cen CENELEC

European Standardization Organizations

CRA Standards Unlocked: Cybersecurity Requirements for Smart Meter Gateways within smart metering systems

We start at 9:30 CET

Webinar moderator

Els SOMERS

Project Manager

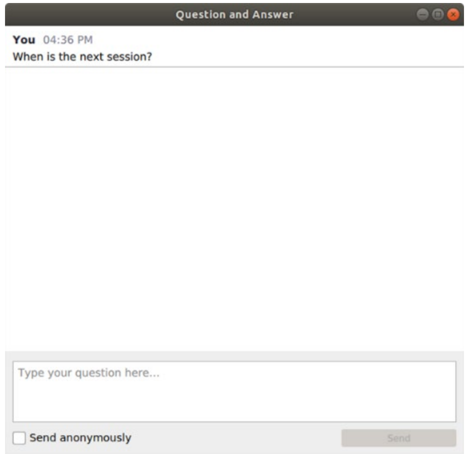
Public Relations

CEN-CENELEC

esomers@cencenelec.eu

Get the most out of the webinar today

- ▶ You are muted
- ▶ Use the Q&A panel to submit your questions



You 04:36 PM
When is the next session?

- ▶ Talk about us with #training4standards #standards4CRA
  - ▶On X [@Standards4EU]()
  - ▶On Bluesky [@cen-cenelec.bsky.social]()
  - ▶On LinkedIn [www.linkedin.com/company/cen-and-cenelec]()

Your speaker today

Enrico Frumento

Rapporteur CEN/CLC JWG13 WG6 PT1, work item for Line 40: Cybersecurity Requirements for **Smart Meter Gateways**

Introduction

Agenda

- Introduction
- Legal overview and WG structure
- What an SMGW does

- Cybersecurity challenges
  - What does critical imply
  - challenges

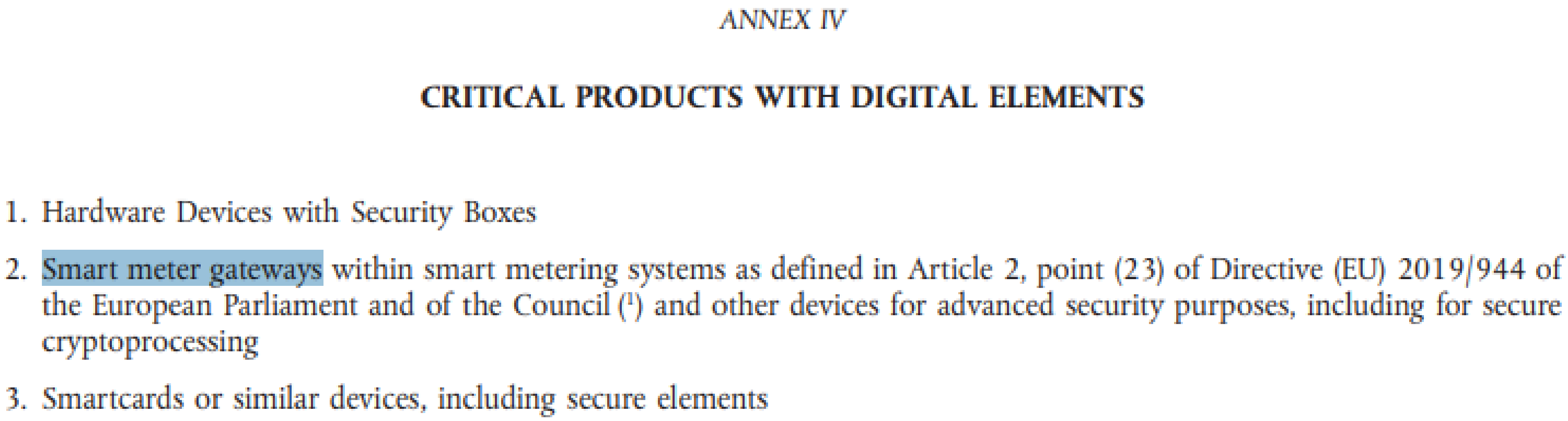
- Vertical standard details
  - Normative references
  - Operational environment
  - Actors
  - Use-cases
  - Assets
  - Threats
  - Risk Factors
  - Requirements
  - Mapping with Essential requirements (Annex ZA)

- Next steps

Legal Overview & WG structure

Legal overview (i)

- CRA, Annex IV "Critical Products with digital elements". No. 2 is :



ANNEX IV

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

1. Hardware Devices with Security Boxes
2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council [1] and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements

Legal overview (i)

- Directive (EU) 2019/944, Article 2 point (23):

