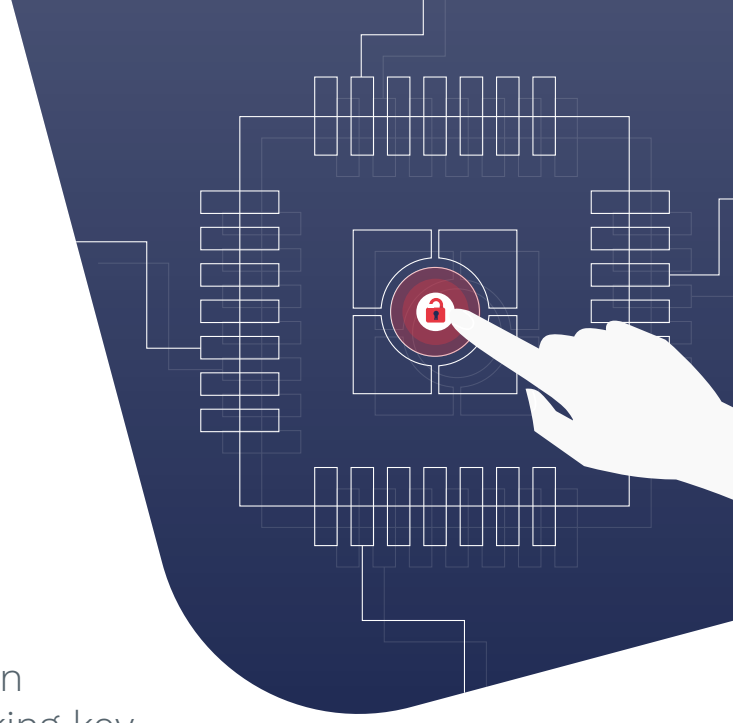
KUDELSKI IOT THINGS



Secure IP: a Robust Security Enclave

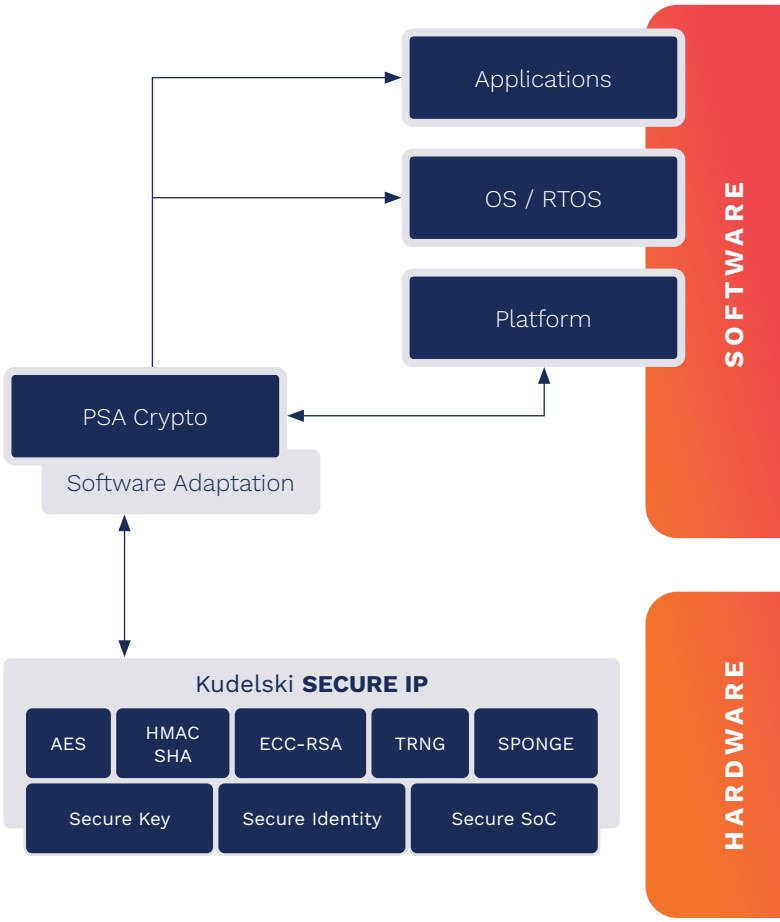
Kudelski IoT Secure Hardware IP has been designed for chipset manufacturers seeking key protection in their system on chip (SoC/ASIC) solutions, robust cryptographic capabilities and services targeting IoT use cases.

