KUDELSKI LABS

Kudelski Secure Enclave 3 (KSE3): Enhanced-Assurance, Configurable Security for Scalable Semiconductor Designs

KSE3 delivers silicon-proven, ultra-compact hardware security IP for configurable semiconductor designs — balancing performance, configurability, and certification readiness. Crypto-agile and quantum-ready, it's engineered for certification to SESIP Level 3, PSA Level 3, and FIPS 140-3.



Table of Contents

01 Market Demands & Industry Advantages

02 Embedded Trust for Next-Generation Chips

03 The KSE Portfolio at a Glance

04 A Common Security Foundation

05 KSE3 Product Overview

06 KSE3 Industry Use Cases

07 Strategic Partnership & Alliances Benefits

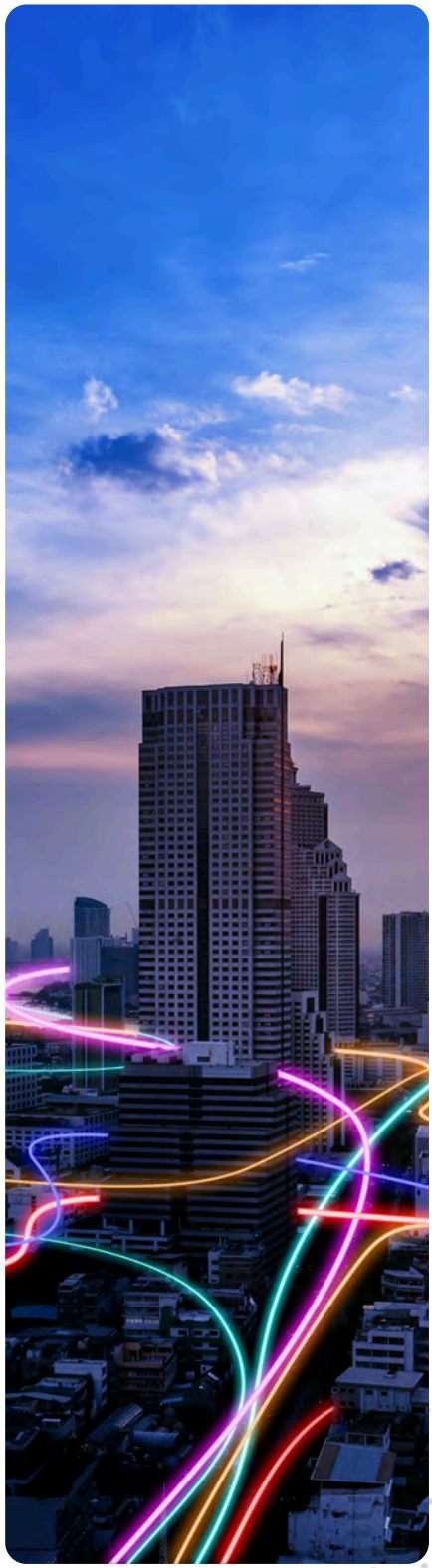
08 Kudelski Labs: Security Innovation Leadership

09 Get Started: Secure Your Silicon Today

01

Market Demands & Industry Advantages

Connected devices face sophisticated threats, long operational lifespans, and evolving cryptographic standards. Industries such as automotive, industrial infrastructure, and space systems need embedded security that is resilient against physical and remote attacks, adaptable to future cryptographic standards, efficient in constrained environments, and certified for regulatory compliance.



Kudelski Secure Enclave (KSE) turns these demands into a commercial advantage:

- **Faster time-to-market** — certification-ready architecture that shortens audit cycles and simplifies regulatory approvals across global standards.
- **Lower design risk and lifecycle cost** — minimizing integration complexity and preventing costly security failures post-launch.
- **End-to-end expertise** — guidance for integration, certification readiness, documentation, and lifecycle management.