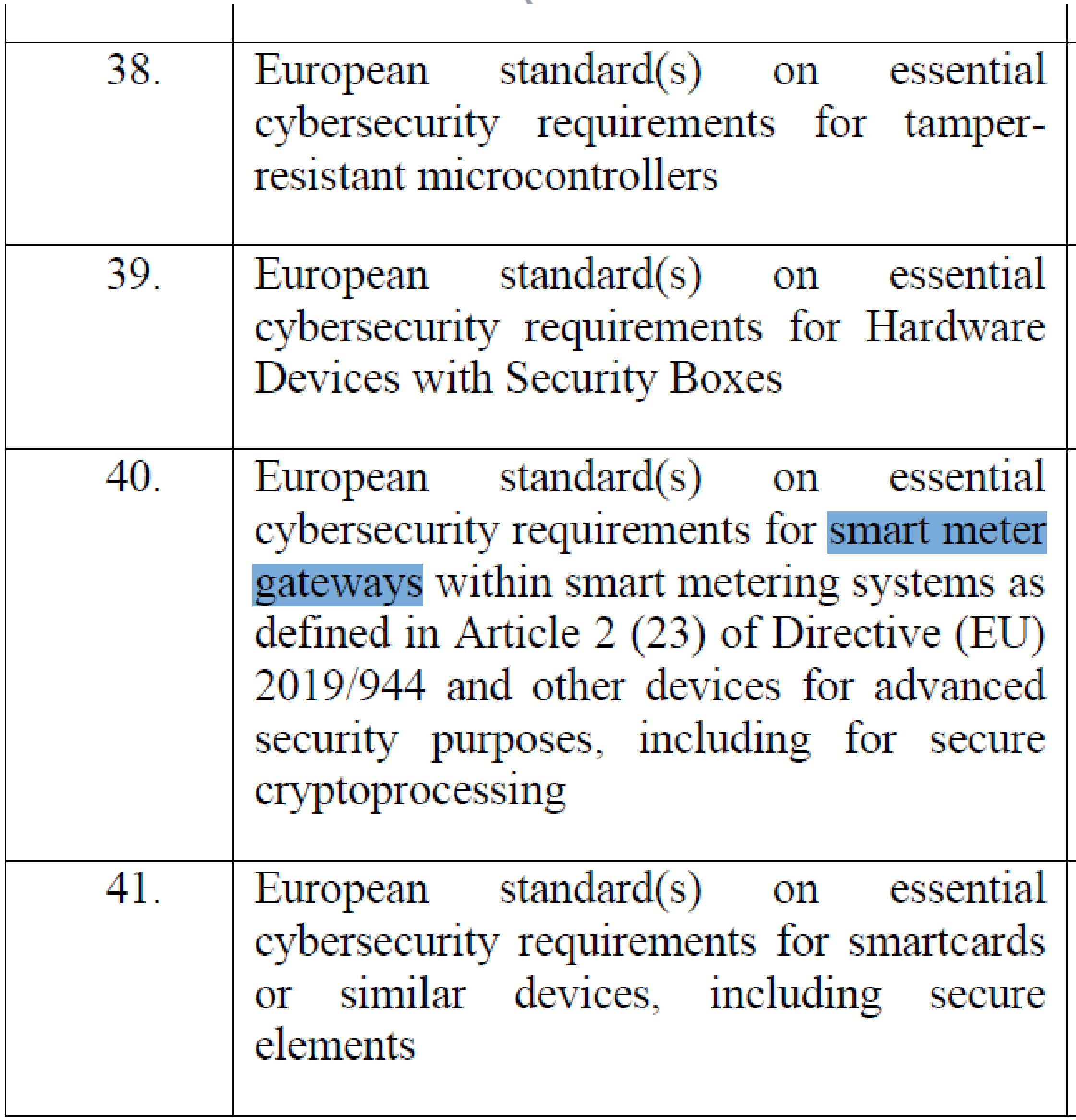
‘***smart metering system***’ *means an electronic system that is capable of measuring electricity fed into the grid or electricity consumed from the grid, providing more information than a conventional meter, and that is capable of transmitting and receiving data for information, monitoring and control purposes, using a form of electronic communication;*

Smart meter != Smart meter gateways != Smart metering system != Smart Grid

Legal overview (ii)

- Standardisation request, Annex I 3.2.2025

  → Standard no. 40 (Smart Mater Gateways)



38.	European standard(s) on essential cybersecurity requirements for tamper-resistant microcontrollers
39.	European standard(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes
40.	European standard(s) on essential cybersecurity requirements for smart meter gateways within smart metering systems as defined in Article 2 (23) of Directive (EU) 2019/944 and other devices for advanced security purposes, including for secure cryptoprocessing
41.	European standard(s) on essential cybersecurity requirements for smartcards or similar devices, including secure elements

Legal overview (ii)

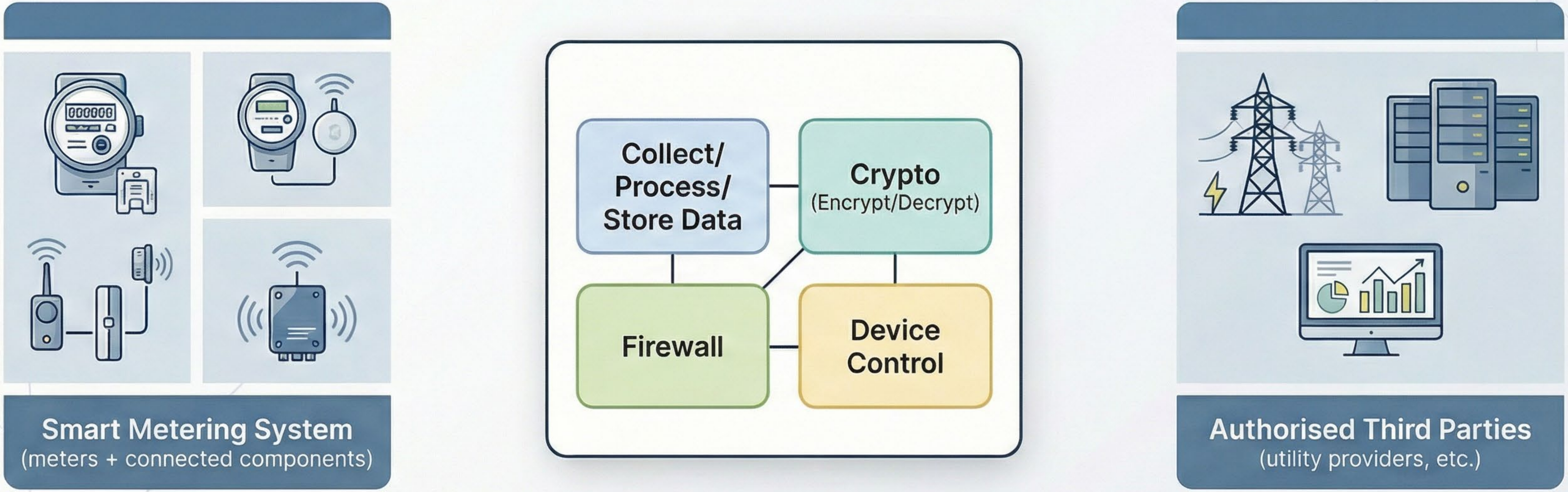
- Implementing Regulation (EU)2025/2392, 28.11.2025, definition on what a SMGW is (definitive)

*"**Smart meter gateways** are products with digital elements that control communication between components in or connected to smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944, and authorised third parties, such as utility providers. Smart meter gateways collect, process and store meter or personal data, protect data and information flows by supporting specific cryptographic needs, such as encryption and decryption of data, incorporate firewalling functionalities and provide the means to control other devices.*

