AKCP sensorProbe+ CRA Readiness Statement

Nov 23, 2026

AKCP is in scope of the EU Cyber Resilience Act (Regulation (EU) 2024/2847, "CRA") as manufacturer of the sensorProbe+ family. AKCP will place CRA-conformant products on the EU market by 11 December 2027. For the vulnerability and incident reporting obligations that have applied since 11 September 2026, AKCP is registered on ENISA's Single Reporting Platform and receives vulnerability reports at security@akcp.com.

This statement is for customers, dealers, distributors and OEM partners of AKCP products in the EU.

Summary of commitments

Commitment	Status
Article 14 reporting of actively exploited vulnerabilities and severe incidents via ENISA's Single Reporting Platform	Active: registered on ENISA's Single Reporting Platform (November 2026); vulnerability reports received at security@akcp.com
Conformity with the CRA essential requirements (Annex I) through internal control (Module A), EU Declaration of Conformity and CE marking	By 11 December 2027
Machine-readable Software Bill of Materials (CycloneDX) for each firmware release	Available on request from Q1 2027; published with firmware downloads afterwards
Security architecture overview and cybersecurity risk assessment summary	Available to customers and partners on request (under NDA) from Q3 2027
Security updates free of charge for the support period	Support end date (month and year) stated for each model at the time of purchase. It is at least 5 years from when each unit is placed on the EU market, and longer where the expected use time warrants it. Each security update stays downloadable for at least 10 years after release
Security enhancements to firmware, default configuration and wireless sensors	Rolling out during 2027 (section 5)

1. Products covered

This statement covers AKCP's STM32H7-based monitoring controllers, their firmware and the LoRa wireless sensors used with them:

- **Controllers:** SP1+, SP2+, SP2+ LCD, SPX+ (incl. SPXN4/8/16), PPX+ and the Wireless Tunnel Server SP-WTS, including optional 4G LTE cellular modem variants (on SP2+, SP2+ LCD, SPX+ and SP-WTS).
- **Wireless sensors:** SP-WT transmitters and the BOS and WTS battery/wireless tunnel sensors (EU868).
- **New models:** products released from 2027 onwards are developed under the same CRA programme.

All products currently sold are H7-based; earlier F4/F7-based hardware is no longer sold new. Units sold under a partner's own brand are covered by the shared responsibilities in section 6.

2. Regulatory position and conformity route

AKCP classifies the sensorProbe+ products as "default" products with digital elements. Their core function is B2B data-centre environmental monitoring and rack access control. They are not routers, network management systems or consumer smart-home security devices under CRA Annex III, as described in Implementing Regulation (EU) 2025/2392.

- **Conformity route:** internal control (Module A), Annex VII technical documentation, EU Declaration of Conformity and CE marking under the CRA, by 11 December 2027.
- **Standards:** AKCP designs against the Annex I essential requirements and will apply the CRA harmonised standards (EN 40000 series) once they are cited in the Official Journal. IEC 62443-4-1/4-2 and ETSI EN 303 645 are used as reference.
- **Radio variants** (SP-WTS and LoRa sensors, optional 4G LTE cellular modem variants on SP2+, SP2+ LCD, SPX+ and SP-WTS): until 10 December 2027 these also fall under the Radio Equipment Directive cybersecurity requirements (Delegated Regulation (EU) 2022/30, EN 18031-1). The CRA replaces those rules from 11 December 2027.

3. Vulnerability handling and Article 14 reporting

AKCP monitors, fixes and reports vulnerabilities in its products under CRA Articles 13 and 14 and its coordinated vulnerability disclosure (CVD) policy.

- **Reporting to authorities:** AKCP is registered on ENISA's Single Reporting Platform and notifies actively exploited vulnerabilities and severe incidents through it: an early warning within 24 hours, a notification within 72 hours, and a final report (14 days after a fix for vulnerabilities, one month after notification for incidents).
- **Informing customers and partners:** AKCP notifies affected own-brand (OEM) partners of an actively exploited vulnerability or severe incident within 12 hours of becoming aware of it, so they can meet their own reporting duties. Dealers, distributors and end users are informed through security advisories with affected versions and mitigations.
- **Fixing:** engineering resources are assigned as soon as a vulnerability is confirmed. Security fixes are delivered as firmware updates, free of charge, with a security advisory stating affected and fixed versions.
- **Detection:** automated static analysis and sanitizer testing in the build workflow, vulnerability scanning, SBOM-based monitoring of third-party components (from Q1 2027), and independent penetration testing (from 2027).
- **Reporting a vulnerability to AKCP:** security@akcp.com. AKCP will publish its coordinated vulnerability disclosure policy and a security.txt file on akcp.com by the end of December 2026.

