Annex No. 6 - Security Requirements for Smart Meters.

1. Security in the Smart Meter Lifecycle

SLC-1.1	Certified Information Security Management System
requirement description	The Manufacturer and the Contractor (Supplier) shall maintain an Information Security Management System (ISMS) certified to ISO/IEC 27001. For the Manufacturer, the scope of certification shall explicitly cover the processes of design, software development, production, initialisation (provisioning) and maintenance of the devices. For the Contractor (where it is not the Manufacturer), the scope shall cover logistics, secure delivery and AMI system configuration processes.
rationale	The ISO/IEC 27001 certificate is formal, internationally recognised evidence that the Manufacturer and the Contractor apply security best practice in information security management. This requirement ensures that security is an integral part of the entire organisation and of all product-related processes, not merely a feature of the device itself. By covering the whole lifecycle – from design to maintenance – it minimises the risk of vulnerabilities being introduced at any stage.
verification criterion	Presentation of a valid ISO/IEC 27001 certificate issued by an accredited certification body. The Statement of Applicability shall unambiguously confirm that all listed processes (design, development, production and maintenance of AMI devices) relevant to the role of the given entity in the AMI project are covered.

SLC-1.2	Documented and Auditable Secure Software Development Lifecycle
requirement description	The Manufacturer shall maintain and apply a documented Secure Software Development Lifecycle (SSDLC). The process shall include, at minimum: static and dynamic code analysis, management of software components (e.g. by means of a Software Bill of Materials – SBOM) and a formal vulnerability management process. All related documentation shall be available for verification. Every version of the software and firmware shall be uniquely identifiable (e.g. by version number and release date), and every software image shall carry a unique cryptographic hash value.

rationale	Security-by-design is a fundamental principle of modern cybersecurity. Requiring a documented SSDLC shifts responsibility for security to the earliest stage – software design and development. This ensures that vulnerabilities are identified and eliminated before the product reaches the market, rather than during the operational phase. Due to intellectual property protection and technological confidentiality, verification of process artefacts may be carried out under controlled conditions, e.g. during an on-site audit at the Manufacturer's premises or under NDA.
verification criterion	The Manufacturer shall provide documentation describing the SSDLC process. The documentation shall include a description of the tools used (SAST, DAST), dependency management procedures (SBOM), vulnerability response policy, and the method of identifying and versioning components (together with examples of version labels and hashes). SAST/DAST tool reports and the SBOM for the delivered software shall be provided.

SLC-1.3	**Secure Software Engineering Practices**
requirement description	The software development process shall be based on recognised secure coding standards appropriate to the hardware platform (e.g. CERT C, MISRA C 2023). The Manufacturer shall use Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools to eliminate vulnerabilities and shall maintain a secure configuration and version management system for software.
rationale	Security-by-design is a fundamental principle of modern cybersecurity and is required by EU regulations such as the Cyber Resilience Act. Using SAST and DAST tools enables automatic detection of common programming errors and vulnerabilities at an early development stage, which significantly reduces the cost of remediation and the risk of exploitation in the production environment. Secure version management is essential to ensure software integrity and traceability. The standards referenced in the requirement (MISRA, CERT) are given as examples; the Manufacturer shall demonstrate the use of a professional coding methodology appropriate to the hardware platform.
verification criterion	The Manufacturer shall provide documentation of the secure coding standards (SSDLC) applied, together with evidence of the use of SAST and DAST tools (e.g. reports, scan logs) and a description of the version and configuration management system. A sample SAST/DAST report covering the firmware delivered shall be provided.

SLC-1.4	Component Supply Chain Management
requirement description	The Manufacturer shall apply a documented process for the assessment and qualification of third-party components (hardware and software). Components may only be used where their origin and integrity have been confirmed (e.g. digital signature, supplier certificate, verified repository, traceability of hardware components).
rationale	Modern devices comprise many components from different suppliers, creating a complex supply chain. An attack on this chain is one of the most serious threats. This requirement, emphasised in the NIS2 Directive, forces the Manufacturer to take responsibility for the security of the whole product, not only the parts it has manufactured itself. The use of a Software Bill of Materials (SBOM) and a Hardware Bill of Materials (HBOM) is good practice in this area. Technical verification (HBOM) should focus on high-risk elements, i.e. components containing digital logic. Due to intellectual property protection and technological confidentiality, HBOM/SBOM documentation is made available under NDA.
verification criterion	The Manufacturer shall provide a documented procedure for the assessment and qualification of suppliers and third-party components (software and hardware). The procedure shall describe the method of verifying integrity (e.g. checksum verification, digital signatures, supplier certificates, traceability of hardware components) and the authenticity of components. Upon request, the Manufacturer shall make available a list of third-party components (SBOM and HBOM) together with evidence of their verification.

SLC-1.5	Auditability of Security Processes
requirement description	The Manufacturer and the Contractor (Supplier) of the device shall consent to periodic audits of their organisation's security processes.
rationale	Ensuring the security of the AMI infrastructure is a shared responsibility of the Manufacturer, the Contractor (Supplier) and the operator. For the DSO to effectively manage risk across the full system lifecycle, it must be able to verify that the security processes declared by the Manufacturer and the Contractor (Supplier) are actually and consistently applied. This requirement formalises the DSO's right to conduct audits, which is standard practice in the security management of critical infrastructure supply chains. Audits are carried out at the premises of the Manufacturer / Contractor (Supplier) under NDA. Auditors shall hold ISO/IEC 27001 Lead Auditor certification and have experience in

	auditing OT/AMI systems.
verification criterion	The Manufacturer and the Contractor (Supplier) shall, by contract, guarantee the DSO (or an authorised third party designated by the DSO) 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 the audits shall be defined in the contract, with the objective of verifying that the practices applied are consistent with the documentation provided.