*This category includes **but is not limited** to smart meter gateways related to smart metering systems measuring **electricity** as defined in Article 2(23) of Directive (EU) 2019/944.*

*It **may** also include smart meter gateways used in other smart metering systems measuring consumption of **other sources of energy** such as **gas** or **heat**, **provided that the gateway meets this description**."*

Smart Meter Gateway:
The Secure Central Communication Hub



Smart Metering System
(meters + connected components)

Collect/ Process/ Store Data

Crypto
(Encrypt/Decrypt)

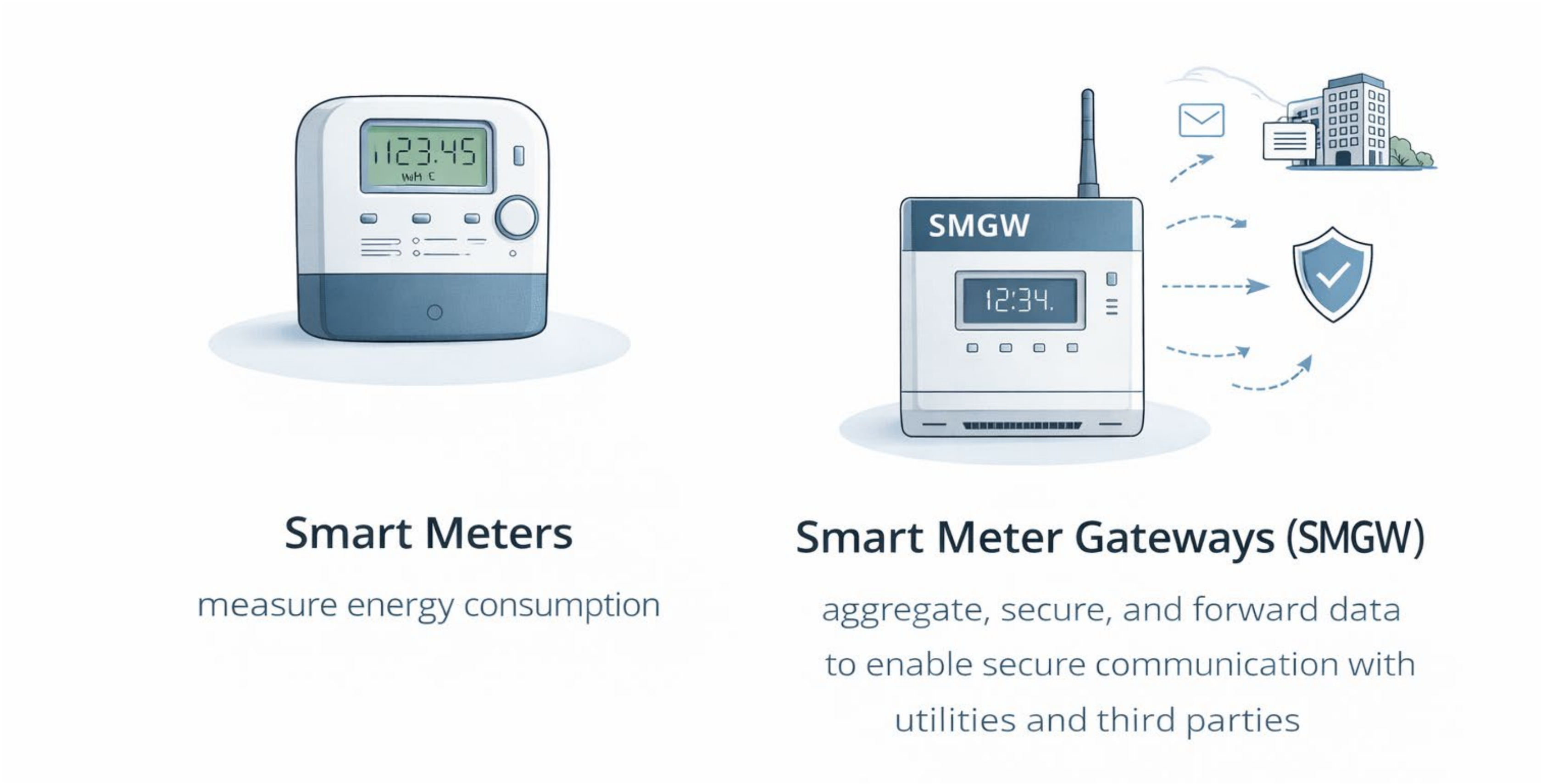
Firewall

Device Control

Authorised Third Parties
(utility providers, etc.)

Applies to: Electricity; optionally Gas/Heat

Smart Meter vs Smart Meter Gateways



Smart Meters

measure energy consumption

Smart Meter Gateways (SMGW)

aggregate, secure, and forward data to enable secure communication with utilities and third parties

Ongoing work

- Initiated in June 2025 (NWI)

- Scope definition
- Expert group sessions
- Cross vertical meetings
- Meetings with the commission

- Draft submitted on December 20th, 2025 for commission review
- Under writing

Team

Expert group

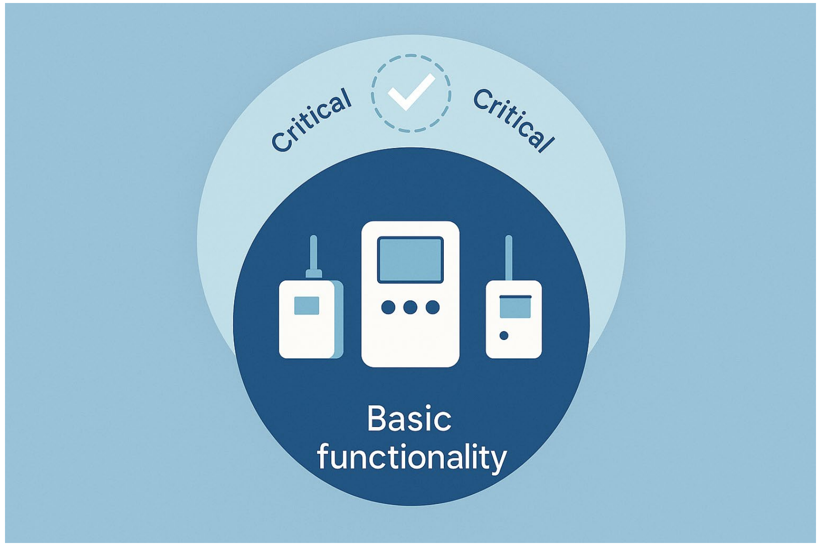
Torben Markussen Kamstrup	Willem Strabbing ESMIG	Eugen Mayer PPC	Michael Buss MeterPS CLC TC13 Chair
Alia Fourati EDF	Andreas Resch BSI	Simon Dunkley Itron	Brecht Wyseur Kudelski Labs
Daniel Garcia Miralles Gridspertise	Riccardo Fiorelli STMicroelectronics	Jürgen Blümer Lackmann	Enrico Frumento (Rapporteur) Cefriel