4. Documentation available to customers and partners

Document	Content	Availability
Software Bill of Materials	CycloneDX SBOM generated automatically in AKCP's build pipeline for every firmware release: RTOS, network and crypto libraries, radio stack and Web UI components, with versions and hashes	On request from Q1 2027; later published with each firmware download
Security architecture overview	Trust boundaries, interfaces and data flows, authentication and cryptography, secure boot and update chain, logging	On request under NDA, Q3 2027
Cybersecurity risk assessment summary	Assets, threats and how each Annex I requirement is addressed	On request under NDA, Q3 2027
EU Declaration of Conformity (CRA)	Per product family	By 11 December 2027
User security information (CRA Annex II)	Support period, secure installation and configuration, update procedure, security contact	With product documentation by 11 December 2027
Installation hardening guidance	Recommended configuration changes at installation	Available now on akcp.com

The full technical documentation is held by AKCP and made available to market surveillance authorities on request.

5. Planned 2027 security enhancements

AKCP's 2027 firmware releases strengthen the products in six areas, delivered as free updates to products in the field where the hardware allows:

- **Firmware authenticity:** cryptographically signed firmware and bootloader images, verified on the device before installation, with hardware flash read and write protection.
- **Secure by default:** mandatory credential setup at first start, authentication enforced on all management interfaces, HTTPS by default with a unique certificate generated on each device, and SNMPv3 available on all models with legacy SNMP versions disabled by default.
- **Legacy protocol retirement:** the legacy TCP 5000 server integration is disabled by default during 2027 and removed before 11 December 2027.
- **Wireless sensors:** stronger link protection and signed firmware updates for LoRa sensors.
- **Security logging:** wider coverage of security events, exportable via syslog.
- **Security testing:** SBOM-based component monitoring, protocol fuzzing and annual independent penetration testing.

No disruption to running installations. The new secure defaults (plain HTTP, SNMPv1/v2c and TCP 5000 off) apply to factory defaults, i.e. newly deployed or factory-reset units. An in-place firmware upgrade on an installed unit keeps its active configuration and shows security warnings in the web interface, so live monitoring and integrations keep working.

Until these releases are installed, partners and end users should follow AKCP's installation hardening guidance, in particular changing all default credentials at installation.

6. Dealers, distributors and own-brand partners

EU partners sell AKCP products in one of two ways, and the CRA assigns different roles to each.

Dealers and distributors of AKCP-branded products act as importers or distributors (CRA Articles 19 and 20), and AKCP remains the manufacturer. AKCP provides the CE marking, the EU Declaration of Conformity, user security information, the security contact and security updates. In return, the partner:

- checks that products carry the CE marking and the required documentation;
- as an importer, adds its own name and contact details to the product, its packaging or its documentation;
- passes on any vulnerability or incident information it receives to security@akcp.com;
- forwards AKCP security advisories to its customers where needed.

6. Dealers, distributors and own-brand partners (continued)

Partners selling under their own name or trademark (OEM / own brand) become the CRA manufacturer of those units (Article 21). The table shows how AKCP supports them; the details are set out in a CRA addendum to the supply agreement.

Obligation	Partner (own-brand manufacturer)	AKCP (OEM supplier)
Conformity, EU DoC, CE marking	Issues them for its brand	Supplies conformity evidence and AKCP's own DoC as reference
Technical documentation	Holds it for 10 years	Supplies the technical content, or gives authorities direct access under NDA
SBOM	Keeps it with its documentation	Delivers it with every firmware release
Vulnerability fixes	Distributes updates to its users	Develops and delivers security updates free of charge
Article 14 reporting	Reports for its branded units	Reports for AKCP-branded units; notifies the partner within 12 hours of awareness
User notification	Informs its users	Supplies advisory text and mitigations
Support period	Declares it to its users	Commits in writing to a support period at least as long

7. Milestones

Date	Milestone
11 Sep 2026	Article 14 reporting via ENISA Single Reporting Platform in force; AKCP registered in November 2026
Dec 2026	Coordinated vulnerability disclosure policy, security.txt and security advisories page published on akcp.com; CRA addenda offered to own-brand partners
Q1 2027	CycloneDX SBOMs available on request for every firmware release
2027 (rolling)	Security enhancement releases (section 5)
Q3 2027	Security architecture overview and risk assessment summary available under NDA
By 11 Dec 2027	CRA technical documentation, EU Declaration of Conformity and CE marking; SBOMs published with firmware downloads

8. Contact

- CRA programme and security vulnerabilities: security@akcp.com

This statement reflects AKCP's plans as of the date above, and AKCP will update it at each milestone or whenever its CRA position changes. It is provided for information. It does not change the terms of AKCP's agreements with its customers and partners.