

AQUA's Position on the Classification of Smart Meters and Gateways under the European Cyber Resilience Act (CRA)

[Reference: Official Regulation \(EU\) 2024/2847](#)

Reference: Draft standards prEN40000-1-1 /-2/-3/-4/-5 on horizontal cybersecurity requirements for products in scope of CRA.

Purpose and Scope

This position paper provides guidance on the classification of smart metering devices within the framework of the Cyber Resilience Act (CRA). It reflects a common industry understanding of how smart meters should be categorized under the regulation.

This document is not legally binding, and compliance with this guidance does not guarantee conformity with the CRA. Manufacturers remain responsible for conducting their own product classification and declaration of conformity.

Context: The Cyber Resilience Act

The Cyber Resilience Act establishes **horizontal cybersecurity requirements** for products with digital elements placed on the European Union market and introduces a **risk-based classification framework**.

Under the CRA:

- Products are subject to **essential cybersecurity requirements** (Annex I)
- Certain products are designated as:
 - **Important products with digital elements** (Annex III)
 - **Critical products with digital elements** (Annex IV)

These categories determine the applicable conformity assessment procedures (Article 32 and Annex VIII of CRA regulation).

The CRA follows a **function-based classification approach**, whereby products are categorized based on their **intended purpose and core functionality**, rather than the sector of deployment (Recital – risk-based approach and proportionality principle).

Importance of Smart Metering

Smart Meters are measuring instruments with additional functionalities, one of which is communication. Smart meters measure and transmit consumption data (water, thermal energy, gas, or electricity) via communication technologies to billing or management systems.

As previously highlighted by AQUA, smart metering systems:

- Enable efficient resource management
- Support digitalization of infrastructure
- Contribute to sustainability and energy efficiency objectives

While deployed in critical infrastructure sectors, smart meter systems primarily function as **measurement and communication devices**, not as cybersecurity or control systems.

CRA Product Classification Framework

Critical products (Annex IV CRA)

Annex IV defines **critical products with digital elements**, typically including:

- Hardware security modules (HSMs)
- Smart cards and secure cryptographic devices
- Trusted execution environments
- Smart meter gateways within smart metering systems

These products are subject to the **European cybersecurity certification schemes** (Article 32 of CRA).

Important products (Annex III CRA)

Annex III lists categories of products with digital elements that are considered **important due to their cybersecurity relevance**, including:

- Operating systems
- Network management systems
- Routers, switches, and firewalls
- Identity management and access control systems
-

These products are subject to **stricter conformity assessment procedures**, including third-party involvement in certain cases (Articles 24–26 CRA).

Default category

Products that are **not listed in Annex III or Annex IV** fall into the **default category** and are subject to:

- Essential requirements (Annex I CRA)
 - Internal conformity assessment procedures (Article 24 CRA) based on harmonized standards
-

AQUA's Position on Smart Meter Classification

AQUA considers that **smart meters placed on the market by its members fall under the *default category*** of the CRA.

Justification

1. Not listed in Annex III or Annex IV

Smart meters are not included in the list of **important products (Annex III)** or **critical products (Annex IV)**.

Accordingly, they fall under the **default conformity assessment procedure** (Article 24 CRA).

2. Core functionality does not match Annex III

Annex III covers products whose **primary function is cybersecurity-relevant**, such as routers, firewalls, or identity management systems.

Smart meters:

- Measure consumption data
- Transmit data within smart metering systems

They do not provide communication **network control, system management, or security enforcement**, and therefore do not meet Annex III criteria.

3. No alignment with Annex IV (critical products)

Annex IV applies to products whose **core purpose is to ensure cryptographic trust**, such as HSMs or secure elements.

Smart meters may use cryptography, but only as a **supporting function**, not as their primary purpose.

They therefore do not qualify as **critical products**.

4. Sector of use is not decisive

The CRA classification is based on **product functionality**, not on whether a product is used in **critical infrastructure**.

The deployment of smart meters in water or energy systems does not alter their classification.

5. Typical architecture confirms endpoint role

Smart meters are **endpoint IoT devices** operating within a broader system architecture:

- No routing or gateway function

- No central system control
- Reliance on external systems for security orchestration

This role is consistent with **default-category products**.

