Factsheet

Kudelski Labs – Kudelski Secure Enclave (KSE)

Family of Secure Enclaves for Advanced Semiconductor Security

KSE is a programmable and modular silicon-proven hardware Root of Trust IP delivering embedded security for advanced semiconductor designs. Offered off-the-shelf and certification-ready, it integrates seamlessly across diverse technology nodes.

Fully self-contained, KSE embeds all essential security mechanisms without relying on the host SoC. Its optimized architecture ensures strong protection with efficient power, area, and performance. Scalable across multiple verticals, KSE reduces design risk, accelerates time-to-market, and enables secure, compliant, high-performance semiconductor products.

Embedded Security IP Functions

- **Secure Boot & Update Services:** Ensures devices boot trusted firmware and receives authenticated updates throughout the product lifecycle.
- **Secure Debug & Provisioning:** Enables controlled debug access and secure device enrolment with pre-loaded credentials.
- **Key Management:** Supports robust generation, storage, and lifecycle handling of cryptographic keys.
- **Attack Resistance:** Shields sensitive operations from side-channel and fault injection attacks.
- **Hardware-Accelerated Cryptography:** Delivers high performance cryptographic operations.
- **Programmability:** Enables post-deployment upgrades, that evolve to security requirements.

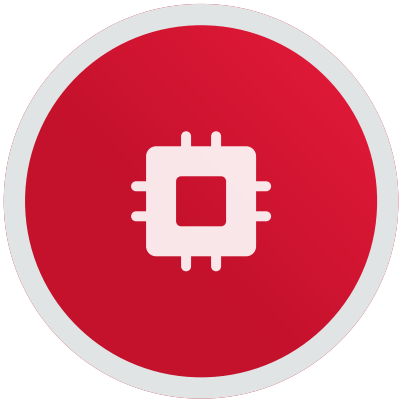
Kudelski Secure Enclave: Built for Secure-by-Design Systems

Built-In Root of Trust:
Provides foundational security services to the chipset and device, and protection against physical and fault-based attacks.

Cryptography Services:
Delivers a full suite of symmetric and asymmetric algorithms, secure key storage, and true random number generation. Futureproof with post-quantum cryptography support.

Certification-Ready:
Across Industry Standards The IP is designed to streamline compliance across Common Criteria, SESIP, PSA, FIPS 140-3, ISO 21434, ASPICE, EVITA, ISO 26262, ISO 9001.

Features & Use Cases



Key Features

KSE delivers comprehensive services and real value across every stage of the chipset lifecycle:

- Tailored & Modular: Pre-validated IP with defined security levels, suitable for single-chip use or integration into broader security platforms.
- Effortless integration: All-in-one integration package with complete drivers and built-in PSA Cryptoprocessor support.
- Certification Services: Support from Target of Evaluation definition to lab assessment and certification.
- Security Surveillance & Maintenance: Continuous monitoring, threat analysis, and remediation to ensure deployed products remain secure.
- Expert Support: Best-in-class security experts guide the full product lifecycle.
- FPGA Designs: Delivers security solutions tailored for FPGA-based implementations.

Use Cases & Verticals

KSE supports a wide range of security functions across the product lifecycle. These use cases demonstrate how the IP delivers value in real-world applications:

- Automotive: Secures ADAS, infotainment, and EV modules reliably.
- Consumer Devices: Protects smart home, wearables, and connected appliances.
- Industrial & Critical Infrastructure: Safeguards IoT, factory automation, and smart infrastructure.
- Telecom & Networking: Ensures integrity for 5G, routers, and edge devices.
- Financial & Payment Systems: Secures transactions across payment terminals and digital wallets.
- Defense & Government: Provides advanced security for military, government, and aerospace.

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.

Contact Us