemented in the form of separate, replaceable modules/libraries. The Manufacturer must demonstrate (e.g., in a test environment) the ability to perform an update that raises the version of the cryptographic library used.

CRY-2.1	**Cryptographically Secure Random Number Generator**
Description	The device must be equipped with a cryptographically secure random number generator, which is the source of entropy for all cryptographic operations.

Rationale	The quality and unpredictability of random numbers is the foundation of security for all cryptographic operations, such as key generation or creation of initialization vectors. Using a weak generator renders even the strongest algorithms useless.
Fit criterion	The Manufacturer will provide design documentation confirming the implementation of a Cryptographically Secure Random Number Generator compliant with current standards (e.g., NIST SP 800-90A or BSI AIS 20/31). Statistical tests on a sample of numbers generated by the device will confirm their high quality (entropy).

CRY-3.1	**Uniqueness of Cryptographic Keys for the Device**
Description	Each meter must possess its own unique set of cryptographic keys. It is forbidden to use default keys, shared keys for a group of devices (group keys), or keys generated in a predictable manner.
Rationale	Using the same keys in multiple devices creates a huge systemic risk – compromise of one device leads to the compromise of the entire group. Unique keys for each meter ensure that the consequences of a potential security breach are limited to only one device.
Fit criterion	Analysis of digital certificates (or public keys) obtained from at least two different devices must show that they are unique. The Manufacturer must provide evidence within the production process (provisioning) audit that each device is initialized with a unique set of cryptographic keys, including a unique Master Key. It will be demonstrated that keys are not simply generated from publicly known identifiers (e.g., serial number), which could make them predictable.

CRY-3.2	**Key Life Cycle Management**
Description	The device must support cooperation within the full key life cycle, including their secure generation, distribution, storage, remote and local rotation (replacement), and secure deletion. All temporary keys must be deleted after use. Cooperation within the key life cycle must be executable by functionalities built into the meter or other applications for handling and cooperating with the device (KMS class).
Rationale	Cryptographic keys should be regularly changed (rotated) to limit the time an

	attacker could use them in case of theft. The device must possess secure, automated mechanisms for key management throughout its entire operation period.
Fit criterion	The device must make available secure functions (e.g., within the DLMS/COSEM protocol) allowing an authorized administrator to remotely and safely replace (rotate) session and application keys. After completion of a cryptographic operation, temporary keys will be overwritten in memory.

CRY-3.3	**Support for External Key Management Systems**
Description	The device must support standard protocols (e.g., SCEP, EST) enabling secure integration with external Key Management Systems (KMS). There must be a possibility to remotely initiate key life cycle operations (e.g., generating a new key pair, request for certificate signing, installation of a new certificate) by an authorized central system.
Rationale	At a large scale, manual key management is impractical and error-prone. Integration with a KMS system allows for automation and enforcement of a consistent security policy regarding the key life cycle (rotation, revocation) throughout the DSO infrastructure.
Fit criterion	The Manufacturer will document the supported protocols and standards for integration with KMS-class systems. Functional tests will be conducted confirming that the device is capable of correctly processing a certificate renewal request initiated by the central system, generating a new key pair and a Certificate Signing Request (CSR).

CRY-4.1	**Hardware Protection of Critical Keys**
Description	The device's private keys and any master keys must be generated, stored, and utilized within a hardware-protected, isolated environment (e.g., Secure Element, Trusted Execution Environment), which prevents their reading or copying in plain text.
Rationale	Private and master keys are the device's most critical secrets. Their compromise allows for impersonating the device or decrypting communication. Hardware isolation ensures that keys never leave the secure environment in plain text, significantly raising resistance to both logical and physical attacks.
Fit criterion	It will be demonstrated (e.g., via design documentation analysis and penetration tests) that no programming function (API) or physical interface exists that would

	allow for the direct reading or export of private/master keys from the protected environment. Cryptographic operations utilizing these keys (e.g., signing) must be performed inside this environment.

CRY-5.1	Digital Identity Based on Certificates
Description	A remote reading meter, when performing functions of a device communicating with a central system, must possess a unique digital identity represented by a digital certificate (e.g., in the X.509 standard), issued by a trusted Certificate Authority (CA) within a Public Key Infrastructure (PKI) dedicated to AMI.
Rationale	In a system comprising millions of devices, digital certificates are the only scalable and reliable way to manage identity and build trust. This requirement is fundamental – it establishes that each device is a unique, cryptographically verifiable unit. This is a necessary condition for fulfilling procedural requirements, such as COM-2.1, which defines how this identity is used for mutual authentication of the communication channel (e.g., within a TLS session). They allow for strong, mutual authentication between the meter and the central system, which is the foundation of secure communication and prevents Man-in-the-Middle attacks.
Fit criterion	Each device is factory-equipped with a unique certificate (e.g., X.509), signed by a trusted certification authority. The device uses this certificate to authenticate itself to the central system (e.g., during TLS session establishment).

