European Standardization Organizations

CRA Standards Unlocked: Deep Dive Session on Cybersecurity Requirements for Smart meter gateways (part 1)

We start at 13:00 CET

Webinar moderator

Els SOMERS

Project Manager

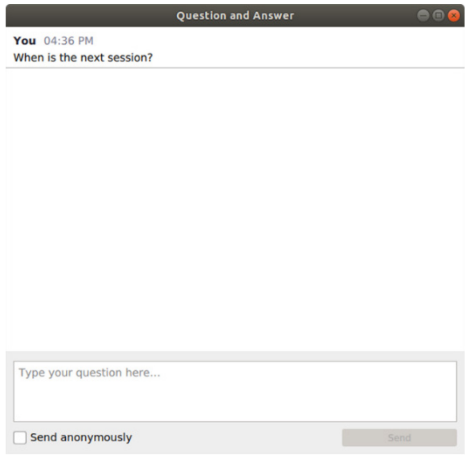
Public Relations

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



- 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 speakers today

Enrico Frumento

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

Your speakers today

Jürgen Blümer

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

Introduction

Opening Objectives

- What we will cover
  - scope/structure + 2 technical deep dives + annexes ZA/D
- What we are *not* doing
  - no vendor specifics;
  - no implementation mandates
- Q&A format:
  - 2 embedded Q&A slots + final open Q&A;

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

Scope & boundaries of the SMGW draft (what is in / out)

- **In-scope (SMGW product boundary)**
- **Smart Meter Gateway (SMGW) as the product with digital elements**
  - The draft targets the SMGW as the primary object for cybersecurity requirements and assessment expectations.
- **Interfaces and security-relevant functions exposed by the SMGW**
  - Focus is on how the SMGW controls communications and access across its interfaces (e.g., towards metering domain / local domain / wide-area).
- **Lifecycle-related cybersecurity capabilities**
  - Secure update, vulnerability handling, logging/monitoring, and evidence expectations are treated as part of the product's cybersecurity posture.

Scope & boundaries of the SMGW draft (what is in / out)

- **Out-of-scope (but relevant as assumptions / dependencies)**
- **External systems are not "standardised" here**
  - Head-end systems, operator SOC processes, external service platforms, and market-specific operational procedures are treated as dependencies/assumptions rather than in-scope products. *(Boundary discussion is welcome in Q&A.)*
- **End devices are not re-specified as products**
  - Smart meters or other downstream devices may be involved in use cases and risk factors, but the draft remains SMGW-focused.
- **No vendor-specific implementation mandates**
  - The draft expresses requirements and assessment criteria, not proprietary design choices.

Legal Overview & WG structure

Legal overview (ii)

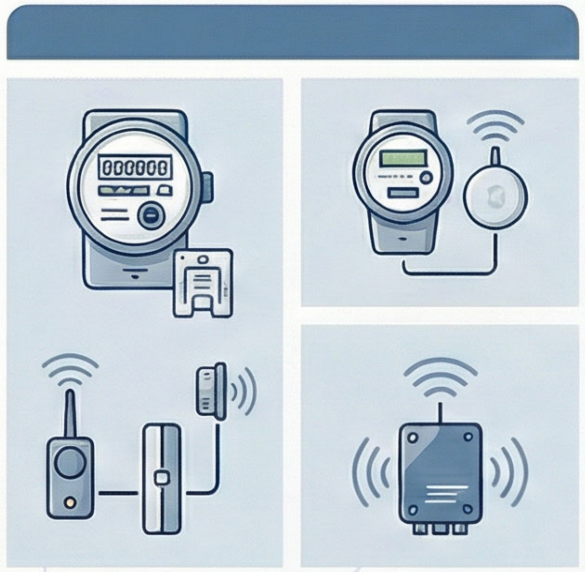
- Implementing Regulation (EU)2025/2392, 28.11.2025, definition on what a SMGW is (definitive)