KEY BENEFITS

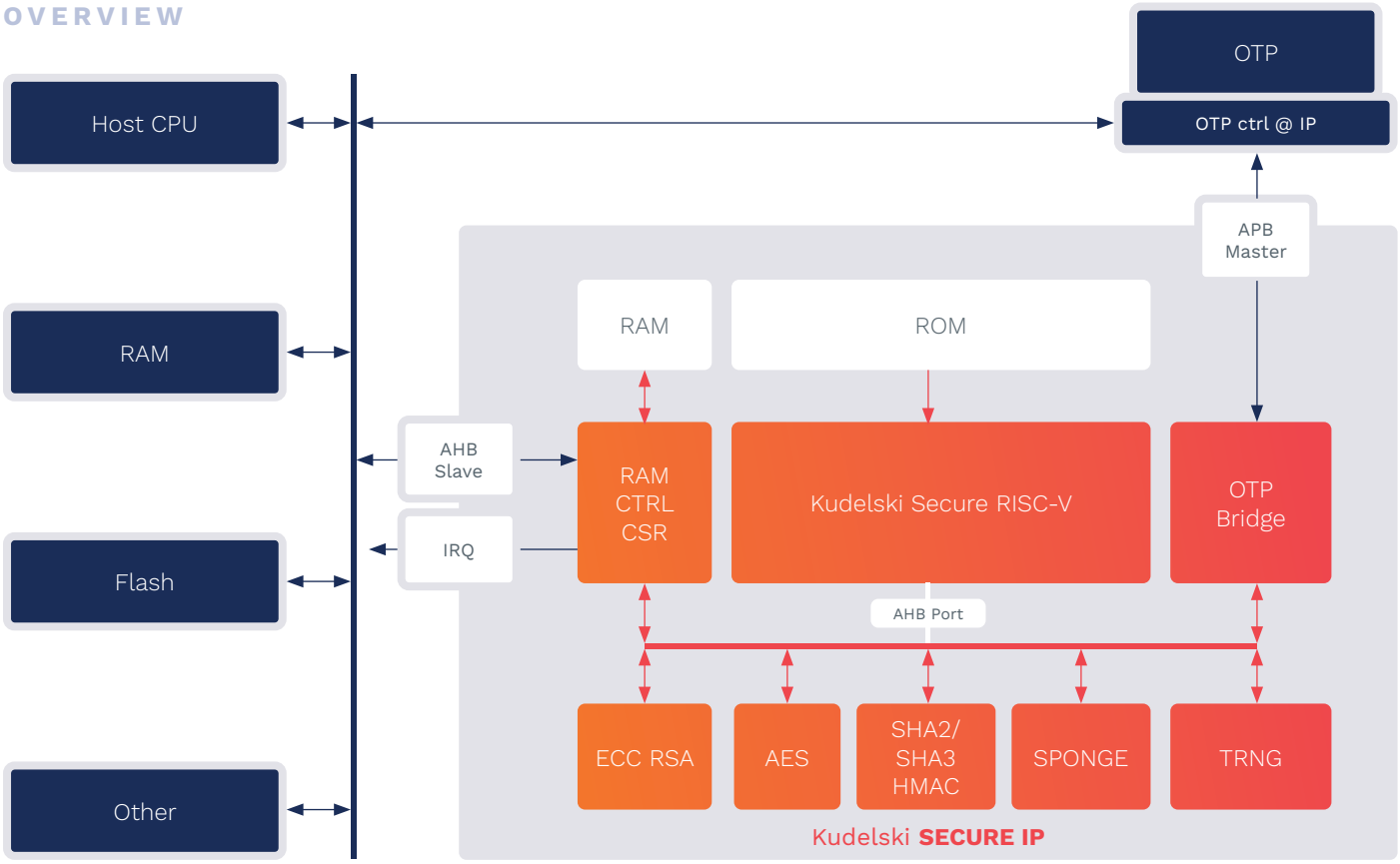
Build secure IoT Solutions

Kudelski provides Secure IP that enables SoC and device manufacturers to build secure IoT solutions. The solution is market proven and certification-ready. Kudelski also provides additional services to help clients with security assessment and for certification of the overall system.

- **Built-in Security** – Security measures have been implemented into the IP block. The IP block supports an achievable certification of PSA and SESIP Level 3.
- **Easy to Integrate** – We provide a full integration and support package including integration validation tools.
- **Optimized Resource Usage** – Specific attention has been paid to small gate count and limited RAM and ROM usage.
- **Fast Startup** – All services are quickly available as there is no software to be loaded into RAM at boot time. This speeds up the secure boot sequence of the SoC and device.
- **Fast Performance** – Our IP block contains optimized HW cryptographic accelerators.
- **Flexible Software Adaptation** – Supports a wide range of platforms, RTOS and OS.
- **Certification support** – Kudelski IoT lab has CSPN accreditation, and we can help customers to prepare for other certifications such as SESIP, PSA, Common Criteria, etc.