6. Case-by-case principle (exception only)

In line with the CRA, classification must be assessed case-by-case.

Only where a device's **primary function changes** (e.g., acting as a gateway or providing cybersecurity services) could Annex III become relevant.

Such cases are **not representative of standard smart meters**.

AQUA's Position on Smart Metering Gateways Classification

Smart meters communicate their measurement data using communication networks. The network infrastructure could be dedicated to smart metering exclusively, global IoT networks or other communication networks. Typical network infrastructure components are gateways.

The gateway may include core functions like

- Receive encrypted Smart Meter Data
- Store encrypted Smart Meter Data
- Transmit stored Smart Meter Data including Meta information
- Forward encrypted and authorized commands to the Smart Meter
- Process Smart Meter Data while decrypting
- Other vertical applications may enforce additional features

Aqua considers applying the function-based approach to define the gateway classification while reflecting different approaches already available on the market.

Aqua considers gateways as **default products with digital elements** if their core function is limited to

- Acting as transport device for end device information
- Do not create commands by themselves to control network end-devices
- Do not act as root of trust for devices in the network
- Do not execute authorization on application layer

Aqua considers gateways not meeting the above listed conditions as **critical products with digital elements** covered by the Smart Meter Gateway (CRA, Annex IV, Top 2).

Devices in this class shall have at least one of the below listed features:

- Decryption of received end point information
- Creating additional information based on decrypted endpoint information
- Autonomous generation of commands executed on end points
- Termination of application layer security for end points

An example of a product that may fall into the critical category, depending on its intended purpose and functionality, is the German BSI Smart Meter Gateway as specified in BSI Technical Guideline BSI TR-03109-1.

Justification:

1. Not listed in Annex III or Annex IV

Limited communication or transport components that do not qualify as smart meter gateways within the meaning of Annex IV may fall under the default category, subject to product-specific assessment based on intended purpose, architecture and core functionality

2. Core functionality does not match Annex III

Annex III covers products whose **primary function is cybersecurity-relevant**, such as routers, firewalls, or identity management systems.

Gateways for Smart Meters not supporting core functions **as network control, system management, or security enforcement** therefore do not meet in Annex III criteria.

3. No alignment with Annex IV (critical products)

Annex IV applies to products whose **core purpose is to ensure cryptographic trust**, such as HSMs or secure elements. Gateways may use cryptography, but only as a **supporting function**, not as their primary purpose. Gateways not acting as source of trust therefore not qualified as critical products.

4. Sector of use is not decisive

The CRA classification is based on **product functionality**, not on whether a product is used in **critical infrastructure**. The categorization shall not be limited to Smart Metering Gateways.

5. Case-by-case principle (exception only)

In line with the CRA, classification must be assessed case-by-case.

AQUA's Recommendation

AQUA recommends:

- Application of a **function-based classification aligned with Annex III and IV CRA**
- Avoidance of classification based on deployment context rather than product functionality
- Enabling Manufacturer self-declaration based on harmonized standards EN/prEN40000 series.

- A **harmonized interpretation across Member States** confirming that smart meters fall under the default category
- A **harmonized interpretation across Member States** confirming that gateways fall under the default category if they transport data without terminating End to End security.
- A **harmonized interpretation across Member States** confirming that gateways fall under the critical category if they act as a source of trust or aim to decrypt data, generate new information based on the decrypted data or initiate actions autonomously.

AQUA encourages policymakers to ensure **legal certainty and proportionality**, in line with the objectives of the CRA.

Outlook

The CRA complements existing frameworks such as the RED Delegated Regulation (EU) 2022/30, contributing to a coherent regulatory framework for connected devices.

AQUA will continue to engage with EU institutions and standardization bodies to ensure that smart metering remains aligned with evolving cybersecurity requirements.

About AQUA

AQUA primarily represents family-owned small and medium-sized enterprises that provide products and solutions for smart metering infrastructure, energy efficiency and water resilience across Europe.

Version: 1.0

By presenting this position, AQUA aims to contribute to a consistent, proportionate, and innovation-friendly implementation of the Cyber Resilience Act within the European Union.