*"**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.*

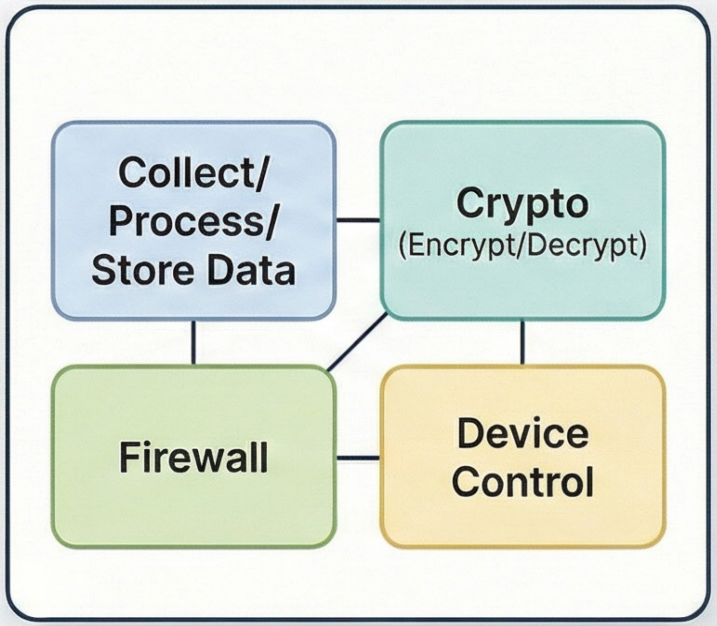
*This category includes **but is not limited** to smart meter gateways related to smart metering systems measuring **electricity** as defined in Article 2(23) of Directive (EU) 2019/944.*

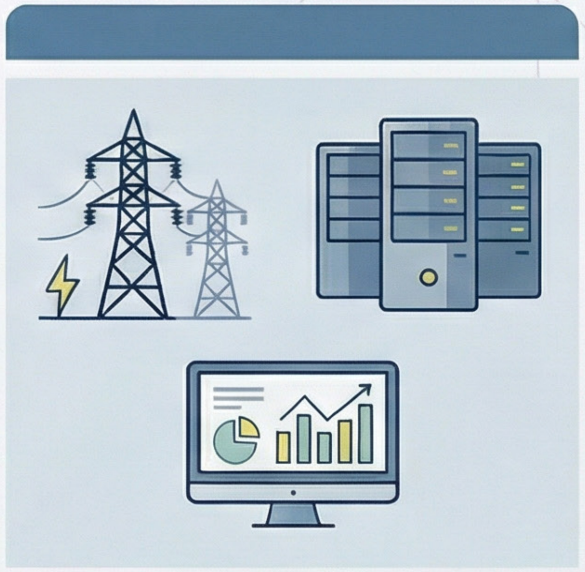
*It **may** also include smart meter gateways used in other smart metering systems measuring consumption of **other sources of energy** such as **gas** or **heat**, **provided that the gateway meets this description**."*

Smart Meter Gateway:
The Secure Central Communication Hub



Smart Metering System
(meters + connected components)





Authorised Third Parties
(utility providers, etc.)