SLC-2.1	**Trusted Hardware Module and Secure Boot**
requirement description	The device shall be equipped with a secure boot mechanism that prevents the system from starting with unauthorised software. Verification of the integrity and authenticity of the software shall be performed using an embedded trusted hardware element storing the Manufacturer's key.
rationale	Software modification is one of the most serious attack vectors. Secure boot implemented in hardware ensures that only authentic software signed by the Manufacturer is launched on the device. This prevents the installation of malicious code that could manipulate metering data or disrupt network operation. "Embedded trusted hardware element" shall be understood as a dedicated chip (e.g., TPM, HSM) or a microcontroller feature (e.g. TrustZone), on condition that the requirement for permanently disabled MCU service interfaces (ACC-4.3) is met. Secure boot mechanisms are described in requirements INT-2.2 and INT-2.3.
verification criterion	The device boot process shall fail (e.g. the device shall enter an error state and shall not launch the main application) if any part of the software (firmware, bootloader, operating system, application) does not pass digital signature verification. Any attempt to boot an unsigned software image shall be blocked. The failed boot event shall be recorded in the event log (e.g. using the bootloader mechanism).

SLC-3.1	**Authentication and Integrity Verification of Updates**
requirement description	The Manufacturer shall digitally sign every update package (firmware). The device shall unconditionally verify this signature before installation begins. Updates without a valid digital signature shall be rejected. The firmware update process of the device may be initiated only by an authenticated account with an assigned administrative role (e.g. a management association).

rationale	The remote update process, although necessary to maintain security, creates a risk of uploading malicious software. The requirement to verify the digital signature ensures that the device only accepts updates originating from an authorised source (the Manufacturer). At the same time, restricting the ability to initiate updates to an administrator role (e.g., a management association) prevents unauthorised attempts to upload software, even if an attacker were able to bypass other security controls.
verification criterion	The device shall reject and not install any update package whose digital signature is invalid, corrupted, or issued by an untrusted signing authority. The failed verification event shall be recorded in the security event log. Update initiation shall only be possible from an account with an administrative role (e.g., a management association).

SLC-3.2	**Anti-Rollback Protection**
requirement description	The device shall implement a mechanism preventing the installation of software versions older than the current version, except when authorised by the DSO.
rationale	Attackers may attempt to install an older version of the software that contains a known and already patched vulnerability to exploit it. The anti-rollback mechanism blocks this attack vector, ensuring that the device always runs a software version at least as secure as the previous one.
verification criterion	Any attempt to install an update package with a version lower than the version currently running on the device shall be rejected by default. The device shall record this event in the security event log. Where specified in the order, the device shall enable a forced rollback to the previous version (N-1) via a specifically authorised DSO system command.

SLC-3.3	**Secure Software Update**
requirement description	The device shall perform the software update process in such a way that the new software version is activated only after successful verification of its integrity and completeness. In the event of an update error (e.g. transmission error, power failure, checksum mismatch), the new version shall not be activated, and the device shall continue operating on the last known stable software version.
rationale	The update process is a critical operation. An error during the update must not lead to permanent damage to the device. The device shall ensure continuity of

	operation and system resilience to unforeseen problems, which is critical in infrastructure with a long lifecycle.
verification criterion	A simulated failed update (e.g., by interrupting the power supply during the update) shall cause the device, after reboot, to resume normal operation. The device shall record this event in the event log.

SLC-3.4	**Scope of Software Updates**
requirement description	The device shall allow updating of key software components, both locally and remotely.
rationale	The ability to update key software components is the foundation of long-term security. It makes it possible to respond to newly discovered vulnerabilities and to adapt to changing standards (e.g., cryptographic standards). In devices with a "monolithic" software architecture, this requirement is implemented by enabling the replacement of the entire firmware image, in which updated key software components have been included. The requirement considers the fact that in smart meters, updating often consists of replacing the entire image containing corrected components, while preserving metrological constraints (WELMEC).
verification criterion	The Manufacturer shall ensure the ability to update all key components of the device firmware remotely and locally. The documentation shall confirm that the architecture allows these functionalities to be replaced as part of the software update process.

SLC-4.1	**Documented Vulnerability Management Process**
requirement description	The Manufacturer shall implement and maintain a formal vulnerability management process, compliant with standards such as ISO/IEC 29147 and ISO/IEC 30111, throughout the defined technical support period of the device. The process shall include proactive monitoring of components for newly discovered vulnerabilities, risk assessment and timely delivery of security patches within defined time frames.
rationale	No software is free from flaws, and new vulnerabilities are discovered continuously. Having a formalised proactive response process is essential to maintain security throughout the long lifecycle of the meter. This is a fundamental requirement of the EU Cyber Resilience Act (CRA). It ensures that identified vulnerabilities will be systematically analysed and patched over time,

	considering the time required for certification processes at Notified Bodies.
verification criterion	The Manufacturer shall present a publicly available Vulnerability Disclosure Policy and an internal vulnerability management procedure. The procedure shall define Service Level Agreements (SLA) for the delivery of patches depending on the criticality of the vulnerability (e.g., based on CVSS) and shall consider the time required for certification processes at Notified Bodies.

