KUDELSKI IOTHINGS

KSE: The preeminent **Security IP Portfolio**

Kudelski IoT's Hardware Security IP Portfolio has been meticulously crafted to cater to chipset manufacturers seeking finely tuned, resilient, advanced cryptographic capabilities.

KEY BENEFITS

Elevate your IoT security with our cutting-edge, embedded security solutions

The Kudelski IoT Security IP Portfolio offers a modular, turn-key, highly optimized, and all-encompassing range of embedded security solutions that fit a wide variety of IoT application requirements. All our solutions are market proven, certification ready, and comply with different industry standards. Kudelski IoT also provides additional services to help clients with key provisioning, security assessments and certification of the overall system.

KSE5 SERIES

Our high-end, distinctive Security IP

Built-in, cutting-edge HW security – Targeting Common Criteria AVA_VAN.5 security level, can be used and integrated in EAL4+ PP0084/PP117 certified products with state-of-the-art tamper resistant processing

Programmable Trust Application (TA) – Customers can develop proprietary TAs securely isolated by the secure platform. Customer can use the IP secure debug to ease TA development and integration

Multiple use cases & verticals – Responds to the security requirements of multiple vertical markets, such as supporting automotive safety and cybersecurity features

Safeguarding external NVM data – Empower application and data security for external NVM with our Secure Flash Access (SFA) block, ensuring top-tier confidentiality, authenticity, integrity, freshness, and real-time access assurance

Advanced cryptographic, Random Number Generation, and Key Protection Services – Seamlessly integrated cryptographic solution, including QRC, secure provisioning, storage, and usage of secret keys.

Built-in advanced security services – Seamless integration of security services including features like secure device lifecycle, secure boot, secure debug, data and communication.

KSE3 SERIES

The Security IP that delivers peak performance

Built-in, robust HW Security – The KSE3 series targets security robustness AVA-VAN3 and enables SESIP/PSA L3 certification

Support for multiple applications and verticals – Responds to security requirements of multiple vertical markets, including automotive cybersecurity features. Kudelski can provide customizable security functions for customers' unique applications

Easy to integrate and use – Designed with a strong emphasis on ease to speed-up hardware and software integrations

Ultra-small design and footprint – Highly optimized for resources and footprint (~130Kgates, 10KB RAM and 80KB ROM for KSE3-100)

Built-in cryptographic & security services – Seamlessly integrated cryptographic solutions and security services for immediate Security IP deployment.

	FEATURES FOCUS	KSE3 SERIES	KSE5 SERIES
	Robustness to Physical and Logical attacks	AVA-VAN.3	AVA-VAN.5**
	Field examples	Soc, IoT devices	Highly secure applications
	Device Attestation	support	support
	Secure Updates		support
	Secure Provisioning and Decommissioning	support	x
	Secure Communication (Protocols)	support	support
	Secure Debug and Test	support	
	Secure Backup and Recovery	support	support
	Account Authentication and Management	NA	NA
SECURITY FUNCTIONAL PRIMITIVES	(Attested) Secure State and Life Cycle Management	x	x
	Genuine Identification	x	x
	Secure Initialization	support	x
	Anomaly Detection and Reaction	x	x
	Cryptographic Key Generation and Injection	x	x
	Cryptographic Key and Certificate Store	x	x
	Secure (Encrypted) Storage	x	x
	Cryptographic Operation	x	x
	Cryptographic Random Number Generation	x	x
	System Event Logging	support	support
	Silicon Root of Trust	x	x
	Residual Information Purging	x	x
	Software Isolation	support	x
	Monotonic Time	support	x
SECURITY PROCESS PRIMITIVES	Security by Design - Software Development Life Cycle	x	x
	Vulnerability and Incident Management, PSIRT	x	x
	Protection of Personal Information		x
	Secure Guidelines for Application	x	x

* Secure Boot, Key protection, Secure Flash access when flash is external. Dual Core, EDC, Memory scrambling.

** Spatial faults resistant architecture, anti-tampering protections for memories, clock, voltage

OUR VISION

From IP to Secure Solutions

Kudelski IoT 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.

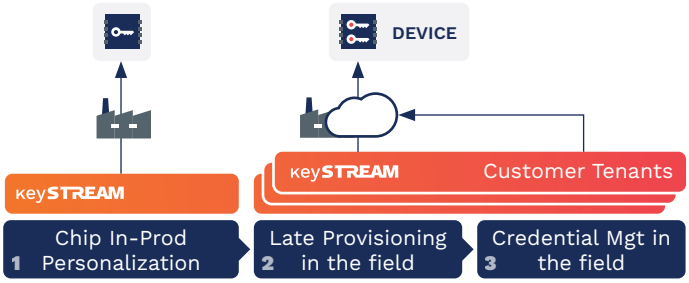
Key Renewability – rotate key material for extended lifetime

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

 V1.8

www.kudelski-iot.com