Applies to: Electricity; optionally Gas/Heat

Team

Expert group

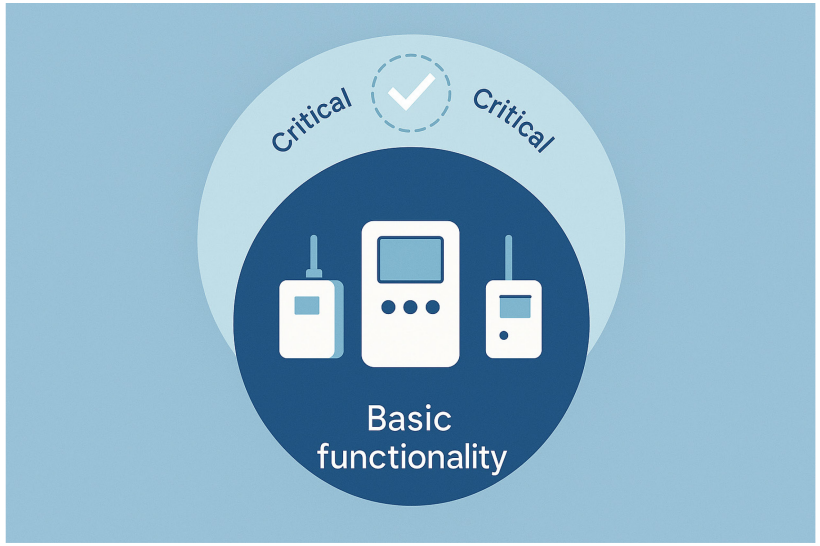
Torben Markussen Kamstrup	Willem Strabbing ESMIG	Eugen Mayer PPC	Alia Fourati EDF	Michael Buss MeterPS CLC TC13 Chair
Andreas Resch BSI	Andy Neidert BSI	Simon Dunkley Itron	Daniel Garcia Miralles Gridspertise	Enrico Frumento (Rapporteur) Cefriel
Riccardo Fiorelli STMicroelectronics	Michael Buss Meterps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

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 we want to validate today (expert feedback targets)

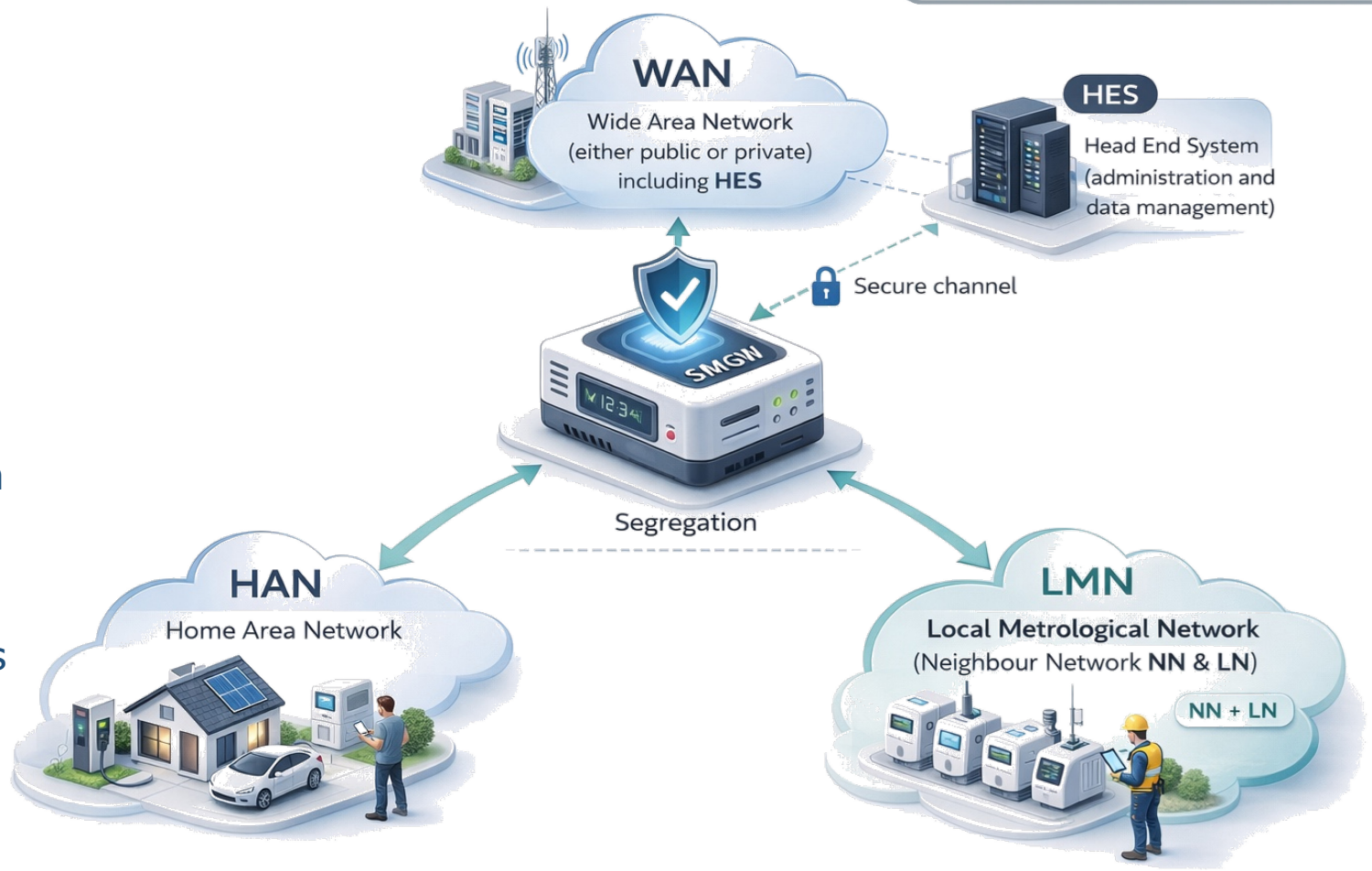
- Are product boundaries and assumptions correct for the market?
- Are the assumptions regarding architecture and operational environment correct for the market?
- Is the capability-based / conditional applicability approach workable?
- Are the SMGW-specific risk factors complete and objectively measurable?
- Are assessment criteria and expected evidence realistic for manufacturers?
- Where does the draft diverge from Common Criteria / BSI PP expectations?