02

Embedded Trust for Next-Generation Chips

Choosing the right security solution is critical for protecting sensitive assets in today's connected world. Hardware-based security offers the most reliable and robust foundation for trust.

Why Choose KSE?

Built for High Assurance

Hardware security isolates critical operations, ensuring resilience against physical and remote attacks.

Designed for Longevity

Ideal for products with long lifecycles, where software-only solutions fall short.

Adaptable to Evolving Threats

Support crypto agility and quantum-resistant cryptography (QRC) counter emerging risks like quantum computing.

Certification-Ready

Engineered to streamline SESIP, PSA, FIPS 140-3, and EU CRA compliance, shortening audit cycles.

Risk-Based by Design

Protection matched to data sensitivity, attack exposure, and operational duration.

Patented Innovation

KSE's core security mechanisms are original Kudelski Labs inventions, protected by patents and backed by decades of advanced research in attack techniques, security and cryptography.

03

The KSE Portfolio at a Glance

The KSE portfolio is organized into three tiers, each engineered for a different level of security assurance and certification — so you can match the right protection to your design without over- or under-engineering it. All three share a common architecture: a silicon-proven secure enclave built on a proprietary 32-bit RISC-V core, crypto-agile and quantum-ready.

KSE²

Ultra-compact root of trust for high-volume consumer IoT, smart devices, and connectivity chipsets. Targets SESIP Level 2 / PSA Level 2 (AVA_VAN.2 "Basic"), FIPS 140-3, and EU CRA Class I/II.

KSE³

Compact, cost-efficient root of trust for automotive, industrial automation, and Edge AI — optimized for gate count without compromising protection. Targets SESIP Level 3 / PSA Level 3 (AVA_VAN.3 "Enhanced Basic"), FIPS 140-3, ISO/SAE 21434, IEC 62443, and EU CRA Class II.

KSE⁵

Maximum assurance for space & defence, digital access, and safety-critical systems. Targets SESIP Level 5 / PSA Level 5 (AVA_VAN.5 "High Assurance") and Common Criteria EAL4+ (PP0084 & PP0117).

KSE2, KSE3 and KSE5 are delivered with comprehensive integration guidelines, supporting tools, and direct access to Kudelski Labs' experts. Our teams in compliance, cryptography, software and hardware design, and systems architecture provide tailored reviews and guidance to ensure seamless integration and propose the best solution for your specific requirements.



04

A Common Security Foundation

Every KSE is built on a common hardware and software platform and designed to the same security principles. What differs is the level of assurance each one is engineered to reach, and the capabilities and options built around it.

Establish Trust:

Every device gets a unique, hardware-backed identity

Capabilities:

- Hardware Root of Trust
- Key Management
- Secure Provisioning
- Attestation

Ensure Integrity:

Firmware, data and code are protected from tampering and rollback

Capabilities:

- Secure Boot & Firmware Update
- Secure Storage
- Attack Countermeasures

Enforce Control:

Hardware-enforced rules over who can access what, and when

Capabilities:

- Lifecycle & Configuration Enforcement
- Secure Debug
- Subsystem Isolation

Adapt Across Lifecycle:

Stays current with new threats and standards over long lifetimes

Capabilities:

- Crypto agility & Post-quantum
- Configurable Feature Set
- Certification Readiness