Harmonised standards and CRA

- Compliance with CRA Essential Requirements will be mandatory by 11 December 2027.
- Harmonised standards support the possible paths to achieve CRA compliance
- **Presumption of Conformity**

What the standard covers

- The standard will cover **multiple types of SMGW and not only the ones belonging to the critical CRA class**.
- There are basic functionalities that all types implement and optional functionalities that, for example, are only implemented in critical SMGWs.

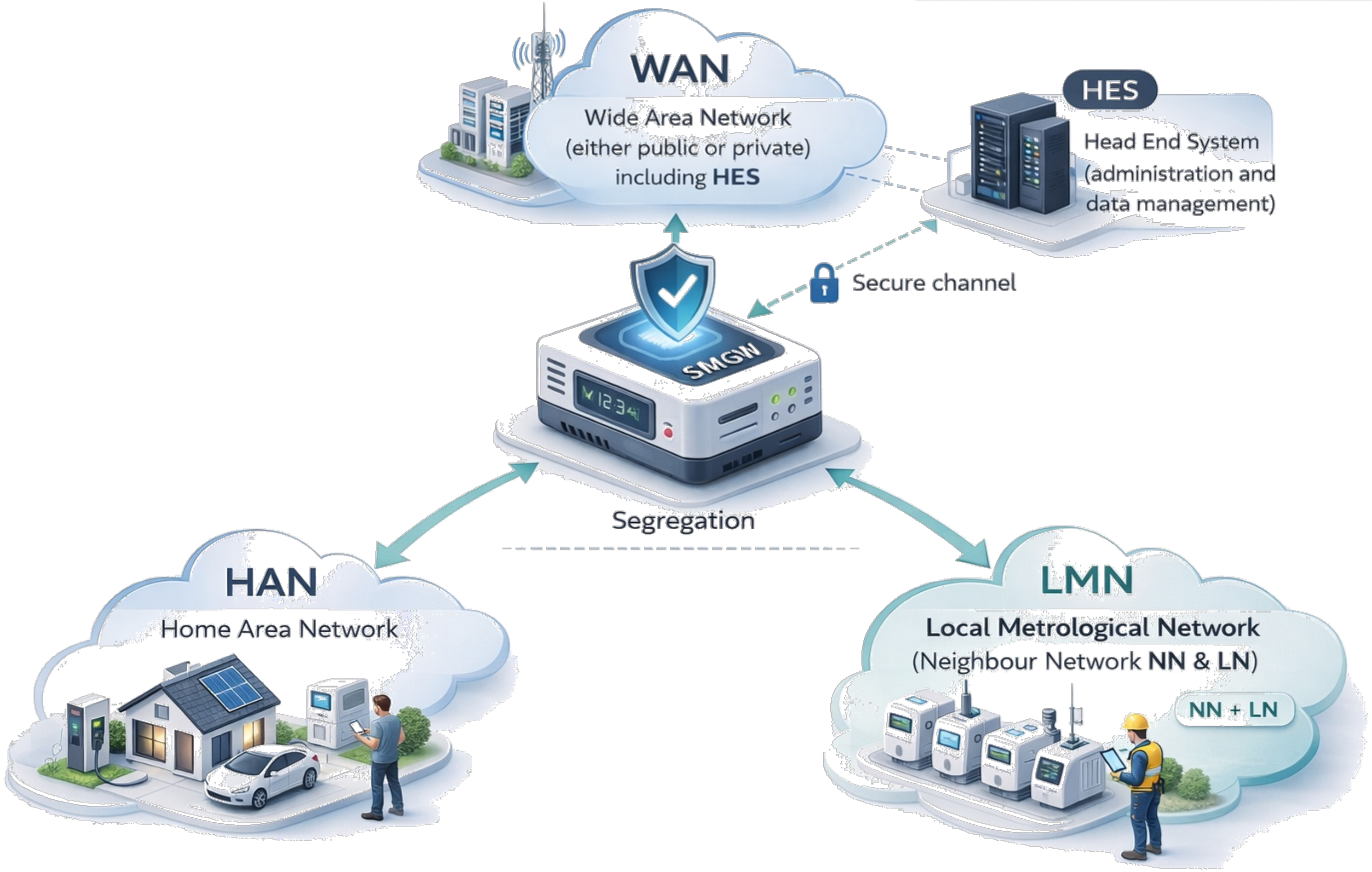


What an SMGW does

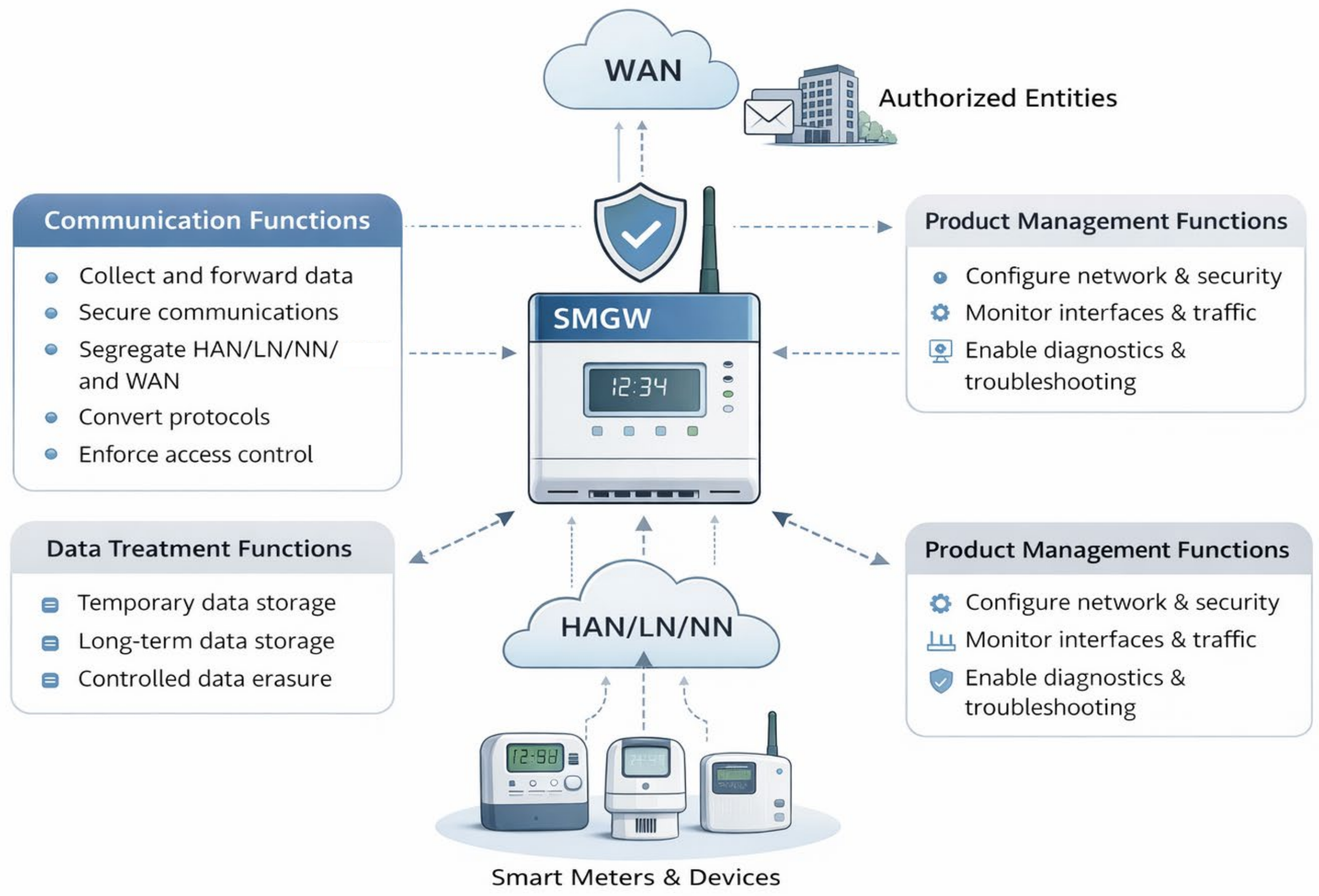
What an SMGW does (general view)

- **WAN:** Wide Area Network (either public or private), including HES
- **LMN:** Local Metrological Network (Neighbour Network NN & Local Network LN)
- **HAN:** Home Area Network
- **HES:** Head End System (administration and data management)

→ CEN/CLC/ETSI/TR 50572 «Functional reference architecture for communications in smart metering systems»



What an SMGW does (general view)



WAN
Authorized Entities
SMGW
12:34
Communication Functions
Collect and forward data
Secure communications
Segregate HAN/LN/NN/ and WAN
Convert protocols
Enforce access control
Product Management Functions
Configure network & security
Monitor interfaces & traffic
Enable diagnostics & troubleshooting
Data Treatment Functions
Temporary data storage
Long-term data storage
Controlled data erasure
Product Management Functions
Configure network & security
Monitor interfaces & traffic
Enable diagnostics & troubleshooting
HAN/LN/NN
Smart Meters & Devices

Smart meter gateways

- are products with digital elements that collect and forward metering data to authorised entities,
- protect data via encryption and authentication,
- segregate the three network areas HAN, LMN (LN / NN) and WAN with protocol conversion,
- and enforce access to specific data and functions by authorised entities

What an SMGW does (general view)

Communication functions

- The SMGW provides core communication capabilities to collect metering data, secure communications, and manage authorised access. It interfaces between smart metering domain (on HAN / NAN) and the WAN, while enforcing protocol and access constraints.