What an SMGW does

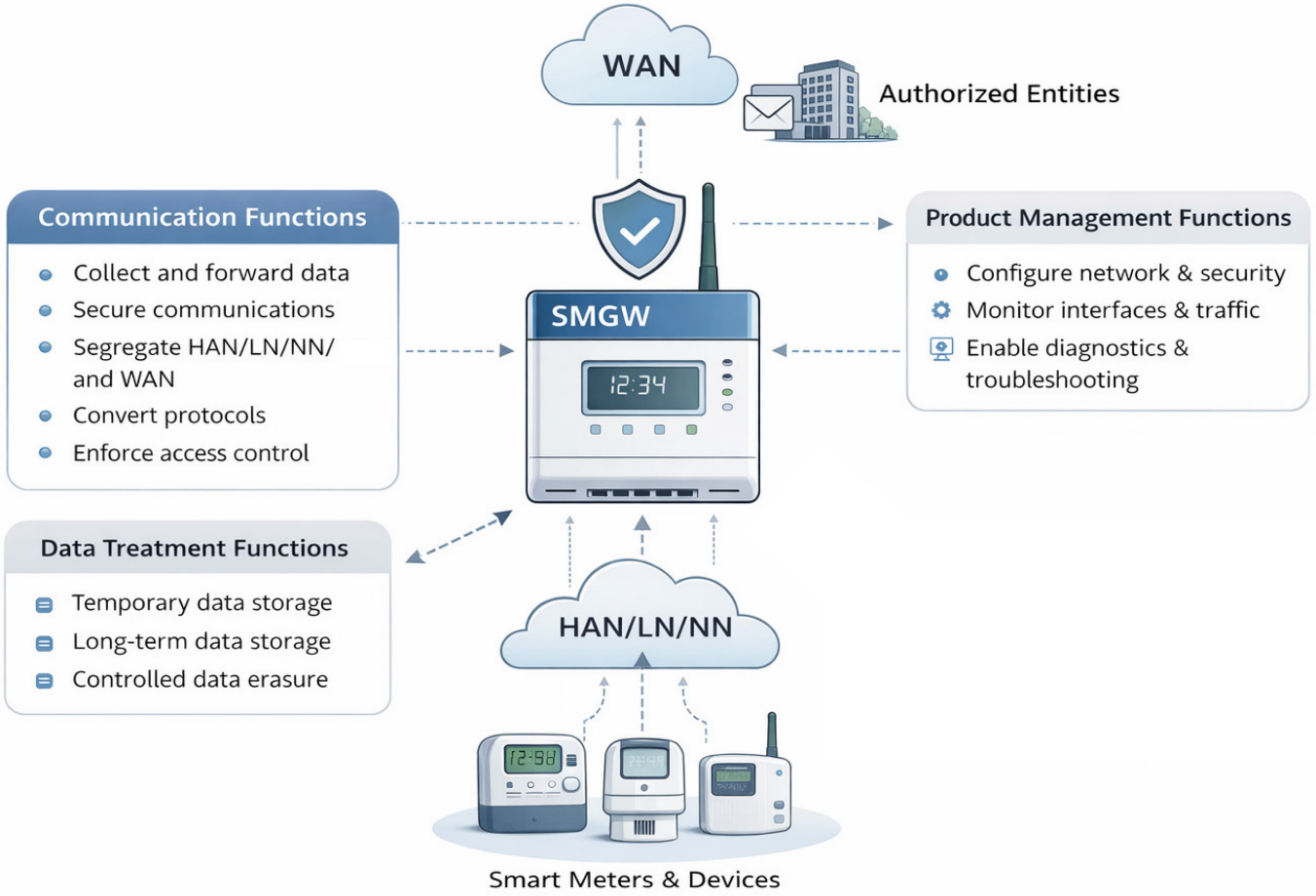
What an SMGW does (general view)