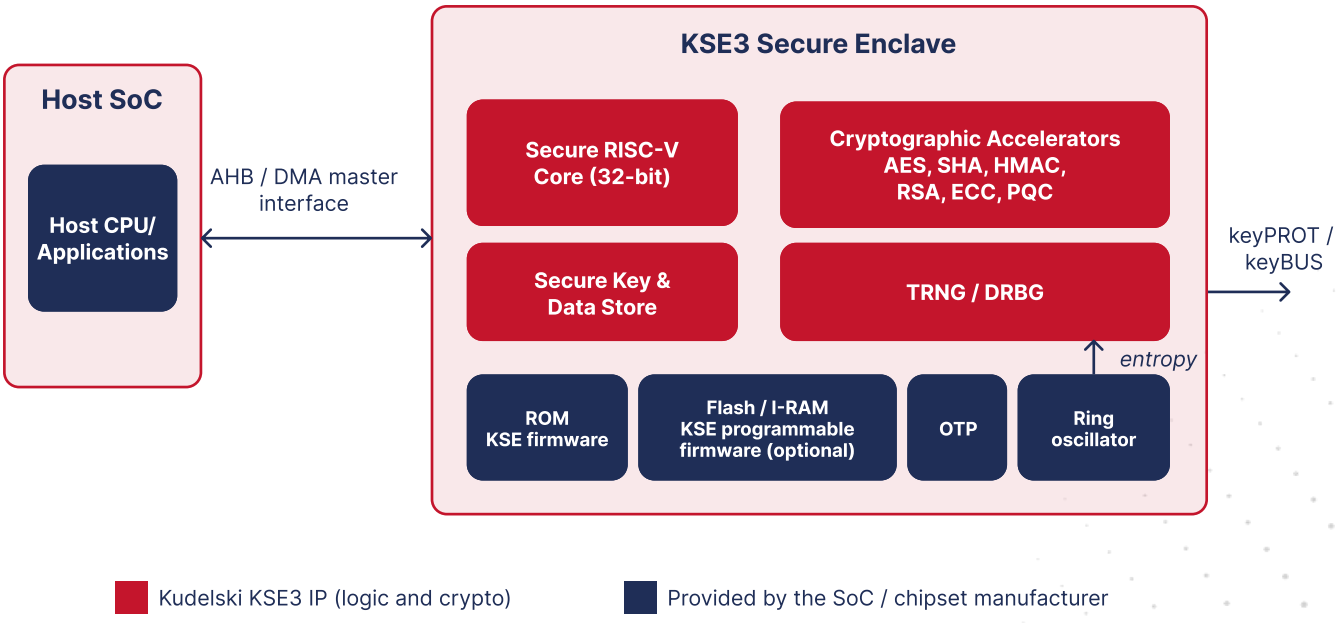
05

KSE3 Product Overview

How KSE3 Works

KSE3 is a siloed hardware security core integrated into the SoC through the standard AHB or DMA interface. Access to crypto modules, keys, memory ranges, and I/O is enforced in hardware, and critical operations such as key derivation and storage execute inside the enclave with no exposure to host software. The core is built on a Kudelski proprietary 32-bit RISC-V processor dedicated to trusted on-chip processing.

Keys leave the enclave only in "wrapped" (authenticated and encrypted) form, bound to a per-device identity, so the host can store an unlimited number of keys in internal or external memory without compromising confidentiality. A high-speed ring-oscillator entropy source, digital countermeasures, and memory scrambling and integrity protection defend the IP against logical and physical attacks, enabling the integrating SoC to reach AVA_VAN.3 robustness.



Configuration Options

KSE3 is available in multiple variants, so you can match the right interface, programmability, and footprint to your design.

Product	Interface & Programmability	Positioning
KSE3-145	DMA master, programmable (I-RAM)	Full-featured master configuration; encrypted firmware updates to external flash
KSE3-135	DMA master, programmable (system flash)	Firmware in secure host-shared flash; for constrained non-volatile memory
KSE3-140	AHB slave mailbox, programmable (I-RAM)	Slave enclave interacting via control registers and mailbox
KSE3-100	AHB slave mailbox, non-programmable (ROM-only)	Smallest footprint; for tight gate-count and NVM budgets
KSE3-7xx	AHB slave / DMA master, programmable (I-RAM or flash)	Industrial & automotive; ISO/SAE 21434, IEC 62443-4-2, ASIL B & ISO 26262

All variants target SESIP Level 3 / PSA Certified Level 3 / FIPS 140-3 / EU CRA Important Product "Class II."