3. Communication Security

COM-1.1	End-to-End Security at the Application Layer
Description	Communication between the meter and the central system must be secured at the application layer level (e.g., using DLMS/COSEM Security Suite 1 or 2), ensuring confidentiality and integrity of data along the entire path, regardless of security measures applied in lower network layers.
Rationale	Security measures at lower layers (e.g., in the cellular network) may be insufficient or outside the operator's control. Encryption at the application level guarantees that data is protected from the moment it leaves the meter until it reaches the central system, and no intermediate systems (e.g., concentrators) have access to it in plain text.

Fit criterion	Network traffic analysis will show that the content of the application protocol (e.g., DLMS) is encrypted, even if communication takes place inside a VPN/IPsec tunnel.

COM-2.1	**Mutual Authentication of the Communication Channel**
Description	Every communication session with the central system must be preceded by strong, mutual authentication of both parties, based on digital certificates (e.g., X.509).
Rationale	Encryption alone is not sufficient security. It is necessary for both parties of the communication to be certain of their interlocutor's identity. Mutual authentication using certificates prevents an attacker from impersonating the system or the device.
Fit criterion	Establishment of a communication session (e.g., TLS) will succeed only if the server presents a valid certificate trusted by the device (e.g., router, meter), and the device presents a valid certificate trusted by the server. An attempt to establish a connection with a server possessing an invalid certificate will be rejected and noted in the event log.

COM-3.1	**Protection against Replay Attacks**
Description	The communication protocol must implement a mechanism for protection against replay attacks, e.g., by using unique, incrementing sequence numbers in messages or one-time cryptographic values (nonces).
Rationale	A replay attack involves intercepting and resending a legitimate message to trigger an unwanted action. Effective protection against such attacks is key to ensuring the integrity and non-repudiation of operations.
Fit criterion	Interception and resending of the same, cryptographically valid message to the device must be rejected by it. The event of rejecting a repeated message will be recorded in the event log.

COM-3.2	Command Validation
Description	The device must validate all received data and commands for their syntactic and semantic correctness. Improper or unknown commands must be ignored or rejected.
Rationale	Sending incorrectly formatted or unexpected data to the device (fuzzing) is a popular technique for finding vulnerabilities in software. Rigorous validation of all input data protects against buffer overflow attacks and other parsing errors that could lead to instability or device compromise.
Fit criterion	Sending a series of deliberately distorted or syntactically incorrect commands (fuzzing) to the device cannot cause its failure, restart, or transition into an unsafe state. The device must reject such commands and continue normal operation.

4. Access Control

ACC-1.1	Authentication Requirement for All Interfaces
Description	Access to all device access interfaces (remote WAN and local, e.g., optical port) must be strictly preceded by a successful strong authentication process. Anonymous access is not permitted, with the exception of the interface used for communication with the home network infrastructure.
Rationale	Every access interface without authentication constitutes an open gate for potential attackers. The requirement for strong authentication at every access point is a basic security principle ensuring that only authorized entities can interact with the device.
Fit criterion	An attempt to execute any operation (beyond basic identification) on any access interface without prior successful authentication must be rejected by the device.

ACC-2.1	Protection against Brute-Force Attacks
Description	Access interfaces must implement a protection mechanism against brute-force attacks, consisting of temporarily blocking access after exceeding a defined, configurable number of failed login attempts. The event must be logged.

Rationale	Brute-force attacks, involving attempts to guess a password or key, are a common threat. The mechanism of a temporary lockout significantly slows down and complicates such an attack, increasing its cost and the likelihood of detection.
Fit criterion	After exceeding the configured number of failed authentication attempts on a given interface, the device must stop responding to subsequent attempts for a defined period. Each failed attempt must be recorded in the event log.