OVERVIEW



Security Functions	Security functions to protect keys and chipset/device lifecycle: • Key management - import key, key generation, ECDH key agreement and key derivations • Secure SoC configuration and lifecycle • SoC master secret key and internal OTP management • Secure provisioning and remote management
Algorithms	• Trimmable AES – A flexible AES implementation with optimized security versus performance • SHA2, SHA3 (224, 256, 384, 512) • HMAC-SHA2 • NIST 800-90a/b/c TRNG • Elliptic curves NIST, BrainPool, Curve25519 – ECDH, ECDSA. Up to 576 bits. • RSA up-to 4K • Sponge for a lightweight, fast, and state of the art secure equivalent to AES
Interfaces	• AMBA3 AHB-Light Slave and AMBA APB Master, Interrupt, Direct SRAM, Direct ROM
Memory	• ROM for additional flexibility, Data SRAM, External OTP
Deliverables	• Technical DataSheet, Integration guidelines, RingOscillator for hardmacro design and verification • Test Plan for RTL and P&R Gate tests, C test application, VHDL test bench • Encrypted RTL using EDA tools standard IEEE 1735, ROM Image • Portable library to use the security services in the device, with API description and including standard APIs for easy application integration.

* Specific security functions or cryptographic algorithms can be easily integrated on-demand.

OUR VISION

From Secure IP to Secure Solutions

Kudelski IoT Secure IP is part of a complete suite of tools and services we provide to enable our vision of enabling chipset vendors, device manufacturers, solution providers and operators to build secure IoT solutions. This holistic view consists of Advisory Services, a Root of Trust, and Lifecycle Services that Kudelski IoT manages.

IN-FIELD LIFECYCLE MANAGEMENT

Onboarding – manage ownership of devices and onboarding on IoT services

Provisioning – secure provisioning of assets into SoC. At any point in time during the lifecycle: in-factory or late provisioning.

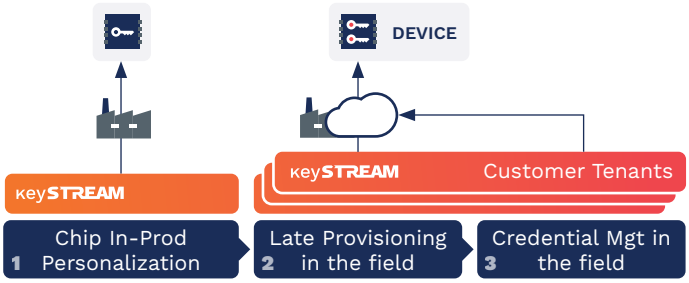
Key Renewability – rotate key material for extended lifetime

Revocation – revoke key material

Certificate Management – generation and management of digital certificates. Integration with 3rd party PKI.

Remote Configuration – secure remote configuration

FOTA – secure management of the firmware update processes



keySTREAM

LIFECYCLE MANAGEMENT

The Kudelski IoT device security management system can be used on top of the Secure IP. The system (keySTREAM) is designed to make lifecycle management of SoC/devices easy, and to support the design of secure IoT solutions. Thanks to the flexibility of the system, customers can choose to activate keySTREAM features on any device that is "keySTREAM ready" – any device that uses a SoC with Kudelski Secure IP.

OUR EXPERIENCE

Security is in our DNA – Our IoT experience is rooted in our 30+ years protecting high-value data and business models.

For protecting Digital TV services, we have developed highly robust and efficient hardware – the NAGRA On-Chip Security (NOCS) for set-top boxes and smart TVs. This is integrated with over 500 different chips and with over 100 million chipsets deployed. Kudelski has also developed custom security chips for smart cards, as well as IP sub-systems for integrated SIM SoC.

Kudelski IoT is the Internet of Things division of Kudelski Group and provides end-to-end IoT solutions, IoT product design, and full-lifecycle services to IoT device manufacturers, ecosystem creators and end-user companies.

These solutions and services leverage the group's 30+ years of innovation in digital business model creation; hardware, software and ecosystem design and testing; state-of-the-art security lifecycle management technologies and services and managed operation of complex system

 V1.6

www.kudelski-iot.com