Cryptographic Services

KSE3 provides a complete, crypto-agile suite spanning classical and quantum-resistant algorithms, all validated to recognized standards.

Class	Algorithms & Standards
Symmetric	AES-128/192/256, ECB, CBC, CTR, CMAC, GMAC, CCM, CCM*, GCM, CBC-MAC; AES key ladder (up to 15 stages); FIPS-197, SP 800-38
Hashing	SHA-2 (224/256/384/512), SHA-3 (224/256/384/512), SHAKE128/256; FIPS 180-4, FIPS 202
MAC & KDF	HMAC-SHA2 (FIPS 198-1); HKDF & CMAC KDF (SP 800-56C, SP 800-108) for TLS 1.2 / 1.3
Asymmetric	RSA 2048 / 3072 / 4096-bit; PKCS#1 v1.5 and v2.x (RSAES-OAEP, RSASSA-PSS)
Asymmetric	ECC all SECP and Brainpool, curves up to 576b. - ECDSA key gen, Sign/verify, ANSI X9-62, 2022-BSI-TR-02102-1, FIPS 186-5 - ECDH key gen and key agreement, 2022-BSI-TR-02102-1
Random Generation	TRNG (SP 800-90B) with DRBG AES-256 CTR (SP 800-90A)
Quantum-resistant Cryptography (QRC)	LMS (SP 800-208), ML-KEM (FIPS 203), ML-DSA (FIPS 204), SLH-DSA (FIPS 205); FN-DSA on roadmap
Chinese Cryptography	SM2 / SM3 / SM4

Key Features & Functionalities

Feature	Description
Secure Applications	
Secure Applications	Security toolbox for applications and cryptographic protocols like TLS, CCC, or FiRa. For example, securing ECDH key agreement, session keys computation, and resumption keys for TLS 1.2/1.3.
UWB Secure Ranging	Dedicated functions to manage UWB SCP11a, CCC, and FiRa processing: the SCP11a Ranging Data Set (RDS) to import CCC/FiRa keys from a secure element, and deriving SCP11 AES session keys (X9.63 key derivation).
Key Management	
Secure Key	Keys are secured within the enclave to ensure confidentiality, integrity, and authenticity. The entire key lifecycle — including provisioning, generation, ECDH key agreement or ML-KEM key encapsulation, derivation, storage, and usage — is secured by the enclave. Keys with associated metadata are stored wrapped outside KSE3.
Secure Key Cache	KSE3 automatically preserves unwrapped cryptographic keys in internal RAM for faster reuse. Applications can lock or erase keys as required.
Secure Key Lifecycle	Service for revoking and activating keys according to key metadata and authorization.
Secure Key Provisioning	
Secure Key Provisioning	Import key service available for secure provisioning at the wafer level, during factory provisioning, and in the field (e.g., initial device connection). Provisioning can use Kudelski Labs keySTREAM or a third-party solution. Remote credentials management is also supported.
Secure Storage	
Secure Storage	Secure storage services using Sponge or AES are provided to the host for protecting data and code, ensuring confidentiality, integrity, and authenticity.
Secure Boot & Firmware Update	
Programmable Firmware	Firmware is stored encrypted and can be updated in the field. At every startup, KSE3 verifies it, so only genuine, up-to-date firmware can run.
Quantum Lifecycle States	KSE3 can be locked to post-quantum or classical cryptography, so customers decide when to switch.
Lifecycle & Chipset Configuration Enforcement	
Secure Lifecycle	Secure the lifecycle states of the chip and device, from manufacturing to end-of-life. Enables lifecycle management of assets, such as cryptographic keys. For example, keys can be restricted to specific lifecycle states or product segments.
Secure Configuration	KSE3 controls access to the SoC's test and debug interfaces throughout the device lifecycle. Each lifecycle owner can open or lock what it needs.
Secure Debug	
Secure Debug	Debug access is unlocked only by authorized parties, with access rights that can be renewed or revoked. Field return analysis is supported without exposing device secrets.
Multi-subsystem Isolation	
Multi-subsystem Isolation	Keys, data, code, security settings and debug access are segmented per SoC subsystem. Each subsystem's assets are isolated from the others.
Master DMA	Direct memory access between the enclave and host memory offloads cryptographic processing from the host CPU.
Secure Attestation	
Secure Attestation	Standards-based attestation of device identity, integrity and boot state, and of keys generated and stored within the enclave.
Monotonic Counters	
Monotonic Counters	Rollback protection for secure boot stages and host applications.
keyPROT / keyBUS	
keyPROT / keyBUS	Optional. Keys shared with on-chip cryptographic engines remain inaccessible to host software, with minimal latency.
Integration & Performance	
PSA Crypto Integration	Integrated with the PSA Cryptographic API and Trusted Firmware-M.
KSSL Software Library	Compact software library developed to industry secure coding standards, for RTOS, TEE and bare-metal hosts.
Fast Startup	Security services are available immediately after power-up.
Fast Resume	Reduced resume latency from suspends and deep-sleep states.
Enhanced Robustness	
Memory Protection Unit (MPU)	On-core MPU with 12 regions and peripherals, enforcing hardware-level code-execution protection and memory isolation within the enclave.
Enhanced Fault-Injection Resistance	Strengthened countermeasures against physical attacks, including fault injection and side-channel analysis, supporting AVA_VAN.3 robustness.