SLC-5.1	**Secure Production Environment and Initialisation**
requirement description	The device initialisation (provisioning) process, including the loading of unique cryptographic credentials, shall take place in a physically and logically secured, controlled and auditable production environment.
rationale	Initialisation is the moment at which the device is assigned its unique digital identity (keys, certificates). Compromise of this process could lead to cloning of devices or theft of master keys, undermining the security of the entire system.
verification criterion	The Manufacturer shall provide evidence of the security of the production environment, for example as part of ISO/IEC 27001 certification (in accordance with SLC-1.1). The documentation shall describe physical and logical access controls to the production line and audit procedures for the credential-loading process. It shall be possible to trace which credentials were loaded into a given device and when.

SLC-6.1	**Future-Proof Design**
requirement description	The device shall have spare compute and memory capacity to allow the future update of cryptographic algorithms and communication protocols to newer, more secure versions, without the need for physical replacement of the hardware.
rationale	The lifecycle of the meter is 15–20 years. Over this period, currently used cryptographic standards may prove insufficient. Providing hardware reserves enables the security level to be raised remotely in the future and prevents the accumulation of technical debt.
verification criterion	The device's technical documentation shall demonstrate that the device has at least a 15% resource reserve (Flash/RAM memory, CPU) compared with the baseline version, enabling the deployment of Security Suite 2 (e.g., AES-256)

	without hardware replacement. The Manufacturer shall provide evidence (e.g., performance tests or declarations) confirming the resource reserve.

2. Strong Cryptography

CRY-1.1	Approved Cryptographic Algorithms
requirement description	Only publicly known, well-established, and, at the time of delivery, considered secure cryptographic algorithms shall be used.
rationale	Requiring adherence to recognized international standards ensures that the implemented mechanisms are resistant to known attacks and have been thoroughly analyzed by the cryptographic community. Minimum Requirements: • symmetric encryption – e.g., AES-128, • public-key cryptography – e.g., ECC with 256-bit keys, • hash functions – e.g., SHA-256.
verification criterion	Documentation review and communication testing shall demonstrate that the device uses exclusively algorithms and parameters (key lengths, curves) compliant with the specified requirements for security functions (encryption, digital signatures).

CRY-1.2	Upgradeability of Cryptographic Mechanisms
requirement description	The software architecture shall allow for 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"). Over the 15–20 year operational lifetime of the meter, currently used cryptographic algorithms may be judged insecure. The ability to update them remotely and locally is essential to maintaining long-term security. In devices with „monolithic" software architecture, this requirement is implemented by enabling the replacement of the entire firmware image in which updated cryptographic functions have been included. This avoids the limitations associated with the lack of dynamic libraries in simple real-time systems.

verification criterion	The software architecture documentation shall demonstrate that cryptographic functions are implemented in source code in a manner enabling their modification and update in the context of a new software release. The Manufacturer shall demonstrate (e.g., in a test environment or through process documentation) the ability to perform an update that changes or upgrades the parameters / version of the cryptographic algorithms used.

CRY-2.1	**Cryptographically Secure Random Number Generator**
requirement description	The device shall 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 the security of all cryptographic operations, such as key generation or the creation of initialisation vectors. Using a weak generator renders even the strongest algorithms useless.
verification criterion	The Manufacturer shall provide technical documentation for the microcontroller (MCU) or dedicated security IC used, confirming the presence of a hardware Cryptographically Secure Random Number Generator (TRNG/CSPRNG) compliant with current standards (e.g. NIST SP 800-90A/B/C or BSI AIS 20/31). The Manufacturer shall declare that the Cryptographically Secure Random Number Generator is used in all cryptographic operations requiring entropy.

CRY-3.1	**Uniqueness of Device Cryptographic Keys**
requirement description	Each meter shall have its own unique set of cryptographic keys. The use of default keys, keys shared across a group of devices (group keys) or keys generated in a predictable manner is prohibited.
rationale	Using the same keys in multiple devices creates enormous systemic risk – compromise of a single device leads to compromise of the entire group. Unique keys for each meter ensure that the consequences of a security breach are limited to a single device.
verification criterion	Analysis of digital certificates (or public keys) obtained from at least two different devices shall demonstrate that they are unique. The Manufacturer shall provide evidence, within the scope of a production process (provisioning) audit, that each device is initialised with a unique set of

	cryptographic keys, including a unique Master Key. It shall be demonstrated that keys are not generated in a trivial manner from publicly known identifiers (e.g. serial numbers), which would make them predictable.

CRY-3.2	Key Lifecycle Management
requirement description	The device shall support operation within the full key lifecycle, including secure generation, distribution, storage, remote and local rotation (replacement) and secure deletion. All temporary keys shall be deleted after use. Key lifecycle operations shall be possible either through functionality built into the meter or through other applications used to operate and interwork with the device (Key Management System).
rationale	Cryptographic keys should be rotated regularly to limit the time they may be exploited after theft. The device shall have secure, automated mechanisms for managing keys throughout its operational lifetime. In the context of the meter, secure deletion means overwriting session keys in RAM after the session ends and invalidating (overwriting) old keys in non-volatile memory after successful rotation to new keys.
verification criterion	The device shall expose secure functions (e.g. within the DLMS/COSEM protocol) allowing an authorised administrator to remotely and securely replace (rotate) session and application keys. Tests shall confirm that, after successful key replacement, the old key is inactive and that temporary (session) keys are cleared from working memory upon closure of the communication session.