ACC-3.1	**Implementation of Privilege Separation Model**
Description	The device must implement a granular access control model based on roles (e.g., RBAC), or an equivalent privilege separation mechanism. Each authenticated identity must be assigned a uniquely defined set of permissions, consistent with the principle of least privilege.
Rationale	Assigning permissions to individual users is inefficient and error-prone. The application of an organized permission model – e.g., based on roles, access levels, or function groups – enables logical grouping of privileges, simplifies management, and ensures the application of the principle of least privilege. Each level or role has access only to functions necessary to perform assigned tasks.
Fit criterion	An authenticated user may execute only operations allowed within the scope of permissions assigned to them (e.g., role, access level, or function profile). An attempt to execute an operation exceeding this scope must be rejected and registered in the event log.

ACC-3.2	**Minimum Set of Privilege Levels**
Description	The device must support at least three predefined distinct privilege levels or predefined equivalent user roles: • administrative (full access, configuration, updates), • service (diagnostics, technical parameters, without critical configuration changes), • end-user (read-only measurement data).
Rationale	Standardizing the minimum set of access levels or user roles increases interoperability and enables consistent permission management across the entire AMI system. Such a distinction reflects typical participants in interaction with the

	meter (administrator, service technician, end-user) and supports the enforcement of the principle of least privilege. In the case of devices without a full role model, functional separation of these levels can be realized through alternative mechanisms (e.g., access levels, service keys, function profiles, or authorization on the side of the higher-level system).
Fit criterion	The device documentation must describe the implemented privilege levels, roles, or other authorization mechanisms and the functions assigned to them. Functional tests must confirm that: • the device distinguishes at least three access levels or equivalent user profiles, • each level possesses a scope of permissions consistent with the description, • attempts to execute operations exceeding the assigned level are rejected and registered in the event log.

ACC-3.3	**User Account Documentation**
Description	All user accounts implemented in the meter, including service accounts, must be documented and presented in the device specification.
Rationale	Hidden or undocumented accounts pose a serious security risk. The requirement for full documentation of all accounts ensures transparency and allows auditors to verify that no unauthorized access points exist.
Fit criterion	The list of user accounts obtained from the device (e.g., via the administrative interface) must be 100% consistent with the list presented in the product's technical documentation.

ACC-4.1	**Attack Surface Minimization**
Description	All physical ports, network protocols, and software services that are unused and unnecessary from the functional point of view must be disabled by default.
Rationale	Every active service or open port constitutes a potential entry point for an attacker (so-called attack surface). Minimizing this surface by disabling everything not absolutely necessary for operation is one of the basic principles of system hardening.

Fit criterion	Port scanning and analysis of the device configuration in the factory state must show that only those services and ports defined as necessary in the product documentation are active.

ACC-4.2	**Possibility to Deactivate Interfaces**
Description	The Operator must have the ability to remotely and locally deactivate individual communication interfaces for a defined period of time.
Rationale	Possessing the ability to dynamically enable and disable interfaces gives the operator flexibility in security management. In the event of detecting a threat or lack of business need, a given interface (e.g., HAN for the consumer) may be temporarily disabled, which further reduces the attack surface.
Fit criterion	An authorized administrator must be able to disable and then re-enable a selected communication interface using a remote or local command. The interface state (active/inactive) must be correctly reported by the device.

ACC-4.3	**Permanent Disabling of Debug Interfaces**
Description	All physical and logical developer and diagnostic interfaces (e.g., JTAG, serial ports with access to system shell) must be permanently and irreversibly disabled in devices intended for operation.
Rationale	Debug interfaces give almost unlimited access to the interior of the device and allow for bypassing most security measures. Leaving them in the production version is an unacceptable risk.
Fit criterion	Physical inspection and electronic tests of the device cannot reveal the presence of active signals on pins corresponding to debug interfaces. Attempts to connect to such interfaces must result in failure.

ACC-5.1	**Password Management**
Description	Authentication to all interfaces based on passwords must meet the following requirements:

	• Factory passwords must be unique for each device and force a change upon first login. • There must be a possibility to define a password complexity policy (minimum length, required character classes) and a password aging policy (maximum validity period, password history). The definable password policy must correspond to currently applied security standards. • Passwords must be transmitted exclusively via encrypted channels. • The system cannot reveal whether a login error concerned the username or the password. • Passwords must be masked during entry. • Password change must generate an entry in the event log.
Rationale	Weak passwords or their improper storage and transmission are among the most common causes of security breaches. Introduction of comprehensive requirements regarding password management significantly raises resistance to attacks involving guessing or interception.
Fit criterion	Functional tests must confirm that: • After logging in with a default password, the system forces its change. • There is an administrative interface for configuring complexity rules. • Network traffic analysis confirms that passwords are transmitted in encrypted form. • The error message is generic (e.g., "Invalid login data"). • Characters entered in the password field are masked. • Password change is noted in the event log.