06

KSE3 Industry Use Cases

KSE3's balance of footprint, performance, and enhanced robustness makes it the right fit for demanding automotive, industrial, and intelligent-edge systems.



Automotive

Vehicles need security that lasts for their full service life and meets automotive cybersecurity requirements. KSE3 authenticates secure boot and firmware updates with classical and/or post-quantum cryptography and isolates up to three host subsystems in hardware. UWB secure ranging, with SCP11a, CCC, and FiRa key import, supports applications such as digital car keys. Certification-ready design supports ISO/SAE 21434.



Industrial Automation

Factory and industrial systems run for many years and are exposed to physical tampering. AVA_VAN.3 robustness gives KSE3 strengthened side-channel and fault-injection countermeasures, and lifecycle and chipset configuration enforcement controls access to host hardware resources, including test interfaces, throughout the device lifecycle. Certification-ready design supports IEC 62443.



Edge AI

AI accelerators and edge devices hold valuable models and sensitive data. KSE3 protects model integrity and data confidentiality with secure storage using per-chip secret hardware keys, and device and key attestation with measured boot proves each device can be trusted. Crypto-agile, quantum-ready security keeps edge deployments protected as standards evolve.



Data Center Security

High-performance environments need cryptographic keys kept out of reach of host software. KSE3 generates and wraps keys inside the enclave, isolates up to three host subsystems in hardware, and uses keyPROT / keyBUS to transfer keys securely to external cryptographic modules. Device and key attestation via IETF RATS / EAT lets operators verify every component.

Also suited to

IoT & Connected Devices · Connectivity & Low-power Chipsets · Embedded MCUs · LoRa Key Protection · Smart Homes & Cities · Asset Tracking