  - Collects measurement data from meters and connected smart metering devices.
  - Forwards collected data to authorised entities.
  - Protects data privacy via secure communication mechanisms.
  - Preserves data integrity using encryption and authentication.
  - Segregates communications between HAN, LN or NN devices and the WAN.
  - Performs protocol conversion to forward messages to smart meters and other devices.
  - Enforces authorised access to specific data and functions based on related services.
  - Prevents data disclosure and / or data manipulation

What an SMGW does (general view)

Data treatment functions

- The SMGW supports data handling for operational needs and regulatory constraints. It provides storage functions for configurations and metering data, and supports controlled erasure aligned with minimum retention requirements.
  - Stores session credentials temporarily when required for communications.
  - Buffers messages directed to smart meters or authorised entities, such as the HES.
  - Stores configurations to support SMGW operation.
  - Stores meter data for operational and service purposes.
  - Stores historical meter data while respecting minimum retention periods, if applicable.
  - Ensures data erasure during decommissioning or reinstallation at a different location.
  - Defers data erasure until regulatory minimum retention periods expire, if applicable.

What an SMGW does (general view)

Product management functions

- The SMGW provides product administration functions to configure operational parameters and maintain service operation. It also supports monitoring and diagnostics to collect operational indicators and enable troubleshooting while controlling exposure of sensitive information.
  - Manages network interface settings for SMGW administration.
  - Configures routing protocol parameters.
  - Administers security policies for the product.
  - Applies quality of service rules.
  - Performs system maintenance operations.
  - Collects interface statistics, error conditions, performance metrics, and security events.
  - Enables diagnostics for connectivity, performance, and configuration issues while managing sensitive operational information.