- **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)



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

SMGW is a system of systems

SMGW is a system of systems

- **SMGW is not a single component**
  - It is a system-of-systems: hardware, firmware, software, interfaces, and lifecycle mechanisms.
- **Assessment needs decomposition**
  - Evidence typically exists at multiple levels (platform security, interface controls, update channel, logging).
- **Why this matters later**
  - Requirement assessment criteria must be testable against the right layer and interface (avoid mismatched evidence).

Capability model: core vs optional capabilities (impact on applicability)

- Principal SMGW capabilities: metering data collection, secure communication, authorised access
- Optional capabilities that increase exposure: data sharing to third parties, command reception, device control
- Applicability principle: requirements depend on capabilities + operational environment + risks
- **Discussion prompt**: Which capabilities should trigger 'advanced/critical' expectations?

Cybersecurity challenges

What does critical imply?

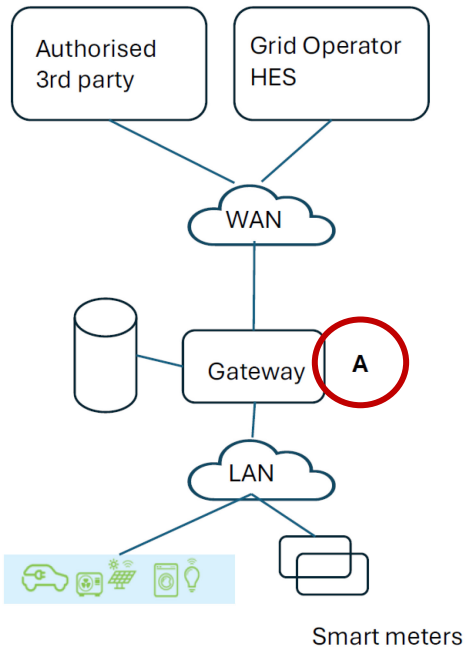
- From an ATT&CK for ICS perspective, smart meter gateways may be targeted through techniques such as **Valid Accounts** (credential abuse), **Exploitation of Remote Services**, or **Modify Parameter/Modify Control Logic** if the gateway supports control functions. Given their cryptographic and firewalling roles, **misconfiguration** or **weak key management** may undermine the entire trust model of the metering ecosystem.
- For sustainable systems, the risk extends beyond operational disruption. **Manipulated smart meter data can distort energy optimisation models, carbon accounting processes, and regulatory compliance reporting**. Consequently, smart meter gateways must be analysed not only as communication devices but as security-critical control points within modern smart grids.