07

Strategic Partnership & Alliances Benefits

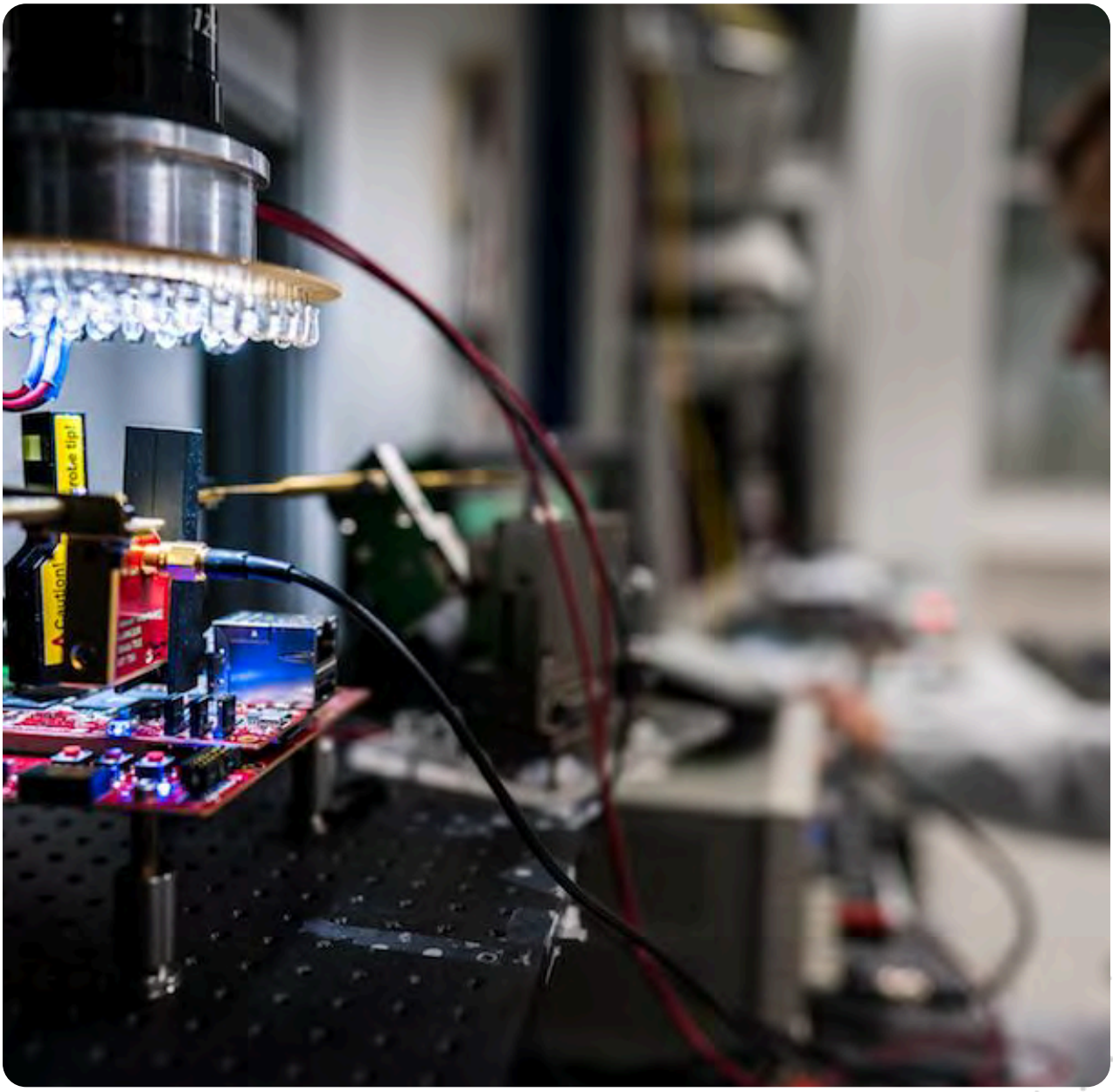
Why partner with Kudelski Labs:

- Decades of expertise in hardware security and cryptography
- Proven track record with global semiconductor leaders
- End-to-end support from design to certification