What an SMGW does (general view)

Additional functions

In addition, some SMGWs can

- implement further functions related to **advanced cybersecurity tasks.**
- Used for:
  - incorporating firewall functionalities, related to direct or remote control of other devices (e.g. connecting and disconnecting local appliances from power), to metrological and tariff-related data processing,
  - provision of other smart grid services.
- Such functions, **if compromised**, could
  - affect functions **critical to the cybersecurity of other products**, networks or services, including securing authentication and access, intrusion prevention and detection, end-point security or network protection;
  - **disrupt or cause damage to a large number of other products or systems**, or to the **security or safety of users** through remote control of devices and appliances.

SMGW is a system of systems

Cybersecurity challenges

What does critical imply?

- It is subject to a 3rd party assessment

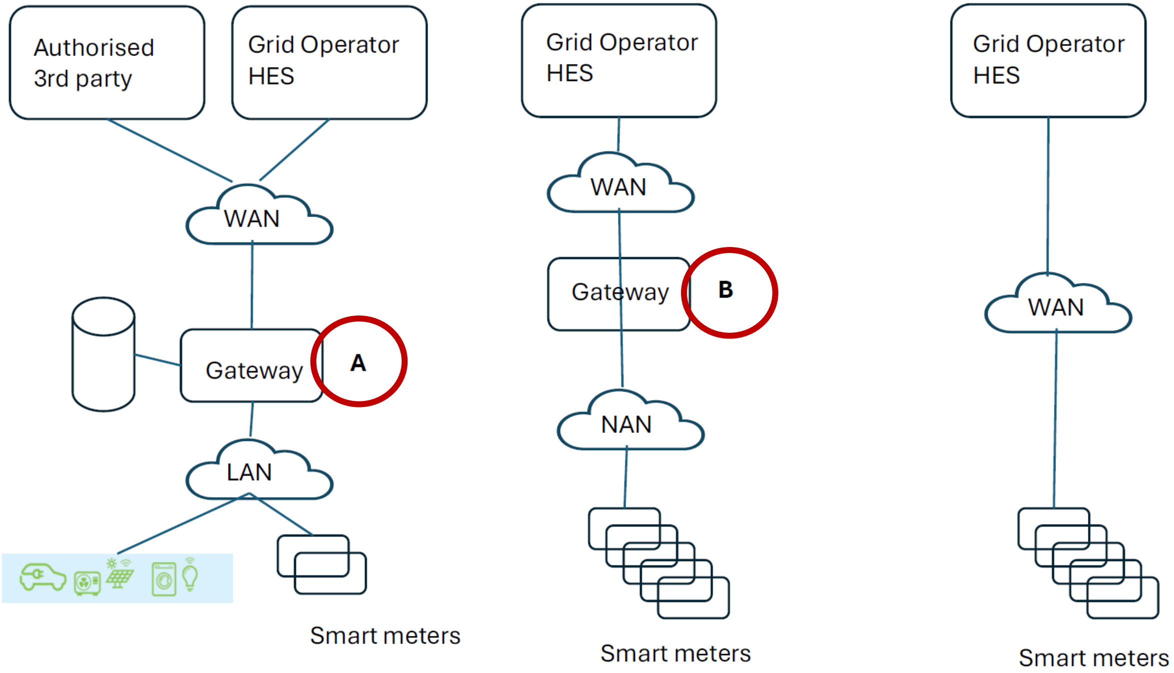
- The criticality is determined by the application sector, thou not all the SMGWs are critical

- It can be certified against a certification framework, but this is not mandatory unless another regulation mandates it

Challenges

- Existing Protection Profiles (e.g., Germany) are based on EUCC and not yet fully aligned with CRA.
- Multiple certification schemes, with multiple assurance and security levels, apply.
- **EU’s heterogeneous landscape of SMGW**
- Harmonised standards aim at providing a clear path to presumption of conformity for SMGW producers across EU.

Challenges (heterogeneous landscape)



- **Examples (real world is more complex)**
- **Gateway A:**
  - typically located inside a consumer's premises
  - able to control local consumption, generation and storage
  - able to store and process metering data
  - enables access by authorised 3rd parties
  - considered a CRA critical gateway
- **Gateway B:**
  - typically located at the substation level (protected environment)
  - connected to smart meters in a neighbourhood
  - passes through encrypted metering data without decryption
  - includes Data Concentrators and Remote Data Processing RDPSs, if not autonomous

Why security in SMGW context?

- Critical infrastructure component
- **Risks**: data interception, manipulation, unauthorised access, privacy, critical infrastructure take down in a cyber-warfare context, etc.
- **EU concern**: grid stability and user privacy

Why security in SMGW context?

Examples of Known Attacks

- Firmware manipulation and backdoors
- Manipulation of actual consumption or generation data
- Manipulation of commands sent to CU
- Access to historical consumption data

Why security in SMGW context?

Examples of Known Attacks

- **May 2023 – Denmark:** a significant sector-wide attack infiltrated 22 energy companies using operational-technology (OT) malware. Though specifics about smart meter gateways were limited, such gateways are considered part of the OT network for metering and grid control – Source
- Researches across Europe confirm that smart meter gateways are **vulnerable via firmware, network interfaces, and compromised SIM or API access (not only)**, opening doors to remote manipulation, data alteration, and even grid disruption – Source

Why security in SMGW context?

