Factsheet

Kudelski Labs – Kudelski Secure Enclave 5 (KSE5)

KSE5: High-Assurance Security for Advanced and Regulated Applications

KSE5 is a silicon-proven hardware security IP platform designed for semiconductor manufacturers developing safety-critical, regulated, and high-security applications. Built around a hardware Root of Trust, KSE5 delivers secure boot, cryptographic services, secure storage, key management, secure provisioning, and lifecycle security within an advanced security architecture.

Designed for environments where security, compliance, and long-term resilience are critical, KSE5 combines advanced attack protection, hardware isolation, and certification-ready security capabilities to support the most demanding semiconductor applications.

Built for High-Assurance and Regulated Applications

If you're developing safety-critical or regulated applications such as automotive systems, industrial control, or critical infrastructure, you need KSE5 to deliver high-assurance security designed to meet strict certification requirements and support long product lifecycles.

Engineered for Advanced Threat Protection

KSE5 combines advanced security architecture, integrated protection mechanisms, and high-assurance security services to support regulated and mission-critical semiconductor platforms.

- Protect sensitive assets against sophisticated physical, side-channel, and fault-based attacks
- Integrate secure boot, provisioning, storage, and lifecycle security within a trusted architecture
- Support advanced certification and compliance initiatives
- Enable long-term security for products deployed over extended lifecycles
- Support crypto agility and quantum-resistant cryptography to address evolving threats

High-Assurance Security for Regulated Environments

Advanced Threat Protection
Protects sensitive assets against physical, side-channel, and fault-based attacks through advanced hardware and software security mechanisms.

Long-Lifecycle Security
Designed to support products operating in regulated and mission-critical environments with long deployment lifecycles.

Certification-Ready Design
Supports certification and compliance initiatives including Common Criteria EAL4+, FIPS 140-3, CRA, ISO/SAE 21434, and IEC 62443.

Quantum-Ready Security
Supports crypto agility and quantum-resistant cryptography to help address future security requirements.

Key Features

Hardware Root of Trust: Provides the foundation for trusted device operation, secure key management, and protection of critical security assets.

Hardware-Accelerated Cryptography: Supports high-performance cryptographic services, including quantum-resistant cryptography, while maintaining strong security assurance.

Advanced Digital Countermeasures: Incorporates advanced protection mechanisms designed to resist sophisticated attack techniques targeting sensitive assets and cryptographic operations.

Secure Boot and Lifecycle Security: Protects device integrity through secure boot processes and comprehensive lifecycle management capabilities.

Certification-Ready Design: Designed to support advanced certification and compliance initiatives required by regulated and safety-critical industries including Common Criteria EAL4+, FIPS 140-3, CRA, ISO/SAE 21434, and IEC 62443.

Trusted Application Support: Supports programmable trusted applications with strong isolation and protection mechanisms for sensitive operations.

Applications

KSE5 is suited for a broad range of connected semiconductor applications, including:

- Automotive safety-critical systems
- Industrial control systems
- Aerospace & defense platforms
- Financial and payment systems
- Critical infrastructure
- Regulated and mission-critical environments
- Long-lifecycle connected products

Why Semiconductor Manufacturers Choose KSE5

- ☑ Reduce risk in safety-critical and regulated environments
- ☑ Support compliance with advanced security standards
- ☑ Protect sensitive assets against sophisticated attacks
- ☑ Deliver long-term security across extended product lifecycles
- ☑ Future-proof platforms with crypto agility and quantum-resistant cryptography
- ☑ Implement high-assurance security without compromising performance

Strategic Intelligence. Impactful Action.

Our embedded 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 assets - devices, identity, data, decisions, commands and actions throughout the lifetime of the device and its ecosystem.

Explore Our Innovations

Contact Us

Kudelski Labs leverages the Kudelski Group's decades of experience in intelligent security to solve the world's most complex cyberthreat challenges at the intersection of connectivity and safety. Its mission is to secure the future—across land, air, space, and industry—through advanced research, real-world engineering, and global partnerships.

info@kudelskilabs.com | www.kudelskilabs.com

KUDELSKI LABS