08

Kudelski Labs: Security Innovation Leadership

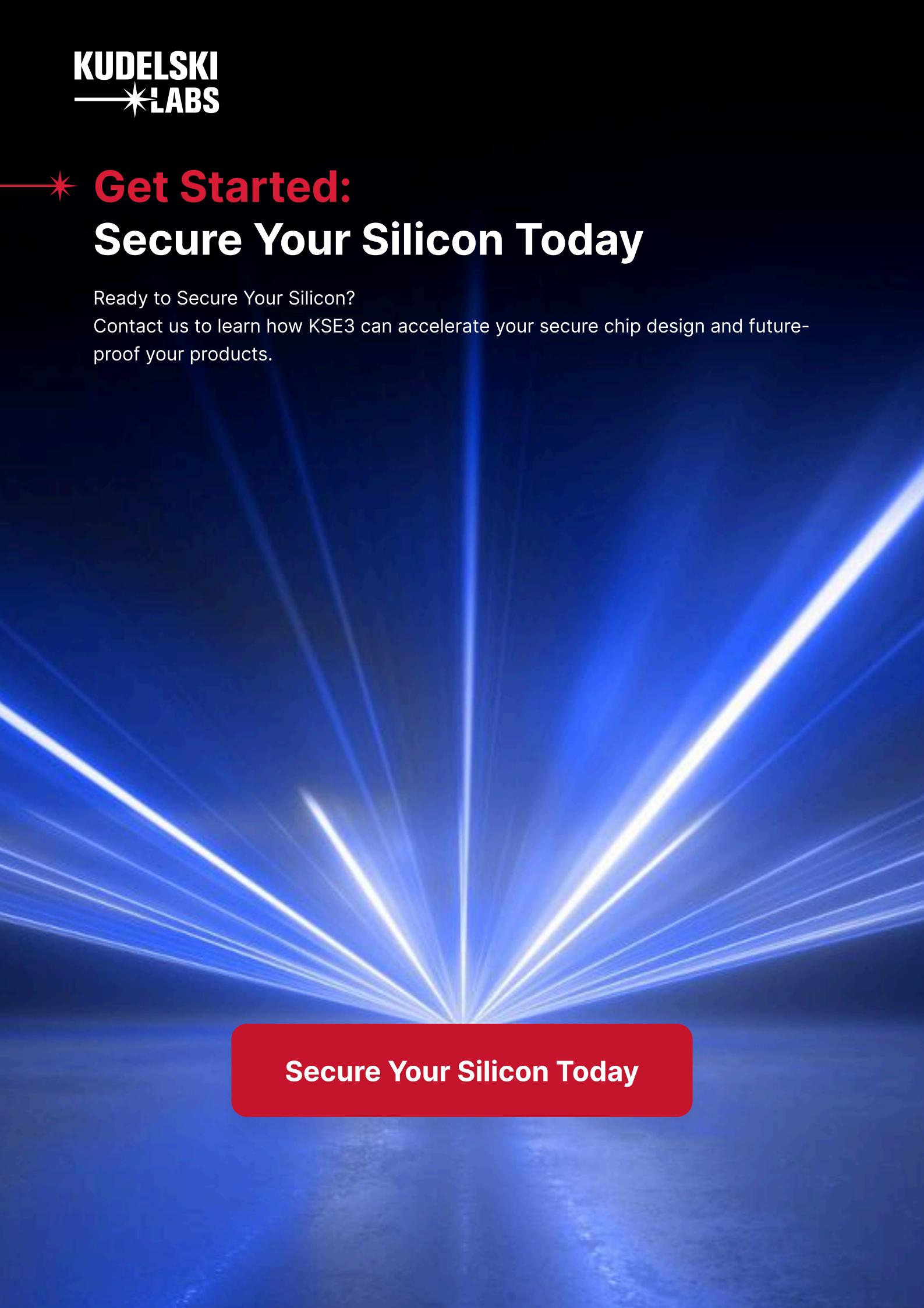
Kudelski Labs is the advanced research and engineering division of the Kudelski Group. Our mission is to secure the future, across land, air, space, and industry, by anticipating emerging threats and enabling innovation with confidence. We combine deep technical expertise, real-world engineering, and global partnerships to help pioneers shape their digital futures.



KUDELSKI LABS

Get Started:
Secure Your Silicon Today

Ready to Secure Your Silicon?
Contact us to learn how KSE3 can accelerate your secure chip design and future-proof your products.



Secure Your Silicon Today