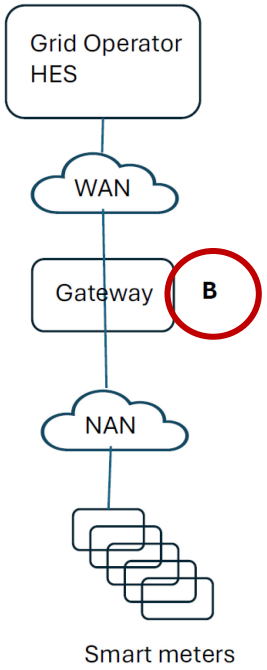
Challenges

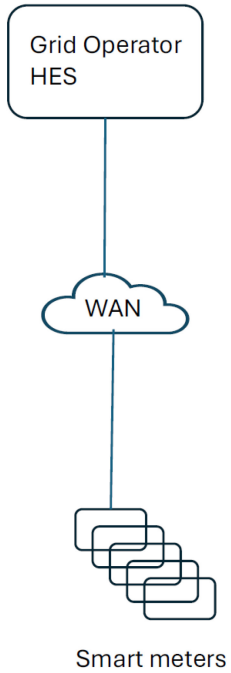
- **EU's heterogeneous landscape of SMGW**
  - different products and architectures in the various member states. The electricity market is not yet harmonised!

- 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
  - may include Data Concentrators and Remote Data Processing RDPSs, if not autonomous
  - considered a CRA critical gateway
- **Others ..**

Capability model: What is a SMGW really?

- The Product landscape in Europe is our challenge.
- Diversity in preparation environment, deployment, and role within the smart grid
- Concentrators vs full gateways
- Technological diversities
- etc

- **Question**: Do you have another kind of SMGWs that might not be considered?

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 (on critical infrastructures)

- 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?

- **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)**

Q&A Slot: Security constrains

- **Which SMGW assets do you consider the most critical to protect first?**
  (e.g., metering data, cryptographic keys, tamper alarms / security events).
- **Which "what can go wrong" scenarios are most relevant in your deployments?**
  (e.g., unauthorised disclosure of metering data; unauthorised commands towards smart meters).
- **Where do you see the main responsibility boundary?**
  Product security (SMGW design) vs operational environment controls (deployment, monitoring).

- **Footer (parking lot):**
  Implementation specifics, crypto choices, and detailed clause interpretation → parked for later deep dives (authorisation / updates / logging).

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

How to read the draft (body vs annexes; normative vs informative)

- **Draft "reading map"**
- **Main body = requirements + assessment orientation**
  - Use the main clauses to understand: *what is required*, *when it applies*, and *how conformity can be assessed (assessment criteria / supporting evidence).*
- **Annexes = structured context and traceability**
  - **Annexes A/B/C (contextual):** assets, functions, threat landscape to support consistent interpretation.
  - **Annex D (bridge):** Common Criteria / product class mapping reference point for stakeholders coming from CC/PP approaches.
  - **Annex ZA (regulatory mapping):** mapping to CRA essential requirements to support presumption of conformity.
- **Normative vs informative (practical takeaway)**
  - **Normative content** (what drives conformity): requirements + any normative annexes as defined by the draft structure.
  - **Informative content** (what drives shared understanding): assets/functions/threats/risk factors and mapping aids—used to interpret, justify, and apply requirements consistently.

Q&A Slot: Scope & boundaries (strict clarifications)

- **Boundary with adjacent products and systems**
  - *Where do you see the most critical boundary for SMGW cybersecurity assessment: SMGW vs smart meter, SMGW vs head-end system, or SMGW vs external service platforms?*
- **Interface ownership and assumptions**
  - *Which SMGW interfaces create the highest ambiguity in terms of responsibility (product vs operator environment) and should be clarified in the draft?*
- **Capability-driven scope triggers**
  - *Which optional capabilities (beyond the "principal" gateway role) do you believe should trigger stricter applicability or stronger evidence expectations (e.g. third-party firmware)?*

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.

