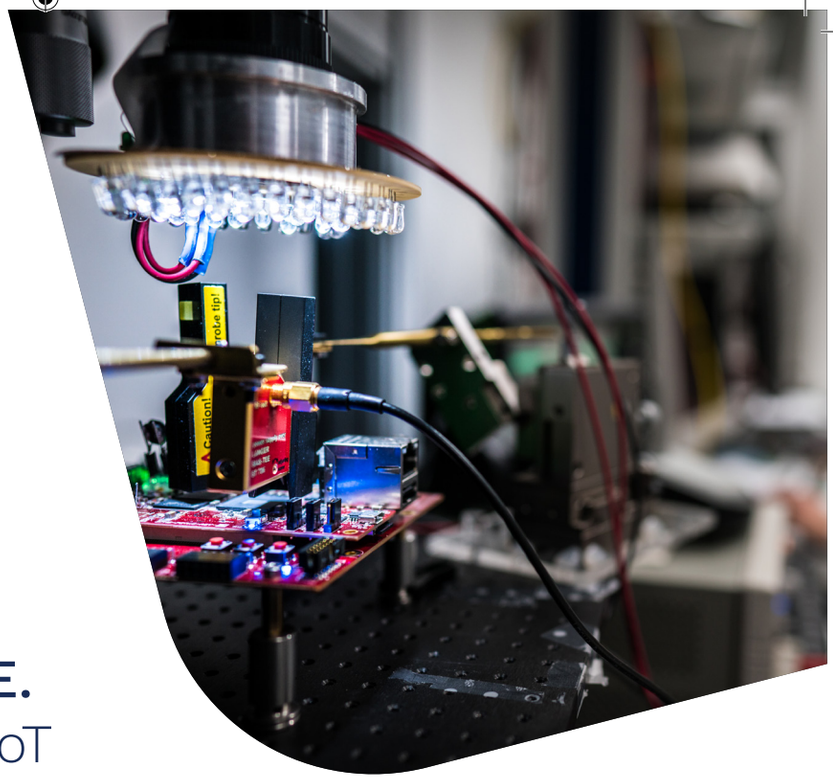
KUDELSKI IOTHINGS

NAGRAVISION
KUDELSKI GROUP



Secure your OCP S.A.F.E. Approval with Kudelski IoT Security Labs

OCP S.A.F.E. approval is key for device and chipset makers. With over 30,000 new vulnerabilities reported last year, strong security is critical. This approval process ensures products meet strict data center and cloud security needs, providing a market edge.

BUILD RESILIENCE

Understanding OCP S.A.F.E. Review Scopes

The OCP S.A.F.E. review framework provides three progressive review scopes, each addressing a critical layer of security. Each scope builds upon the last, ensuring holistic security and alignment with industry best practices.

SCOPE 1

Code and Architecture Assessment

Focuses on manual code review, documentation, and build environment validation. This includes reviewing your existing threat model or developing one if needed. This scope covers the essential security requirements for all types of devices and firmware.

SCOPE 2

Trust Boundary Isolation

Examines the architecture and design features that enforce security between trust boundaries, including a review of all relevant code. This scope adds the review of the trust boundaries inside the product if applicable for the specific device.

SCOPE 3

Physical Attack Resilience

Tests the implementation of security mechanisms against local attacks, such as fault injection and side-channel attacks. Real attacks validate your product's robustness against sophisticated threats. Scope 1 is the basis for all the other scopes as well.

IoT security LABS

Kudelski IoT Security Labs, an approved OCP S.A.F.E. Security Review Provider, is here to help.

Backed by decades of expertise and ISO/IEC 27001:2022 certification, our labs deliver rigorous, actionable evaluations that align with the OCP S.A.F.E. framework. Our labs have been conducting hardware security evaluations since 1999.

Whether you're seeking to validate your code, establish a robust architecture, or defend against physical attacks, we provide a step-by-step roadmap to successful OCP S.A.F.E. approval. With Kudelski IoT, you can confidently bring secure and trusted products to market.

DELIVERABLES

What to Expect from Kudelski IoT's Security Reviews

Partnering with Kudelski IoT means transparency, actionable insights, and a seamless security review process. If issues are identified, they are immediately communicated to you to allow you fixing them as soon as possible. After a delta review (with short turn-around time), the final short-form report will only reflect the security posture of your product after all mitigations have been put into place. Our deliverables include:

Detailed Threat Model Review

Analysis of the threat landscape for your product and creation of a new threat model if necessary. This might then also guide you in the choice of scope for your product.

Hardware Attack Simulations

For Scope 3 reviews, real-world attack scenarios assess vulnerabilities to physical threats.

Architecture and Security Design Review

Comprehensive review of appropriate documentation or other available information.

Findings Report

A comprehensive report detailing identified vulnerabilities and proposed mitigations for your use.

Code and Design Analysis

In-depth evaluation of your code, design features, and build environment.

Endorsement Support

A short-form report aligned with OCP guidelines for publication on the OCP S.A.F.E. website to achieve OCP S.A.F.E. endorsement of your product.

WHY KUDELSKI?

By choosing Kudelski IoT, you're partnering with a team that understands the challenges of security and delivers targeted feedback to ensure your success. Kudelski IoT has a proven track record of helping global manufacturers secure their products from chipsets to devices. Our evaluations are built on:

Physical Attack Resilience

40+ years of digital security experience, enabling us to anticipate and address emerging threats.

Certified Labs

ISO/IEC 27001:2022 accreditation of our laboratory services ensures the highest standards of information security, guaranteeing the integrity and confidentiality of your data.

Proven Methodologies

Industry-leading techniques for security testing and attack simulations, providing comprehensive and reliable assessments.

www.kudelski-iot.com

BENEFITS

Why OCP S.A.F.E. Approval Matters for Your Business

Our approach ensures that your devices not only meet current standards but also set the benchmark for security excellence. Achieving OCP S.A.F.E. reviews with Kudelski IoT provides tangible benefits:

Market Differentiation

Stand out with trusted, approved products, gaining a competitive edge in the marketplace.

Accelerated Development

Address vulnerabilities early to reduce delays, ensuring a smooth and efficient product development lifecycle.

Customer Confidence

Build trust with end users through verified security, enhancing your brand reputation and customer loyalty.

Long-Term Resilience

Future-proof your products against evolving threats, safeguarding your investments and ensuring long-term success.