ACC-5.2	**Session Logout and Lockout Mechanisms**
Description	The device must implement a mechanism for automatic logout (or locking) of a session with elevated privileges (e.g., administrative, service) after the lapse of a configurable period of inactivity.
Rationale	Leaving an active, privileged session unattended creates a risk of its unauthorized takeover by third parties. Automatic logout after a period of inactivity is a basic remedial measure, consistent with the principle of minimizing the attack time window. It is a standard security function in mature IT/OT systems.
Fit criterion	After the lapse of the configured inactivity time on a local or remote interface, the user session must be automatically terminated. Each subsequent operation requiring privileges must require re-authentication.

5. Integrity Protection

INT-1.1	Protection of Stored Data Integrity
Description	Critical data stored in non-volatile memory (measurement data, authentication and encryption keys, logs) must be secured with cryptographic mechanisms (e.g., MAC authentication codes or checksums) in order to verify their integrity.
Rationale	Ensuring that data saved in memory has not been changed (intentionally or accidentally) is key for the credibility of the entire system. Cryptographic mechanisms, such as MAC, act like a digital seal, allowing for verification of data inviolability at any time.
Fit criterion	Deliberate modification of a block of protected data in memory (e.g., using developer tools) must be detected by the device during the next attempt to read this data. Detection of an integrity violation must be registered in the event log.

INT-1.2	Protection against Residual Information
Description	Temporary memory (e.g., buffers) used to store cryptographic keys or other sensitive data must be securely cleared (overwritten) immediately after the completion of an operation.
Rationale	Leaving sensitive data in memory after operation completion creates a risk that it may be read by later, less privileged processes. Secure memory clearing eliminates this threat.
Fit criterion	In the case where the manufacturer provides a copy of the meter with a deliberately unsecured developer interface, analysis based on a memory dump of the device after performing a cryptographic operation. Analysis cannot reveal any fragments of used session keys or other sensitive data in plain text. In the absence of the possibility for the manufacturer to provide a copy of the meter with a deliberately unsecured developer interface, analysis based on the presented SBOM and HBOM documentation in the context of applied solutions and the method of their implementation. Documented technical possibilities for implementing a protection mechanism against residual information and a written declaration by the manufacturer regarding the implementation of this mechanism must exist.

INT-2.1	Logical Separation of Functions and DoS Resilience
Description	The software architecture must ensure strong, logical separation between metrological and communication components. A DoS/DDoS attack on the communication interface cannot affect the continuity and correctness of measurement functions.
Rationale	Compromise of the communication module cannot threaten the device's primary function, i.e., energy measurement. Logical separation guarantees that even in the case of a successful attack on the network part, the metrological part remains intact and functions correctly.
Fit criterion	Conducting a DoS attack (e.g., port flooding) on the communication interface of the device cannot cause stoppage or disruption of the energy consumption measurement and registration process. After the attack ceases, communication functions must return to normal operation.

INT-2.2	Safe Fallback to Operation after Failure
Description	The device must maintain a secure state in the event of a failure (e.g., self-test error, cryptographic function error). After a failure, the device must return to the last known secure state; it cannot reveal confidential information or allow access control bypass.
Rationale	Device failure cannot create a security loophole. The "fail-secure" principle guarantees that in the event of an error, the device automatically transitions into a state of maximum security (e.g., blocks access) instead of "hanging" in an open state. Device failure cannot reveal confidential information such as cryptographic keys or authentication data. Device failure also cannot affect the security of other system elements.
Fit criterion	Simulation of a critical component failure (e.g., loss of communication with the cryptographic module) must cause the device to transition into a defined emergency state. Upon restart, the device must boot in a secure configuration, and log analysis cannot reveal the leakage of any sensitive data.

INT-2.3	Self-Testing at Startup

Description	The device must conduct self-tests of key security functions (e.g., cryptographic mechanisms, random number generator) during the boot process to verify their correct operation.
Rationale	Ensuring that basic security mechanisms work correctly at every startup is key to maintaining trust in the device. Self-tests allow for early detection of hardware failures or software damage that could weaken defenses.
Fit criterion	Intentional damage (at the software level) to one of the security modules (e.g., AES library) must be detected during the next device restart. The device must signal an error and not continue normal startup.