CRY-3.3	Support for External Key Management Systems
requirement description	The device shall support mechanisms enabling secure interworking with external Key Management Systems (KMS). It shall be possible to remotely initiate key lifecycle operations (e.g. generation of a new key pair, Certificate Signing Request, installation of a new certificate or replacement of symmetric keys) using standard mechanisms of the communication protocol (e.g. Security Suite 1 or 2 in DLMS/COSEM).
rationale	At large scale, manual key management is impractical and error prone. The meter shall enable automation of identity and key management processes through standard protocol functions (e.g. DLMS objects and methods), allowing Key Management Systems to remotely enforce rotation and certificate revocation policies without involving field technicians.

verification criterion	The Manufacturer shall document the supported methods of remote key management in accordance with the DLMS/COSEM standard. Functional tests shall be performed to confirm that the device is able to correctly process a certificate renewal request initiated by the central system, generating a new key pair or renewing the certificate (where applicable) at the request of the Head-End System.

CRY-4.1	**Hardware Protection of Critical Keys**
requirement description	Device private keys and all master keys shall be generated, stored and used within a hardware-protected, isolated environment (e.g. Secure Element, Trusted Execution Environment) that prevents them from being read or copied in plaintext.
rationale	Private and master keys are the most critical secrets of the device. Their compromise allows an attacker to impersonate the device or to decrypt communications. Hardware isolation ensures that keys never leave the secure environment in plaintext. This requirement may be satisfied either by a dedicated external chip (Secure Element) or by built-in features of modern microcontrollers (e.g., TrustZone), provided that the requirement for permanently disabled MCU service interfaces (ACC-4.3) is met.
verification criterion	It shall be demonstrated (e.g. through analysis of design documentation and penetration testing) that there is no programming function (API) or physical interface permitting direct reading or export of private/master keys from the protected environment. Cryptographic operations using these keys (e.g. signing) shall be performed inside that environment.

CRY-5.1	**Certificate-Based Digital Identity**
requirement description	A Remote Reading Meter that establishes a direct connection to the central system shall have a unique digital identity confirmed by an X.509 standard certificate, in accordance with DLMS/COSEM Security Suite 1 or higher. The certificate shall be issued by a trusted Certification Authority (CA) within a dedicated AMI Public Key Infrastructure (PKI). Where communication takes place via intermediate devices (e.g. data concentrators) or over technologies with critically low bandwidth, security mechanisms based on symmetric cryptography (Security Suite 0) may be used, provided that application-layer end-to-end security is ensured in accordance with DSO guidelines.

rationale	In a system comprising millions of devices, digital certificates are the only scalable and reliable way to manage identity and establish trust. This requirement is foundational – it establishes that every device is a unique, cryptographically verifiable entity. It 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). It enables strong, mutual authentication between the meter and the central system, which is the basis of secure communication and prevents Man-in-the-Middle attacks.
verification criterion	Each device is factory-provisioned 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 Application-Layer Protection**
requirement description	Direct communication between the meter and the central system shall be secured on the application layer (e.g., using DLMS/COSEM Security Suite 1 or 2), ensuring the confidentiality and integrity of data along the full path, regardless of security mechanisms applied at lower network layers. Where communication takes place via intermediate devices (e.g., data concentrators) or over technologies with critically low bandwidth, security mechanisms based on symmetric cryptography (Security Suite 0) may be used, provided that application-layer end-to-end security is ensured in accordance with DSO guidelines.
rationale	Security at lower layers (e.g., in the mobile network) may be insufficient or beyond the operator's control. Application-layer encryption ensures that data is protected from the moment it leaves the meter until it reaches the central system, and that no intermediate system (e.g., a concentrator) has access to the data in plaintext. Application-layer encryption ensures that data is protected from the moment of its generation in the meter until processing by the Head-End System (HES). A key aspect is the role of the meter as the endpoint (terminator) of the application session. This means that no intermediate device (e.g., a PLC concentrator, communication modem or VPN server) may have access to data in plaintext. The requirement focuses on the protocol and the logical data path; the technical isolation of cryptographic processes from the communication stack is regulated complementarily in requirement CRY-4.1.

verification criterion	Network traffic analysis shall demonstrate that the content of the application-layer protocol (e.g. DLMS) is encrypted, even when communication takes place inside a VPN/IPsec tunnel.

COM-2.1	**Mutual Authentication of the Communication Channel**
requirement description	Every direct communication session with the central system shall be preceded by strong mutual authentication of both parties, based on digital certificates (e.g. Security Suite 1 or 2). Where communication takes place via intermediary devices (e.g. data concentrators) or over technologies with critically low bandwidth, security mechanisms based on symmetric cryptography (Security Suite 0) may be used, provided that application-layer end-to-end security is ensured in accordance with DSO guidelines.
rationale	Encryption alone is not a sufficient security measure. Both parties to the communication must be able to verify the identity of their counterparty. Mutual authentication by means of certificates prevents an attacker from impersonating the system or the device.
verification criterion	Establishment of a direct communication session (e.g. TLS) shall succeed only if both the server presents a valid certificate trusted by the meter and the meter presents a valid certificate trusted by the server. An attempt to establish a connection with a server presenting an invalid certificate shall be rejected and recorded in the event log.

COM-3.1	**Protection Against Replay Attacks**
requirement description	The communication protocol shall implement a mechanism to protect against replay attacks, for example by using unique, monotonically increasing sequence numbers in messages or cryptographic nonces.
rationale	A replay attack consists in intercepting and re-transmitting a legitimate message to trigger an unwanted action. Effective protection against such attacks is essential to ensure the integrity and non-repudiation of operations.

verification criterion	Interception and re-transmission of the same, cryptographically valid message to the device shall be rejected by the device. The rejection of a replayed message shall be recorded in the event log.

