UWPA Cybersecurity Compliance Notes

Table of content

Purpose

This document provides extended cybersecurity requirements for the UWPA LoRaWAN® Wireless Endpoint Gateway. It complements the installation manual by detailing the conditions necessary to ensure compliance with Directive 2014/53/EU (RED), Article 3(3)(d) – protection of the network.

These requirements must be followed by installers, system integrators and maintenance personnel.

Compliance with this essential requirement is demonstrated through the harmonised standard EN 18031-1:2024 "Common security requirements for radio equipment — Part 1: Internet connected radio equipment", referenced in Annex I to Commission Implementing Decision (EU) 2022/2191 as amended by Commission Implementing Decision (EU) 2025/138, with the restrictions set out therein. The UWPA implementation falls outside the scope of those restrictions, and the conformity assessment is carried out under Module A (internal production control) as set out in Annex II to Directive 2014/53/EU.

Security Concept

The cybersecurity of the UWPA device is ensured through two complementary pillars.

Protection of local interfaces (USB, RS485). Access to the device configuration and to the data exchanged over local interfaces is protected by the operating environment. This approach relies on:

- restricted physical access to the device;
- controlled installation environment (key-locked electrical panel);
- a factory-applied tamper-evident seal that makes unauthorised opening of the device housing detectable.

Protection of radio communications (LoRaWAN). Data transmitted over the radio interface are protected by the native security features of the LoRaWAN protocol. The device operates exclusively in Over-The-Air Activation (OTAA) mode; all radio frames are authenticated and encrypted using protocol-native cryptography. The UWPA does not accept configuration commands, parameter reads, or firmware updates over the radio interface; the LoRaWAN interface is functionally unidirectional from an operational standpoint.

Failure to maintain the installation conditions described in this document compromises the first pillar and invalidates the security assurances stated in the EU Declaration of Conformity.

Prescribed Installation Environment

- The device must be installed inside a key-locked electrical panel.
- Access to the panel must be restricted to authorized and qualified personnel only.
- The device must not be installed in areas accessible to unauthorized personnel.
- All physical interfaces (USB, RS485, power terminals) must be inaccessible without opening the panel.

Physical Security Requirements

Access Control

- Only personnel explicitly authorized by the system owner/operator may access the device.
- Unauthorized access to the device or its interfaces is strictly prohibited.

Device Handling

- Do not expose the device to environments where it can be physically tampered with.
- Avoid installations that allow direct access without tools or authorization.

Tamper-Evident Seal

The device is equipped with a factory-applied tamper-evident seal.

Initial Installation

- Verify that the seal is present and intact before installation.
- Do not install the device if the seal is:
    - Missing
    - Damaged

- Showing signs of tampering

If any issue is detected, contact Carlo Gavazzi support.

Maintenance and Inspection

- Inspect the seal during periodic maintenance.
- A damaged or missing seal indicates potential unauthorized access.
- Report any anomalies to the system owner.

Housing Opening

- Opening the device housing irreversibly breaks the seal.
- The device may only be opened by Carlo Gavazzi authorized personnel.
- Unauthorized opening invalidates cybersecurity compliance.

Maintenance Requirements

- Perform periodic inspections of installation conditions.
- Ensure that:
  - The electrical panel remains locked
  - Access restrictions are enforced
  - The tamper seal is intact
- Any deviation from prescribed conditions must be corrected immediately.

Non-Updatable Firmware

The UWPA firmware is permanently stored in read-only memory and cannot be modified through any interface — neither remotely, nor locally via USB, nor through any other means. This design provides two cybersecurity guarantees: the integrity of the firmware running on the device is preserved throughout its operational life, and the firmware is inherently protected against tampering attempts, including attempts that would require physical access to the device.

In the event that a relevant firmware issue is identified, whether related to cybersecurity, functionality, or network behaviour, Carlo Gavazzi Controls S.p.A. defines the appropriate corrective action on a case-by-case basis. This may include updated documentation, configuration changes, or other mitigation measures; physical replacement of the affected device is adopted as a last resort when no other effective mitigation is available.

Compliance Warning

Compliance with Directive 2014/53/EU (RED) cybersecurity requirements is valid only if all conditions described in this document are met.

If the device is installed or operated outside these conditions:

- Cybersecurity protections may be compromised
- Compliance assumptions are no longer valid

Responsibility

The installer and system operator are responsible for:

- Ensuring correct installation conditions
- Maintaining physical security over time
- Preventing unauthorized access
- Promptly reporting any sign of tampering, seal damage, or unauthorized access to Carlo Gavazzi