INT-3.1	**Detection of Case and Terminal Cover Opening**
Description	The device must be equipped with physical sensors detecting and recording at least the following events: opening of the meter case (with the exception of non-dismountable meter cases) and opening of the terminal cover. Each such event must be immediately registered and reported.
Rationale	Detection of physical interference attempts is the first line of defense against manipulation. Recording and alarming about case opening allows for a quick reaction to potential fraud or sabotage attempts.
Fit criterion	Physical opening of the terminal cover or the case must result in the immediate recording of events in the security log. These events must contain an accurate timestamp.

INT-4.1	**Magnetic Field Detection**
Description	The device must be equipped with a sensor detecting attempts at manipulation using an external magnetic field. Detection of such a field must be immediately registered and reported.
Rationale	Neodymium magnets can be used to attempt to disrupt the operation of electronic measurement components. A dedicated sensor allows for the detection of such attempts and constitutes a deterrent measure.
Fit criterion	Bringing a magnet (of defined field strength) close to the meter must cause the recording of an event in the security log and the sending of an alarm to the

	central system.

6. Logging and Auditing

LOG-1.1	Scope of Logged Security Events
Description	The device must register all events significant from a security point of view in a dedicated security event log. The minimum set of events includes: • successful and failed authentication attempts, • security configuration changes, • software updates (successful and failed), • detected physical manipulation attempts, • software integrity errors (e.g., failed secure boot), • cryptographic function errors, • system time changes, • device reset, • critical system errors.
Rationale	A complete and detailed event log is a necessary tool for monitoring the system security status, detecting anomalies and incidents, and conducting post-incident investigations. Defining a minimum, standard set of logged events ensures data consistency and utility throughout the AMI system.
Fit criterion	Execution of each of the operations listed in the description (e.g., failed login, firmware update) must result in the appearance of a corresponding, detailed entry in the event log.

LOG-1.2	Detail of Log Entry
Description	Each entry in the event log must contain at least: • accurate timestamp, • event type, • identifier of the entity initiating the event (if applicable), • result of the operation (success/failure) (if applicable), • interface where the event took place (if applicable).
Rationale	For logs to be useful, they must contain sufficient context information. Defining a minimum set of attributes for each entry guarantees that registered events will be understandable and possible to correlate during analysis.

Fit criterion	Analysis of entries in the event log must confirm that each of them contains all required fields, and their content is consistent with the actually performed operation.

LOG-2.1	**Protection of Event Log against Modification**
Description	The event log must be protected against unauthorized modification and deletion. Only adding new entries should be possible. An attempt to modify or delete existing entries must be blocked and itself registered as a security event (if technically possible).
Rationale	The credibility of the event log depends on its integrity. Attackers often try to cover their tracks by modifying or deleting logs. A "write-only" (or "append-only") mechanism is a basic protection measure, ensuring that the event history remains intact.
Fit criterion	An attempt to modify or delete an entry in the memory where the event log is stored must be detected by the device's integrity mechanisms. No API function allowing for editing an existing entry can exist.

LOG-2.2	**Authorized Access to Event Log**
Description	Access to read, modify, and delete entries in the event log must be controlled and restricted to authorized roles (in accordance with the privilege separation model).
Rationale	Although modification of individual entries is forbidden (LOG-2.1), there may be legitimate administrative operations, such as clearing the entire log during service. This requirement ensures that such operations can be performed only by the most privileged roles and that this action itself is also registered.
Fit criterion	A user with a role of lower privileges cannot have access to the function of reading or clearing the security log. An attempt to execute such an operation must be blocked and registered.

LOG-3.1	**Capacity and Management of Event Log**

Description	The device must possess non-volatile memory sufficient to store a configurable, specified minimum of recent security events. After the buffer is full, the oldest entries must be overwritten by the newest ones (FIFO mechanism - First-In, First-Out).
Rationale	Ensuring appropriate log capacity is key for the ability to analyze events from a reasonable period. The circular buffer mechanism is a standard and secure method of managing limited memory, guaranteeing that the newest events are always available.
Fit criterion	After generating security events that exceed the minimum configured quantity, the oldest (first) event must be overwritten, and the log must contain the minimum number of newest events specified in the configuration.

LOG-4.1	**Time Synchronization**
Description	The device must implement a secure time synchronization mechanism (e.g., using DLMS/COSEM messages) to ensure the accuracy and credibility of timestamps in all event logs.
Rationale	Accurate and synchronized timestamps are necessary for correlating events between different devices and systems during incident analysis. Unreliable time prevents the reconstruction of the attack chronology.
Fit criterion	The device must reject time setting attempts originating from unauthenticated sources. Changing the system time must be possible only for authorized roles and must be registered in the event log (successful or failed). Tests will show that the device maintains correct time in accordance with the configured, trusted source.