COM-3.2	**Command Validation**
requirement description	The device shall validate all received data and commands for syntactic and semantic correctness. Malformed or unknown commands shall be ignored / rejected.
rationale	Sending malformed or unexpected data to a device (fuzzing) is a common technique for discovering software flaws. Rigorous validation of all input data protects against buffer overflow attacks and other parsing errors that could lead to instability or compromise of the device.
verification criterion	Sending the device a series of deliberately malformed or syntactically incorrect commands (fuzzing) shall not cause the device to crash, restart, or enter an unsafe state. The device shall reject such commands and continue normal operation.

4. Access Control

ACC-1.1	**Authentication Requirement for All Interfaces**
requirement description	Access to all access interfaces of the device (remote WAN and local, e.g., the optical port) shall be unconditionally preceded by a successful strong authentication process. Anonymous access is not permitted, with the following exceptions: • "Public Client" association in the DLMS/COSEM standard (restricted to reading basic device information necessary to establish a session); • The interface used for communication with the Home Area Network (HAN) infrastructure, if it operates exclusively in a one-way data publication (push) mode.
rationale	Every access interface without authentication constitutes an open gateway for potential attackers. The requirement for strong authentication at every access point is a fundamental security principle, ensuring that only authorised entities can interact with the device. The HAN interface, due to its specific nature (the

	user cannot initiate communication towards the meter), is not treated as an access interface within the meaning of this requirement.
verification criterion	Any attempt to perform any operation (other than basic identification within the public association) on any access interface without prior successful authentication shall be rejected by the device.

ACC-2.1	**Protection Against Brute-Force Attacks**
requirement description	Access interfaces shall implement a mechanism to protect against brute-force attacks, resulting in temporarily blocking access after a defined, configurable number of failed login attempts. The event shall be logged.
rationale	Brute-force attacks, which consist in attempting to guess a password or key, are a common threat. A temporary blocking mechanism significantly slows down and hinders such an attack, increasing its cost and the probability of detection.
verification criterion	After the configured number of failed authentication attempts on a given interface has been exceeded, the device shall cease to respond to further attempts for a defined period. Every failed attempt shall be recorded in the event log.

ACC-3.1	**Implementation of Privilege Separation Model**
requirement description	The device shall implement a granular access control model based on associations (in accordance with the DLMS/COSEM standard), or an equivalent privilege separation mechanism (e.g., RBAC). Each authenticated identity shall be assigned an unambiguously defined set of privileges, in accordance with the principle of least privilege.
rationale	Assigning privileges to individual users is inefficient and error prone. Using an organised privilege model – e.g., based on roles, access levels or functional groups – allows logical grouping of privileges, simplifies management and ensures the application of the principle of least privilege. Each level or role has access only to the functions necessary to perform its assigned tasks.
verification criterion	An authenticated association may perform only those operations permitted within its assigned privilege scope (e.g. role, access level or functional profile). Any attempt to perform an operation exceeding that scope shall be rejected and recorded in the event log.

ACC-3.2	Set of Privilege Levels
requirement description	The device shall support the ability to define separate privilege levels or equivalent user roles. At least two predefined privilege levels or predefined equivalent user roles shall exist: • administrative (full access, configuration, updates); • public (read-only access to basic device information necessary to establish a session).
rationale	Standardising the minimum set of access levels or user roles increases interoperability and enables consistent privilege management throughout the AMI system. This distinction reflects the typical actors interacting with the meter (administrator, end user, other levels) and supports enforcement of the principle of least privilege.
verification criterion	The device documentation shall describe the implemented privilege levels, roles or other authorisation mechanisms and the functions assigned to them. Functional tests shall confirm that: • the device distinguishes at least two access levels or equivalent user profiles; • each level has a privilege scope consistent with its description; • it is possible to define additional access levels and to assign them a scope of privileges; • attempts to perform operations exceeding the assigned level are rejected and recorded in the event log.

ACC-3.3	Documentation of User Accounts
requirement description	All user accounts implemented in the meter, including service accounts, shall be documented and presented in the device specification.
rationale	Hidden or undocumented accounts constitute a serious security risk. The requirement for full documentation of all accounts ensures transparency and enables auditors to verify that no unauthorised access points exist. The requirements for accounts are intended to safeguard against the implementation of insecure mechanisms outside the DLMS standard (engineering accounts, passwords). Within DLMS, accounts do not exist as such.

verification criterion	The list of user accounts (if any) obtained from the device (e.g. via the administrative interface) shall be 100% consistent with the list presented in the product's technical documentation.

ACC-4.1	**Attack Surface Minimisation**
requirement description	All unused physical ports, network protocols and software services that are not required from a functional point of view shall be disabled by default.
rationale	Every active service or open port is a potential entry point for an attacker (the so-called attack surface). Minimising this surface by disabling everything that is not necessary for operation is one of the fundamental principles of system hardening.
verification criterion	Port scanning and analysis of the device configuration in its factory state shall demonstrate that only those services and ports that have been defined as necessary in the product documentation are active.

