Factsheet

Kudelski Labs – OCP S.A.F.E. Security Review

OCP S.A.F.E. Security Assurance Framework & Evaluation

OCP S.A.F.E. certifies device and chipset security, helping vendors meet global standards and accelerate market trust.

OCP S.A.F.E. is the Open Compute Project's security appraisal program for data centre and cloud infrastructure devices.

Kudelski Labs, an OCP-approved Security Review Provider, delivers independent, third-party assessments across three progressive scopes: code and architecture, trust boundary isolation, and physical attack resilience. Our streamlined process reduces audit overhead, accelerates compliance, and helps vendors stand out in a competitive market. Partnering with Kudelski Labs enables faster time-to-market, long-term resilience, and increased customer confidence for device and chipset manufacturers worldwide.

OCP S.A.F.E. Security Review

- **Comprehensive security review across three scopes:** code and architecture assessment, trust boundary isolation validation, and physical attack resilience testing for device and chipset manufacturers seeking certification.
- **Kudelski Labs, an OCP-approved Security Review Provider,** leverages ISO/IEC 27001:2022 certification and over 25 years of hardware security expertise to deliver trusted, independent, third-party assessments.
- **Our process includes threat modelling, code review, penetration testing, compliance reporting, and real-world attack simulations,** equipping vendors with actionable insights to strengthen security and streamline the assessment process.

Certified Security. Trusted Devices

Scope-Based Progression: Three-layered review: code, architecture, physical resilience.

Independent Expertise: Testing by Kudelski Labs, OCP-approved Security Review Provider based in Switzerland and France.

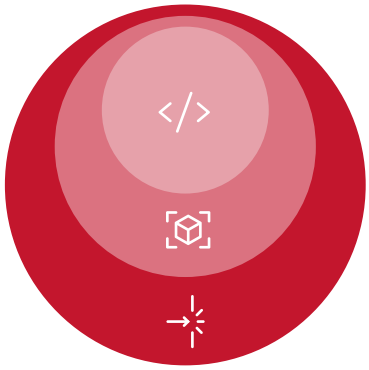
Accelerated Compliance: Faster certification, reduced audit complexity, and increased customer confidence.

How it Works

Scope 1: Code and architecture

Scope 2: Trust boundary isolation

Scope 3: Physical attack resilience



Kudelski Labs OCP SAFE Process

Key Features

Comprehensive security evaluation for device and chipset vendors, covering code, architecture, and physical attack resilience.

- Threat model creation and review tailored to device architecture.
- Manual code and architecture assessment for robust security foundations.
- Validation of trust boundary isolation to prevent unauthorised access.
- Physical attack resilience testing against real-world threats.
- Real-world attack simulations for comprehensive risk evaluation.
- Compliance reporting to support OCP endorsement.

Use Cases

Kudelski Labs applies its structured review process to support a wide variety of use cases, including:

- Audit chipset and device security for data centre deployment.
- Build threat model with expert review.
- Security audit with independent validation.
- Demonstrate compliance for enterprise contract bids.
- Launch hardware platform with attack resilience certification.
- Prove security level for new market entry.
- Build strategic differentiator to position products with competitive security assurance

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