Factsheet



Kudelski Labs – Kudelski Secure Enclave 2 (KSE2)

KSE2: Right-Sized, Configurable Security for High-Volume Semiconductor Designs

SESIP LEVEL 2 | PSA CERTIFIED LEVEL 2 | FIPS 140-3 | AVA_VAN.2 (JIL 16-20) | EU CRA CLASS I/II

KSE2 is a silicon-proven, ultra-compact hardware Root-of-Trust IP for semiconductor manufacturers. Built on a proprietary 32-bit RISC-V secure processor and isolated as a secure enclave from the rest of the SoC, it delivers secure boot, secure updates, cryptographic services, random number generation, secure storage, key management, secure provisioning, and lifecycle security.

KSE2 is engineered to enable SoC and module certification at SESIP Assurance Level 2 and PSA Certified Level 2, targeting AVA_VAN.2 robustness (JIL attack quotation 16–20, "Basic"). Crypto-agile and quantum-ready, it supports both classical and post-quantum cryptography, keeping designs ahead of evolving standards and future threats, while remaining among the smallest security IPs for its feature range.

Built for Configurable Security

If you're developing high-volume semiconductor designs where gate count, cost, and footprint are tightly constrained, KSE2 gives you a configurable root of trust that matches protection precisely to each design, so security scales with your product, not against your gate budget.

- Configurable by design, enable only the security services and cryptographic capabilities each product needs, tailored to your requirements
- Optimize gate count, RAM, and ROM for area and cost-constrained designs
- Security platforms used across multiple products — configure the feature set per product without reworking the design each time

Fast, Efficient Integration

- Wrapped-key architecture — unlimited keys stored securely in host memory
- Fast startup — no firmware load at boot; services available immediately
- Compact KSSL software library (~20 KB, ~35 KB with PQC) for RTOS, TEE, or bare metal
- Native PSA / Trusted Firmware-M (TF-M) integration

KSE2 at a Glance

AVA_VAN.2 ("Basic")
Resistance to attackers with basic attack potential (JIL 16–20), covering common software and logical threats such as fuzzing, buffer overflows, and timing analysis, with baseline countermeasures against glitch/fault injection and side-channel attacks.

Configurable Architecture
Tailor cryptographic and security services to specific platform requirements while maintaining consistent interfaces and integration flows.

Certification-Ready Design
Supports SESIP Level 2, PSA Certified Level 2, FIPS 140-3, AVA_VAN.2 (JIL 16–20), IEC 62443, ISO/SAE 21434, and EU CRA (Important Product, "Class I/II").

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

Security & Cryptographic Services

Key Management
Key generation, derivation, activation & revocation, key cache, and key wrapping — using a unique per-chip OTP secret

Secure Storage
Host data/code protected with per-chip secret HW keys

Secure Boot & Firmware Update
Authenticated with classical and/or post-quantum cryptography

Secure Provisioning
Wafer, factory, and in-field; zero-touch onboarding

Lifecycle & Chipset Configuration Enforcement
Controlled access to host hardware resources

Secure Debug
PKI-based debug authorization per the ADAC standard

Multi-subsystem Isolation
Up to three hardware-isolated host subsystems

Secure Attestation
Device and key attestation via IETF RATS / EAT with measured boot

Monotonic Counters
OTP-based, for host secure-boot stages

keyPROT / keyBUS
Secure key transfer and communication with external cryptographic modules

Cryptographic Services
Symmetric, Hashing, MAC & KDF, Asymmetric (RSA & ECC), Random Generation, PQC (LMS/XMSS, ML-KEM, ML-DSA, SLH-DSA), Regional

Applications

KSE2 is suited for a broad range of connected semiconductor applications, including:

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

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