Operational environment → applicability decisions (practical view)

- **Uncontrolled / Controlled / Monitored environments:** what evidence is expected in each case
  - *Example: remote management allowed only with additional controls and monitoring*
  - *Example: stronger logging / tamper evidence expectations in monitored environments*
- **Discussion prompt**: are these categories sufficient for real deployments?

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.
  - Reliable Time
- **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 categories

Threats are divided into **main** categories:

- Data Modification and disclosure
- Threats on SW
- Threats on HW
- Threats on Communication
- Threats on keys /cryptographic
- Physical Threats
- Supply Chain & Delivery Threats

Main Threats details

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
- T.Availability
  - Attacker blocks the availability of data
- T.Tests
  - Rootkits in firmware; Backdoors left from development/testing

Main Threats details

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 Threats details

Threats are divided into categories:

- T.Firmware_Malfunction
  - Attacker takes advantage of:
    - bypassing the secure boot
    - Logic bombs triggered by time or conditions
    - Buffer overflows
    - Stack/heap corruption
    - Use-after-free vulnerabilities
    - Race conditions
    - Insecure deserialization
- T.Firmware_Integrity
  - Attacker tries to manipulate or downgrade the installed Firmware or compromise the boot loader
- T.Firmware_Replace
  - Attacker tries to install unauthorized firmware or unsigned / weakly signed firmware

Main Threats details

Threats are divided into categories:

- T.Fake_Devices
  - Attackers could try to connect unknown equipment (meter / CLS) to the product to disrupt communication or to introduce malicious data including replay attacks.
- T.Communicaton_Disclosure
  - Attacker has access to data communicated between product and its peers
- T.Communication_Manipulation
  - Attacker manipulates data communicated between product and its peers
- T.Control_Integrity
  - Attacker could try to manipulate control data transfered from Smart Meter Gateway to LMN or CLS devices
- T.Key_Integrity
  - Compromised cryptographic keys

Main Threats details

Threats are divided into categories:

- T.Key_Disclose
  - Key extraction from memory or Insecure key storage
  - Reuse of keys across devices
  - Missing key rotation storage
- T.Key_Weakness
  - Weak key generation
  - Use of deprecated algorithms
  - Insufficient key lengths
  - Poor random number generation
  - Incorrect certificate validation
  - Broken certificate chains
  - Expired or revoked certificates not detected

Main Threats details

Threats are divided into categories:

- Physical Threats
  - T.Casing
  - T.DigitalElements
  - T.Theft
  - T.Destruction
  - T.Manufacturing
  - T.InitialConfiguration
  - T.Decommissioning_Failure

Operational environment → threats

- **Do you feel comfortable with the categories of threats?**
- **Do you expect to see other threats?**

