Factsheet

Kudelski Labs – keySTREAM

keySTREAM
Security Lifecycle Management

keySTREAM — the trust backbone that transforms secure chips into secure ecosystems.

keySTREAM enables semiconductor manufacturers to extend the value of their secure silicon beyond the chip. It provides a scalable platform for device identity, credential provisioning, and lifecycle management — allowing device manufacturers to deploy connected products that are trusted from day one.

It delivers end-to-end lifecycle management, from device identity and credential management to remote updates (FOTA) and revocation. By ensuring continuous compliance with emerging cybersecurity regulations such as the EU Cyber Resilience Act (CRA), keySTREAM enables semiconductor and device manufacturers to maintain trusted operations at scale — protecting users, safeguarding supply chains, and keeping connected products secure throughout their lifetime.

keySTREAM
Security That Starts at the Chip

- **Lifecycle Control:** Manage credentials, enforce security policies, and deliver secure firmware updates remotely, keeping devices compliant, resilient, and protected against evolving threats without redesigning hardware.
- **Data Integrity:** Guarantee that data generated and transmitted by your silicon-based products remains genuine, tamper-proof, and cryptographically verifiable throughout its entire operational lifecycle.
- **Silicon-Rooted Trust:** Embed unique, tamper-proof identities at the chip level during manufacturing, ensuring every device is authentic and secure from the very first boot.

Why Semiconductor Manufacturers Choose keySTREAM

Silicon-First Security:
Embed trust at the hardware level.

Flexible Integration:
IP blocks, SE, or software client.

Future-Proof:
Continuous updates and lifecycle management.

Features & Use Cases

Key Features

keySTREAM delivers silicon-to-cloud security with flexible integration options for chipmakers and OEMs.

- Secure Device Identity – Each device is provisioned with a unique, cryptographically verifiable identity anchored in silicon.
- Credential Provisioning at Scale – Automated, audited issuance of certificates and keys at production, in the field and during the entire product lifecycle.
- Lifecycle Management – Renewal, rotation, and revocation of credentials throughout the device's operational lifetime.
- Firmware & Update Integrity – Built-in support for signing, verification, and secure firmware distribution (FOTA).
- Regulatory Compliance – Enables conformity with cybersecurity frameworks such as the EU Cyber Resilience Act (CRA) and ETSI EN 303 645.
- Cloud & Ecosystem Integration – Seamless interoperability with leading IoT clouds, PKI infrastructures, and secure-element vendors.

Use Cases

keySTREAM addresses critical security needs across diverse semiconductor-driven applications

Secure Cloud Onboarding for IoT Devices

- Use Case: A smart lighting manufacturer uses keySTREAM to provision AWS IoT credentials in the field.
- Value: Devices ship cloud-ready with unique keys and certificates injected through secure manufacturing flows — eliminating manual setup and enabling zero-touch onboarding.

Edge AI and Sensor Nodes with Secure Updates

- Use Case: Edge AI modules use keySTREAM for secure code-signing certificate provisioning and firmware update validation.
- Value: Protects intellectual property and prevents rogue firmware from running on edge devices in the field.

Lifecycle Credential Management for Industrial Gateways

- Use Case: An OEM builds industrial gateways, credentials are managed through keySTREAM for renewal and revocation.
- Value: Simplifies certificate rotation and firmware signing over the full device lifecycle — aligned with EU CRA security compliance requirements.

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