ACC-4.2	**Interface Deactivation Capability**
requirement description	The operator shall be able to remotely and locally deactivate individual communication interfaces for a defined period.
rationale	The ability to dynamically enable and disable interfaces gives the operator flexibility in managing security. In the event of a detected threat, or where there is no business need, a given interface (e.g. the HAN for the consumer) may be temporarily disabled, further reducing the attack surface.
verification criterion	An authorised administrator shall be able, using a remote or local command, to disable and subsequently re-enable a selected communication interface. The state of the interface (active / inactive) shall be correctly reported by the device.

ACC-4.3	**Permanent Disabling of Debug Interfaces**
requirement description	All physical and logical developer and diagnostic interfaces (e.g. JTAG, serial ports with access to a system shell) shall be permanently and irreversibly disabled on devices intended for operational use.

rationale	Debug interfaces provide near-unrestricted access to the internals of the device and allow most security measures to be bypassed. Leaving them enabled in the production version is an unacceptable risk. Permanent disabling (e.g. by blowing eFuse in the microcontroller) is standard security practice for smart meters. Repair mechanisms at the Manufacturer, if any, shall rely on authorised and secure processes (e.g. a service bootloader), not on hardware interfaces.
verification criterion	Physical inspection and electronic testing of the device shall not reveal active signals on pins corresponding to debug interfaces. Attempts to connect to such interfaces shall fail.

ACC-5.1	**Password Management**
requirement description	Password-based authentication on all interfaces shall meet the following requirements: • Factory passwords shall be unique per device and shall require change on first login. • It shall be possible to define a password complexity policy (minimum length, required character classes) and a password aging policy (maximum validity period, password history). The password policy so defined shall match current security standards. • Passwords shall be transmitted only over encrypted channels. • The system shall not reveal whether a failed login attempt concerned the username or the password. • A password change shall generate an event log entry.
rationale	Weak passwords or improper storage and transmission of passwords are among the most common causes of security breaches. Introducing comprehensive password management requirements significantly improves resistance to attacks based on guessing or interception. The requirement safeguards against the implementation of insecure mechanisms outside the DLMS standard (engineering accounts, passwords). Considered fulfilled within DLMS.
verification criterion	Where the device uses password-based authentication, functional tests shall confirm that: • After logging in with the default password, the system enforces a change. • An administrative interface exists to configure complexity rules. • Network traffic analysis confirms that passwords are transmitted in encrypted form. • The error message is generic (e.g. "Invalid login credentials"). • A password change is recorded in the event log.

ACC-5.2	Session Logout and Locking Mechanisms
requirement description	The device shall implement an automatic logout (or lock) mechanism for elevated privilege sessions (e.g. administrative, service) after a configurable idle period.
rationale	Leaving an active privileged session unattended creates a risk of unauthorised hijacking by third parties. Automatic logout after an idle period is a fundamental countermeasure, consistent with the principle of minimising the attack time window. It is a standard security function in mature IT/OT systems.
verification criterion	After the configured idle time on a local or remote interface has elapsed, the user session shall be automatically terminated. Any subsequent operation requiring privileges shall require re-authentication.

5. Integrity Protection

INT-1.1	Integrity Protection of Stored Data
requirement description	Critical data stored in non-volatile memory (metering data such as current energy register values, authentication and encryption keys, logs) shall be protected by cryptographic mechanisms (e.g. Message Authentication Codes (MAC) or checksums) to enable verification of their integrity. Integrity protection shall cover the following data categories: metering and billing data, cryptographic keys, security configuration, event logs.
rationale	Ensuring that data stored in memory has not been altered (intentionally or accidentally) is crucial to the credibility of the entire system. Cryptographic mechanisms such as MACs act as a digital seal, allowing the integrity of data to be verified at any time.
verification criterion	Deliberate modification of a block of protected data in memory (e.g. using developer tools) shall be detected by the device during the next attempt to read that data. Detection of an integrity breach shall be recorded in the event log.

INT-1.2	Ochrona przed Informacjami Pozostałymi
requirement	Pamięć tymczasowa (np. bufory) używana do przechowywania kluczy

description	kryptograficznych lub innych danych wrażliwych musi być bezpiecznie czyszczona (nadpisywana) natychmiast po zakończeniu operacji.
rationale	Pozostawienie wrażliwych danych w pamięci po zakończeniu operacji stwarza ryzyko, że mogą one zostać odczytane przez późniejsze, mniej uprzywilejowane procesy. Bezpieczne czyszczenie pamięci eliminuje to zagrożenie.
verification criterion	Where the Manufacturer provides a copy of the meter with a deliberately unsecured developer interface: analysis based on a memory dump of the device taken after a cryptographic operation. The analysis shall not reveal any fragments of session keys or other sensitive data in plaintext. Where the Manufacturer cannot provide a copy of the meter with a deliberately unsecured developer interface: analysis based on the SBOM and HBOM documentation provided, in the context of the solutions applied and the manner of their implementation. There shall be documented technical capability to implement the residual-information protection mechanism.

INT-2.1	**Functional Segregation and Protection Against DoS Attacks**
requirement description	Software architecture shall ensure strong logical separation of requirements between metrological and communication components. A DoS/DDoS attack on the communication interface shall not affect the continuity and correctness of metering functions.
rationale	Compromise of the communication module must not endanger the fundamental function of the device, i.e. energy metering. Logical separation ensures that even in the event of a successful attack on the network part, the metrological part remains intact and operates correctly.
verification criterion	Performing a DoS attack (e.g. port flooding) on the device's communication interface shall not cause the metering / energy consumption recording process to stop or be disrupted. After the attack has ceased, communication functions shall return to normal operation.