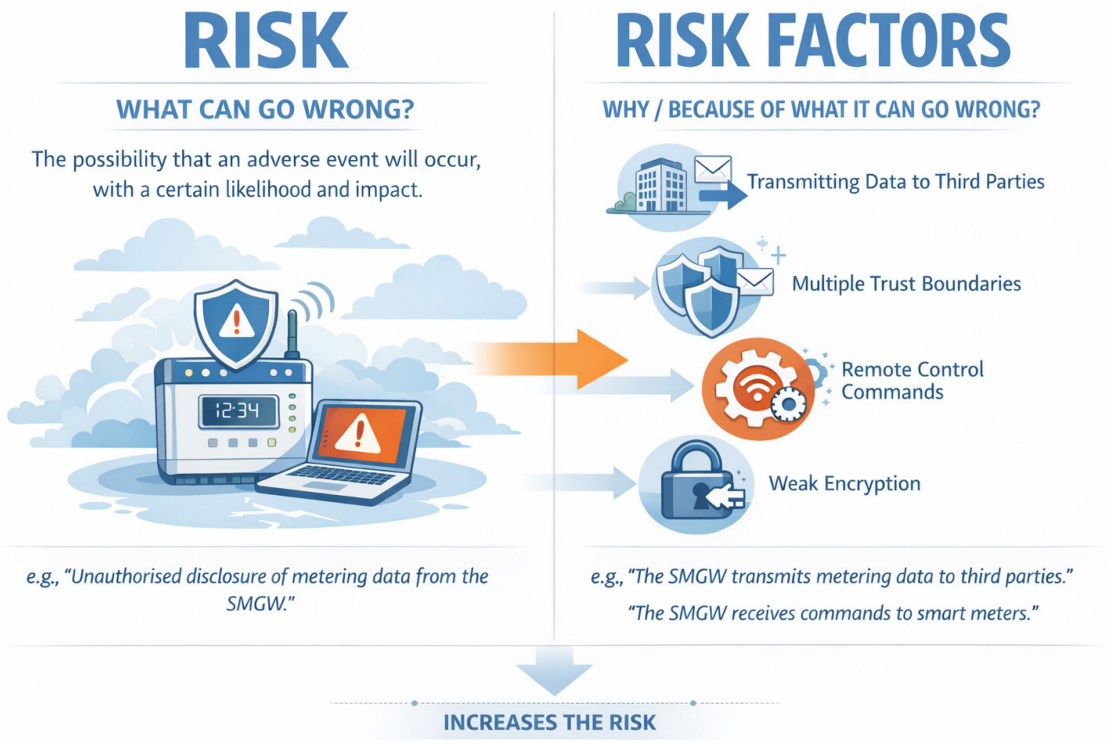
Main Risk Factors

- 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, …)

What is a risk factor

- **Generally speaking:** *risk* is **what can go wrong**, *risk factor* is **why / because of what it can go wrong**.

- **Risk:** the possibility that an adverse event will occur, with a certain likelihood and impact *(e.g., "Unauthorised disclosure of metering data from the SMGW").*
- **Risk factor:** a characteristic or condition that increases the likelihood or impact of that risk *(e.g., "The SMGW transmits metering data to third parties", which increases exposure and the number of trust boundaries or "The SMGW sends commands to smart meters").*



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

Operational environment → risk and risk factors

- **Do you see other risk factors and requirements to be included/removed?**

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

Why Annex ZA matters (CRA mapping & presumption of conformity logic)

- **What Annex ZA provides (in practice)**
- **A structured mapping between the SMGW standard and CRA essential requirements**
  - Used to demonstrate how the standard supports CRA compliance by design (traceability).
- **A "regulatory view" of the technical text**
  - Helps stakeholders (manufacturers, authorities, SMEs, OSS) identify where each CRA requirement is addressed in the standard.
- **A basis for presumption of conformity**
  - Annex ZA is the bridge to the regulatory framework: if applied correctly, it supports the presumption logic linked to CRA essential requirements.

- **What Annex ZA is *not***
- **Not an extra set of requirements**
  - It is a mapping/traceability annex; the "shall" requirements remain in the main body (and any normative annexes as defined).
- **Not a substitute for applicability decisions**
  - Applicability still depends on the draft's context: operational environment, risk factors, capabilities.

Annex ZA

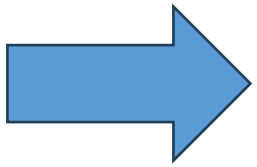
Mapping between this standard and the essential requirements of CRA regulation

- 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

Operational environment → risk and risk factors

- **Are you planning to use the standard?**
- **Is your device type covered?**
- **What did you find helpful in this presentation?**
- **Do you have any suggestions/concerns linked to the scope or the content of this standard?**

What next?

- Presentation will be uploaded for consultation
- A deep-dive session part 2 is planned before the first public enquiry 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