- **Security Features of SMGWs vary across Europe**
- **SMGWs aren’t one-size-fits-all**; they're a patchwork of varied security capabilities, shaped by differing national requirements
  - **For example, Germany**: its BSI-backed Protection Profile (BSI-CC-PP-0073, TR-03109) mandates rigorous EU Common Criteria certification for SMGWs, setting a high bar
- **Elsewhere in the EU**, SMGW security levels — and what qualifies as ‘critical’ — remain instead undefined
- Such complexity raises fundamental questions we are addressing: which devices must meet the Standard? **How do you draw the line**?
- Presumption of Conformity
- **Our aim is to write a standard that covers all SMGWs, without knowing all possible current and future architectures (based on Functional Capabilities)**

SMGW vertical standard details

Draft Structure

Body

- 1. Scope
- 2. Normative references
- 3. Terms and abbreviations
- 4. Product context
  - 4.1 Intended product reasonable & foreseeable use
  - 4.2 Product Functions
  - 4.3 Product Architecture
  - 4.4 Operational Environment
  - 4.5 Risk assessment framework
  - 4.6 Actors
  - 4.7 Reasonably foreseeable use cases
  - 4.8 Context summary
- 5. Cybersecurity Requirements
- 6. Vulnerability Handling Requirements

Annexes

- A – SMGW Data Assets
- B - SMGW Functions
- C – Threat landscape and security considerations
- D – Product class SMGW using Common Criteria
- E - Security Problem definition
- F - Risk acceptance criteria and risk management methodology
- G - Life cycle
- H - Relationship with other verticals
- I – Vulnerability handling
- J - Use cases
- K - Cryptographic Algorithms
- L - Security Target
- ZA - Relationship between this European Standard and the essential requirements

Normative and not references

- Smart metering systems
  - CEN-CLC-ETSI TR 50572:2011 Functional reference architecture for communications in smart metering systems
- CRA Horizontal standards
  - prEN 40000-1-2 (JT013089), Principles for cyber resilience
  - prEN 40000-1-3 (JT013090), Vulnerability handling
  - prEN 40000-1-3 (JT013091), Generic Cybersecurity requirements
- BSI-backed Protection Profile
  - BSI-CC-PP-0073, TR-03109
- National cybersecurity certification schemes (e.g. France)

Architecture and main possible functions

- The assessment will consider
  - If the capability is present in an SMGW or not
  - That the implementation can be in hardware, firmware, application layer or a mix of them
  - The role of the operational environment

Operational Environment

3 types of environments are considered

- **Uncontrolled environment**: Physical access cannot be reliably restricted to authorised persons.
  - e.g. unattended outdoor cabinet.
- **Controlled environment**: Installed in a non-public closed facility with restricted access (basic physical protection).
  - e.g. secured substation building.
- **Monitored environment**: Publicly accessible location with concealing casing and manipulation (tamper) detection.
  - e.g. street distribution cabinet with tamper detection; publicly accessible meter enclosure.

Actors

There are several categories of actors

- Smart Meter Gateway Access
  - Third-party, Local user (LU), SMGW admin (GWA), SMGW Service Technician (SRV), HES operators/admins, External market participants (EMP)/Eligible party, Metering point operator (MPO), …
- External Entities
  - Metered data administrator, Manufacturer, SMGW Owner, TSO/DSO, Supplier, Installer, …
- Other Roles
  - Direct marketers, Device operators, Service providers, Energy service providers, …

Use cases

- UC1: On-premises deployment
  - This deployment corresponds to the Local Network Access Point (LNAP) in the reference communication architecture for smart metering systems described in CEN/CLC/ETSI TR 50572:2011.
  - SMGWs are physically located within residential (a public area, such as a meter room, or a private area, for example inside a single-family house), commercial, or industrial buildings, close to the smart meters connected to the SMGW.
- UC2: Grid infrastructure deployment
  - This deployment corresponds to the Neighbourhood Network Access Point NNAP in the reference communication architecture for smart metering systems described in CEN/CLC/ETSI TR 50572:2011.
  - SMGWs are securely connected via NN to a number of smart meters across a group of premises at electricity substations or regional concentrator nodes. In this case, the SMGW is typically installed in a secondary distribution substation or at another point of the smart metering system.
- UCx: other use cases are under preparation

Main Assets

- **Command and Control data**
  - For CU
- **Meter data assets**
  - Meter data assets are related to the metering functionality.
- **Metrology and calibration assets**
  - Metrology and calibration assets are related to metrology and calibration data and functionalities.
- **User assets**
  - User assets are related to data associated with the local user (LU).
- **Communication assets**
  - Communication assets are related to the establishment and management of secure communication within and across the SMGW network.
- **System operation assets**
  - System operation assets are related to the maintenance and operation of the SMGW.

Risk Profiles

- Risk profiles are defined for Core SGWM and for each use case
- So far, two risk profiles are under discussion: basic and advanced

Main Threats

Threats are divided into categories:

- T.DisclosureWAN
  - A remote attacker may try to read/disclose confidential information in the user data
- T.DisclosureLocal
  - A local attacker may try to read/disclose confidential information in the user data
- T.DataModificationWAN
  - A remote attacker may try to modify user data or SMGW security functionalities (TSF) via WAN
- T.DataModificationLocal
  - A local attacker may try to modify user data or TSF via LMN, HAN, WAN

Main Threats

Threats are divided into categories:

- T.ResidualData
  - A local attacker or a remote attacker may try to read/disclose user data (e.g., meter data) from the SMGW which are no longer needed for SMGW operation.
- T.ResidentData
  - A remote attacker or local attacker may try to access (i.e., read, alter, delete) user data or TSF data for which they don't have permission
- T.Privacy
  - A remote attacker may try to obtain more detailed information from the SMGW than actually required to fulfil the tasks defined by its role or the contract with the consumer.
- T.TimeModification
  - A local attacker or remote attacker may try to alter the SMGW time
- T.Infrastructure
  - A remote attacker may try to obtain control over the SMGW, or over devices in the HAN or LAN via the SMGW, to cause damage to external entities

Main Risk Factors

- Risk Factors (RF) are defined for each SMGW use case
  - Condition, characteristic or contextual element of a SMGW, its environment, its configuration, or its operational use that increases the likelihood or potential impact of a cybersecurity threat (RF-x).
- Main RF categories
  - Baseline
  - Unauthorised access
  - Management operations
  - Protocol implementations
  - Data operations
  - Specific SMGW RFs (e.g., metering data collection, delivering metering data to 3rd party, applying commands to SMGWs, …)

Main Requirements

- **Requirements on documentation** fall into 11 categories
  - Secure by design
  - No known exploitable vulnerabilities
  - Secure by default configuration
  - Security updates
  - Access control and authentication
  - Data protection
  - Data minimisation
  - Availability and resilience
  - Attack surface and mitigation
  - Monitoring and logging
  - Data management
- Each requirement is composed of 4 sections:
  - Applicability
  - Correlated requirements: the content of the related requirements
  - Assessment Criteria: activities, verdict, supporting evidences

Example

Authorisation

Applicability

- This clause establishes requirements for controlling what authenticated users can do on the product.