INT-2.2	**Secure Recovery After Failure**
requirement description	The device shall maintain a secure state in the event of a failure (e.g. a self-test error, a cryptographic function error). After a failure, the device shall return to the last known secure state and shall not disclose confidential information nor allow

	access controls to be bypassed.
rationale	A device failure must not create security gaps. The "fail-secure" principle ensures that in the event of an error the device automatically transitions to a state of maximum security (e.g. by blocking access), rather than in an insecure open state. A device failure must not disclose confidential information such as cryptographic keys or authentication data. Nor may failure affect the security of other system elements.
verification criterion	Simulation of a failure of a critical component (e.g. loss of communication with the cryptographic module) shall cause the device to enter a defined failure state. After restart, the device shall start in a secure configuration, and log analysis shall not reveal any leakage of data.

INT-2.3	**Self-Test at Startup**
requirement description	The device shall perform self-tests of key security functions (e.g. cryptographic mechanisms, random number generator) during the boot process, in order to verify that they operate correctly. In the event of a self-test error, the device shall: continue the metering function, record the event in the event log, send an alarm notification to the Head-End System (HES), and signal the error state locally. A device that remains in a security-function self-test error state requires local intervention (replacement).
rationale	Ensuring that basic security mechanisms operate correctly at every startup is essential to maintaining trust in the device. Self-tests allow early detection of hardware failures or software corruption that could weaken security. Any damage to security modules shall be detected at the next device restart.
verification criterion	Deliberate corruption (at the software layer) of one of the security verification modules (e.g. the AES library) shall be detected at the next device restart. The device shall signal an error and shall not continue normal startup.

INT-3.1	**Detection of Housing and Terminal Cover Opening**
requirement description	The device shall be equipped with physical sensors detecting and recording at least the following events: opening of the meter housing (except in the case of housings of non-dismantlable meters), opening of the connection terminal cover, and opening of the communication module cover – where applicable (not applicable for meters with an integrated communication module). Each such

	event shall be immediately recorded and reported.
rationale	Detection of attempts at physical tampering is the first line of defence against manipulation. Recording and alarm generation on the opening of the housing enables a rapid response to potential attempts at fraud or sabotage.
verification criterion	Physical opening of the terminal cover, the communication module cover (where applicable) or the meter housing shall result in immediate recording of the event in the security event log.

INT-4.1	**Magnetic Field Detection**
requirement description	The device shall be equipped with a sensor detecting attempts at manipulation using an external magnetic field. Detection of such a field shall be immediately recorded and reported.
rationale	Neodymium magnets may be used in attempts to disrupt the operation of electronic metering components. A dedicated sensor enables such attempts to be detected and serves as a deterrent.
verification criterion	Bringing a magnet (of a defined field strength) close to the meter shall cause the event to be recorded in the security event log and an alarm to be sent to the central system.

6. Logging and Audit

LOG-1.1	**Scope of Logged Events**
requirement description	The device shall record, within a dedicated security event log, all security-relevant events. The minimum set of events shall include: • successful authentication attempts, • activation of brute-force protection mechanisms, • changes to security configuration, • software updates (both successful and failed), including firmware upload, verification, and activation, • detected physical tampering attempts, • software integrity failures (e.g., unsuccessful secure boot), • cryptographic function errors, • system time modifications,

	• device resets, • critical system errors. Event retention at the central level is at least 12 months for all events. At the local (device) level: at least 90 days for critical/high-severity events and at least 30 days for low-severity events.
rationale	A complete and detailed event log is an indispensable tool for monitoring the security state of the system, detecting anomalies and incidents, and conducting post-incident investigations. Defining a minimum, standard set of logged events ensures consistency and usability of data throughout the AMI system.
verification criterion	The performance of each of the operations listed in the description (e.g. a failed login, a firmware update) shall result in the appearance of an appropriate, detailed entry in the event log.

LOG-1.2	**Event Log Entry Detail**
requirement description	Each entry in the event log shall contain at least: • an accurate timestamp, • the event type, • the identifier of the entity initiating the event (where applicable), • the result of the operation (success/failure) (where applicable), • the interface on which the event occurred (where applicable).
rationale	For logs to be useful, they must contain sufficient contextual information. Defining a minimum set of attributes for each entry guarantees that recorded events will be understandable and capable of being correlated during analysis.
verification criterion	Analysis of entries in the event log shall confirm that each entry contains all the required fields and that their content is consistent with the operation performed.

LOG-2.1	**Protection of the Event Log Against Modification**
requirement description	The event log shall be protected against unauthorised modification and deletion. Only the addition of new entries shall be possible. Any attempt to modify or delete existing entries shall be blocked and recorded as a security event (where technically feasible).

rationale	The credibility of the event log depends on its integrity. Attackers often attempt to cover their tracks by modifying or deleting logs. A "write-only" (or "append-only") mechanism is a fundamental protective measure, ensuring that the history of events remains intact.
verification criterion	The device shall reject and log any attempt to modify or delete existing entries. Tests using an authenticated administrative account shall confirm that individual entries cannot be altered or removed. Existing log entries shall be immutable via the API.

LOG-2.2	**Authorised Access to the Event Log**
requirement description	Access to read and to delete entries in the event log shall be controlled and restricted to authorised roles (in accordance with the privilege separation model). Modification of existing entries is prohibited (except in justified administrative operations). The software update log and logs subject to legal metrological control are non-erasable under field conditions; operations on these logs are only possible in laboratory conditions. Every operation of clearing the remaining logs, performed by an authorised role, shall be recorded in the security event log.
rationale	Although modification of individual entries is prohibited (LOG-2.1), there may be justified administrative operations, such as clearing the entire log during service. This requirement ensures that such operations can only be performed by the most privileged roles and that the operation itself is also logged.
verification criterion	A user with a role of lower privileges shall not have access to functions for reading or clearing the security log. Any attempt to perform such an operation shall be blocked and recorded.

