Factsheet

Cyber Resilience Act Compliance

Be one of the first in the market with premium security and a fully certified CE product

Kudelski Labs empowers product manufacturers to meet EU Cyber Resilience Act (CRA) requirements through secure-by-design services, cloud-native trust infrastructure, and full product lifecycle compliance.

Our platform-agnostic approach, combined with our SaaS solution keySTREAM for provisioning and OTA updates, ensures CRA readiness from factory to field. With advisory services, embedded security IP, and certification expertise, Kudelski Labs simplifies compliance, reduces risk, and accelerates time-to-market, helping OEMs lead with premium security and fully certified CE products.

CRA Compliance

The Kudelski Labs Approach

- **Accelerates CRA compliance:** With security-by-design and lifecycle security.
- **Works across any product or vendor:** No silicon lock-in.
- **Supports certification readiness:** With advisory and infrastructure services.
- **Empowers leadership:** With premium security and CRA readiness.
- **Your product focus:** Analysis of how CRA applies to your products.

Kudelski Labs Your CRA Compliance Partner

Secure-by-Design ensures Secure-for-Life:
CRA demands lifecycle security. We help you achieve it from day one.

Platform Agnostic Support:
Any device. Any vendor. No silicon lock-in.

Trusted Certification Partner:
Backed by decades of security expertise and global certification experience.

How it Works

Cyber Resilience Act compliance is achieved through a combination of secure design, product lifecycle tools and certification support.

- Threat analysis and risk assessments (TARA)
- Secure provisioning and onboarding via Kudelski Labs keySTREAM
- Vulnerability management and secure OTA updates
- Embedded security IP (KSE3, KSE5 and PQC modules)

New Devices

OEMs designing new connected products must ensure CRA compliance now. This involves implementing secure-by-design principles, preparing technical documentation and planning for lifecycle security.

The Kudelski Labs approach:

- Advisory Services - architecture guidance, TARA and CRA gap analysis
- keySTREAM - Secure provisioning, onboarding and product lifecycle management
- Security IP Hardware root of trust for secure-by-design chips

In-Field Devices

Explore retrofitting products with secure update mechanisms and unlock vulnerability management via keySTREAM, without disrupting operations.

The Kudelski Labs approach:

- Gap Analysis & Remediation - Identify compliance gaps and create a remediation roadmap
- Lifecycle Security Enablement - Add secure update mechanism and vulnerability management via keySTREAM
- Post-Market Resilience - Detect, respond and patch at scale to maintain compliance

Strategic Intelligence. Impactful Action.

Our semiconductor security expertise is rooted in more than three decades of hardware, software and cybersecurity experience. We use our expertise and technology to protect all key semiconductor assets - devices, identity, data, decisions, commands and actions throughout the lifetime of the device and its ecosystem.

Explore Our Innovations

Contact Us

info@kudelskilabs.com | www.kudelskilabs.com

KUDELSKI LABS