Requirements

- **[AUTH-2-RQ-1-01]** The product shall implement a privilege separation mechanism that requires user authentication before granting administrative access.
- [AUTH-2-RQ-1-02] The product shall not allow any user to perform actions beyond their authorised privilege level.
- [AUTH-2-RQ-1-03] The product shall enforce access control on all management interfaces consistently, preventing privilege escalation through alternative interfaces.
- [AUTH-2-RQ-1-04] The product shall implement command authorisation that validates each command based on the authorised privilege level before execution.
- [AUTH-2-RQ-1-05] The product shall enforce the principle of least privilege during normal operation

Example

[AUTH-2-RQ-1-01] Verify the product implements a privilege separation mechanism that requires user authentication before granting administrative access.

Activities

Verify:

- Manufacturer documentation describes privilege separation mechanism and authentication requirements.
- Product implements privilege separation between administrative and non-administrative access.
- Administrative access requires user authentication.
- Authentication occurs before administrative privileges are granted.
- Non-administrative users cannot access administrative functions without authentication.
- Privilege levels are clearly defined and enforced.
- Administrative operations require appropriate privilege level.
- Attempted administrative access without authentication is denied.
- Attempted administrative access with non-administrative credentials is denied.
- Privilege separation mechanism prevents unauthorised elevation to administrative access.

Example

Verdict

- PASS if all the following conditions are met/FAIL if one of the following conditions is not met:
- Product implements privilege separation mechanism;
- Administrative access requires user authentication;
- Authentication occurs before granting administrative privileges;
- Non-administrative users cannot access administrative functions;
- Privilege levels are defined and enforced;
- Unauthorised administrative access attempts are denied.

Example

Supporting evidence

- Manufacturer documentation describing privilege separation mechanism;
- Product configuration showing privilege levels;
- Test results demonstrating authentication requirement for administrative access;
- Attempted administrative access without authentication showing denial;
- Attempted administrative access with non-administrative credentials showing denial;
- Verification confirming privilege separation enforcement;
- Analysis confirming privilege levels are properly defined and enforced.

Annex ZA

Mapping between this standard and the essential requirements of CRA regulation

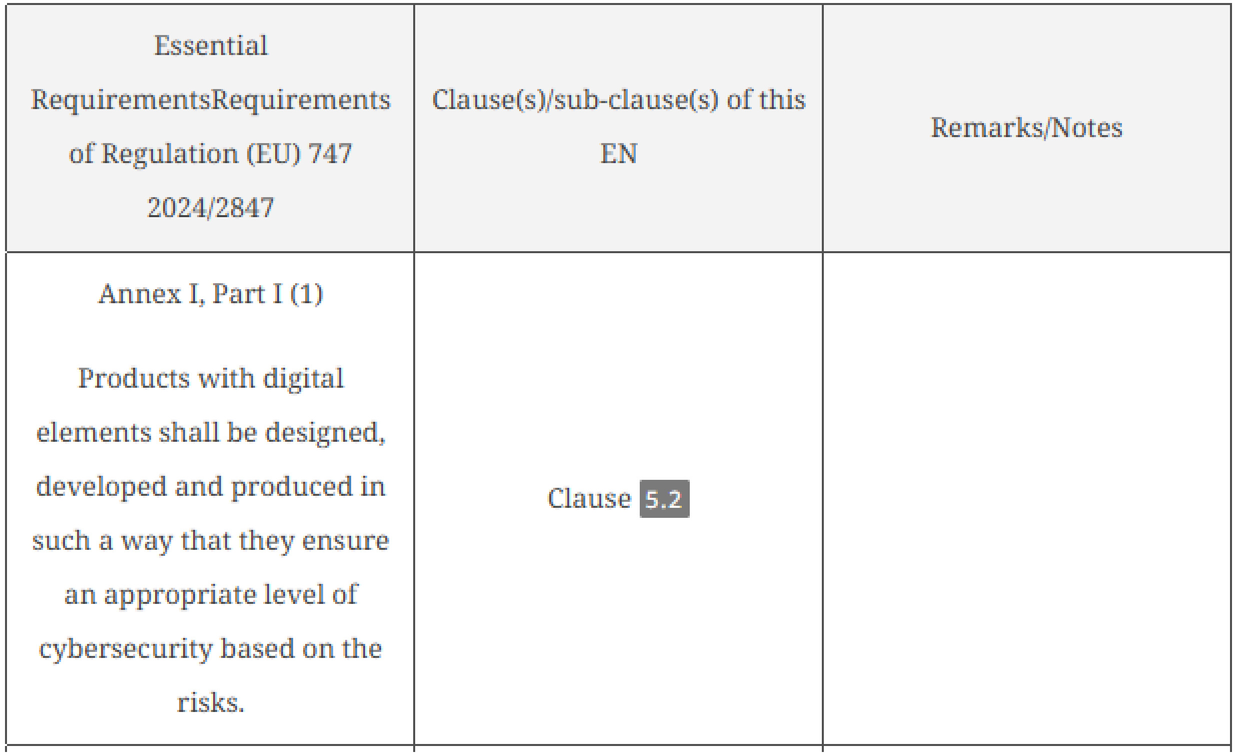
- Mapping with Annex I, Part I

All covered

- Mapping with Annex I, Part II

All covered

Complete PoC



Essential RequirementsRequirements of Regulation (EU) 747 2024/2847	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
Annex I, Part I (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.	Clause 5.2	

…

Conclusions

What next?

- Presentation will be uploaded for consultation
- Provide us with your first feedback and questions, in the coming days
- A deep-dive session is planned on March 2nd with the expert group to address your questions and our main challenges
- Field experts are welcome to join the group via their national standardisation bodies to accelerate towards completion

Thank you !

Enrico Frumento

https://www.linkedin.com/in/enricofrumento/

www.cencenelec.eu

Follow us:

Tag us @Standards4EU