LOG-3.1	**Event Log Capacity and Management**
requirement description	The device shall have non-volatile memory sufficient to store a configurable, defined minimum of the most recent security events, managed according to the following rules: • The security event log and operational logs operate in circular buffer mode, ensuring the retention of events from a period of not less than 90 days under the nominal device load. Once the buffer is full, the oldest entries shall be overwritten by the newest (FIFO mechanism). • The software update log and logs subject to legal metrological control operate in write-once mode – without the FIFO mechanism. Once such a

	log is full, the performance of a further update is blocked, in accordance with the requirements of WELMEC Guide 7.2. Clearing these logs is only possible under laboratory conditions.
rationale	Ensuring adequate log capacity is crucial to enabling analysis of events from a reasonable period. Circular buffer mechanism is a standard and secure method of managing limited memory, guaranteeing that the most recent events are always available.
verification criterion	After the generation of security events exceeding the configured minimum, the oldest (first) event shall be overwritten, and the log shall contain at least the configured minimum number of the most recent events.

LOG-4.1	**Time Synchronisation**
requirement description	The device shall implement a secure time synchronisation mechanism (e.g. using DLMS/COSEM messages) to ensure the accuracy and reliability of timestamps in all event logs.
rationale	Accurate and synchronised timestamps are essential for correlating events between different devices and systems during incident analysis. Unreliable time makes reconstruction of the chronology of an attack impossible.
verification criterion	The device shall reject time-setting attempts originating from unauthenticated sources. Changing the system time shall be possible only for authorised roles and shall be recorded in the event log (whether successful or failed). Tests shall demonstrate that the device maintains correct time in accordance with the configured, trusted source..

LOG-5.1	**Critical Event Alarming**
requirement description	Selected critical security events (e.g. detection of physical tampering, multiple failed logins, opening of the communication module cover – except for integrated meters) shall trigger the sending of an alarm notification.
rationale	Event logging alone is not sufficient; in the case of critical incidents, an immediate response is necessary. The alarming function ensures that the system operator is promptly informed of potential threats, enabling appropriate action to

	be taken.
verification criterion	Triggering an event defined as critical (e.g. opening of the housing – where applicable) shall result not only in a log entry but also in the immediate initiation of the sending of the corresponding alarm notification to the HES.

7. Physical Security

PHY-1.1	**Sealing Capability**
requirement description	The meter housing (except for meters with non-dismantlable housings) and the terminal cover shall be designed in such a way as to allow sealing. The construction shall make it impossible to access the interior of the device or the terminals without breaking or visibly damaging the seal.
rationale	The seal is the basic visual deterrent and evidentiary measure indicating an attempt at unauthorised physical intervention. It is a fundamental physical security requirement.
verification criterion	Physical inspection of the device shall confirm the existence of dedicated points for the attachment of seals. Any attempt to remove the housing or terminal cover without removing the seal shall be impossible without visibly destroying the seal.

PHY-2.1	**Local Service Ports Protection**
requirement description	Physical communication interfaces, except for the optical port, shall be located in such a way as to require the removal of a sealed cover (e.g. the terminal cover) in order to access them.
rationale	Communication interfaces constitute a potential attack vector. Placing them behind a sealed cover ensures that access is possible only to authorised personnel and that every such intervention leaves a physical trace (a broken seal). The optical port, due to operational practices associated with its use, need not be subject to this additional protection.
verification criterion	Physical inspection of the device shall confirm that all physical communication interfaces, except for the optical port, are not accessible from the outside without prior removal of the terminal cover.

PHY-3.1	Meter Housing Protection Against Mechanical and Environmental Factors
requirement description	The device housing shall provide protection against basic attempts at forcible intervention and shall comply with the relevant standards for electrical equipment regarding protection against environmental factors.
rationale	The housing constitutes the first physical barrier protecting the sensitive electronic components inside the meter. It shall be sufficiently robust to hinder simple, forcible attempts at access to the interior.
verification criterion	The product documentation shall confirm compliance with the relevant standards (e.g. those concerning the IP and IK protection ratings). A visual inspection shall confirm the solidity of the construction and the absence of obvious weaknesses.

Glossary of Abbreviations

Abbreviation	Definition
Standards, norms and 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
NDA	Non-Disclosure Agreement
WELMEC	European Cooperation in Legal Metrology
Models, processes and methodology	
SSDLC	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
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
X.509	Standard X.509
SE	Secure Element
TEE	Trusted Execution Environment
HSM	Hardware Security Module
TPM	Trusted Platform Module
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
HES	Head-End System
WAN	Wide Area Network
HAN	Home Area Network
EST	Enrollment over Secure Transport
Hardware and system architecture	
MCU	Microcontroller Unit
FLASH	Flash Memory

RAM	Random Access Memory
CPU	Central Processing Unit
TrustZone	Microcontroller Unit TrustZone
Energy infrastructure and metering systems	
AMI	Advanced Metering Infrastructure
DSO	Distribution System Operator
HES	Head-End System
Organisations and regulations	
NIS2	Network and Information Security Directive 2
BSI	German Federal Office for Information Security
NIST	National Institute of Standards and Technology