LOG-5.1	**Alerting on Critical Events**
Description	Selected, critical security events (e.g., detection of physical manipulation, multiple failed logins) must cause the sending of an alarm message.
Rationale	Logging events alone is not enough; in the case of critical incidents, an immediate reaction is necessary. The alerting mechanism ensures that the system operator is immediately informed of potential threats, allowing for

	appropriate actions to be taken.
Fit criterion	Triggering an event defined as critical (e.g., case opening) must result not only in a log entry but also in the immediate initiation of sending an appropriate alarm message to the HES system.

7. Physical Security

PHY-1.1	**Possibility of Sealing**
Description	The meter case and terminal cover must be constructed in a way that enables their sealing. The construction must prevent access to the interior of the device or the terminals without breaking or visibly damaging the seal.
Rationale	A seal is a basic, visual deterrent and evidentiary measure indicating an attempt at unauthorized physical interference. This is a fundamental physical security requirement.
Fit criterion	Physical inspection of the device must confirm the existence of dedicated points for applying seals. An attempt to remove the case or terminal cover without removing the seal must be impossible without its visible destruction.

PHY-2.1	**Protection of Local Service Ports**
Description	Physical service ports, with the exception of the optical port, must be placed in a location that requires the removal of a sealed cover (e.g., terminal cover) to gain access to them.
Rationale	Service ports constitute a potential attack vector. Placing them behind a sealed cover ensures that access to them is possible only for authorized personnel and every such intervention leaves a physical trace (broken seal). The optical port, due to operational practices related to its use, may not be covered by this additional protection.
Fit criterion	Physical inspection of the device must confirm that all physical service ports, with the exception of the optical port, are not accessible from the outside without prior removal of the terminal cover.

PHY-3.1	Casing Resilience
Description	The device casing must provide protection against basic attempts at forcible interference and meet appropriate standards regarding electrical devices in terms of protection against environmental factors.
Rationale	The casing constitutes the first physical barrier protecting sensitive electronic components inside the meter. It must be sufficiently robust to hinder simple, forcible attempts to access the interior.
Fit criterion	Product documentation must confirm compliance with appropriate standards (e.g., regarding IP and IK protection ratings). Visual inspection must confirm the robustness of the construction and lack of obvious weaknesses.

Abbreviation Dictionary

Abbreviation	English Name
Standards, norms, certifications	
ISO/IEC 27001	Information Security Management System
ISO/IEC 29147	Vulnerability Disclosure
ISO/IEC 30111	Vulnerability Handling Processes
NIST SP 800-90A	Recommendation for Random Number Generation
BSI AIS 20/31	Requirements for Random Number Generators
IP / IK	Ingress Protection / Impact Protection
Models, processes and methodology	
SDLC	Secure Software Development Life Cycle
SAST	Static Application Security Testing
DAST	Dynamic Application Security Testing
SBOM	Software Bill of Materials
HBOM	Hardware Bill of Materials
SLA	Service Level Agreement
CRA	Cyber Resilience Act
DoS / DDoS	Denial of Service / Distributed Denial of Service
FIFO	First-In, First-Out
CSR	Certificate Signing Request
RBAC	Role-Based Access Control
KMS	Key Management System
Security and cryptography	

AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
SHA-256	Secure Hash Algorithm
MAC	Message Authentication Code
TLS	Transport Layer Security
VPN	Virtual Private Network
IPsec	Internet Protocol Security
PKI	Public Key Infrastructure
CA	Certificate Authority
X.509	Standard X.509
SE	Secure Element
TEE	Trusted Execution Environment
TRNG / CSPRNG	True / Cryptographically Secure Random Number Generator
Communication and protocols	
DLMS/COSEM	Device Language Message Specification / Companion Specification for Energy Metering
PLC	Power Line Communication
M-Bus	Meter-Bus
HES	Head-End System
WAN	Wide Area Network
HAN	Home Area Network
NTP	Network Time Protocol
SCEP	Simple Certificate Enrollment Protocol
EST	Enrollment over Secure Transport

Energy infrastructure and meter systems	
AMI	Advanced Metering Infrastructure
OSD	Distribution System Operator
HES	Head-End System
Organizations and regulations	
NIS2	Network and Information Security Directive 2
BSI	German Federal Office for Information Security
NIST	National Institute of Standards and Technology