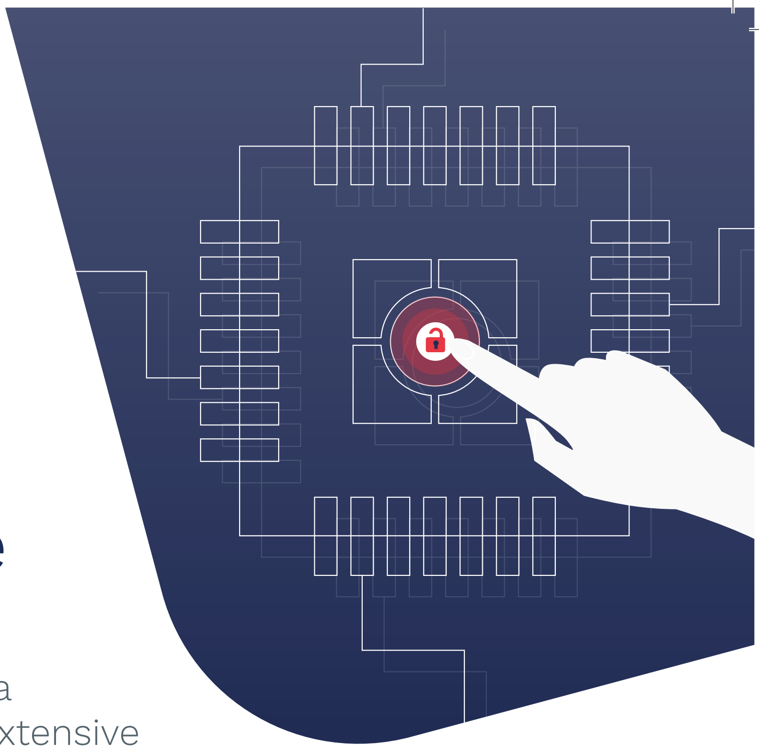
KUDELSKI IOT THINGS



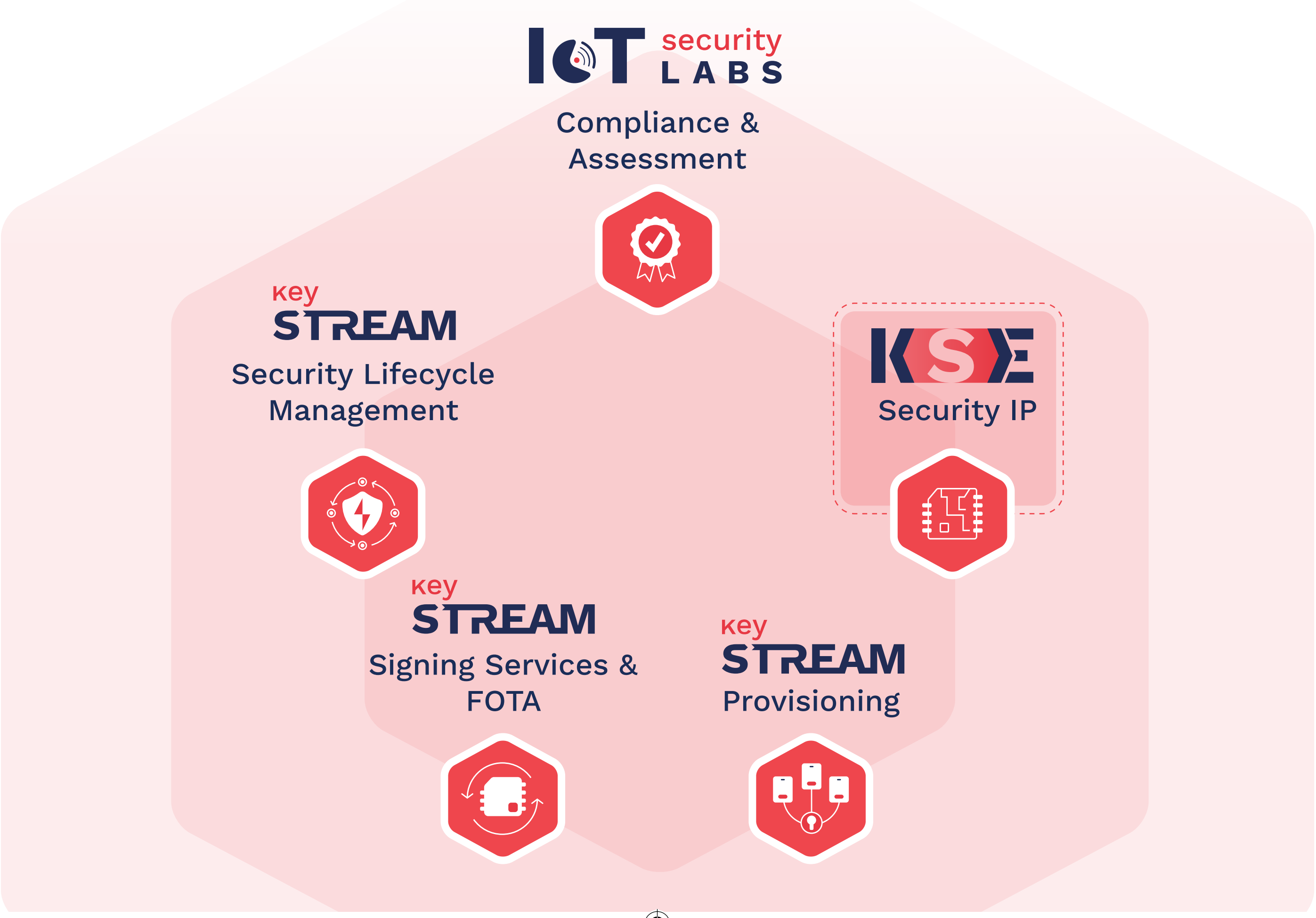
KSE The Cutting-Edge Hardware Security IP

Kudelski's IoT security approach embraces a comprehensive 360° perspective, offering extensive support to SoC manufacturers throughout the design and manufacturing lifecycles. We offer a complete suite of solutions and services that help you meet today's most challenging security requirements.

360° OFFERING

Security primitives to effectively develop comprehensive and secure end-to-end IoT solutions

The Kudelski IoT Security IP series, known as KSE, is the foundation of our integrated and comprehensive approach to security. Together with our Advisory Services and keySTREAM Lifecycle Services, we enable chipset vendors, device manufacturers, solution providers, and end-user customers with the essential security primitives necessary for the effective development and protection of end-to-end IoT solutions. This approach ensures a robust security framework that supports the entire IoT ecosystem throughout its entire lifecycle.



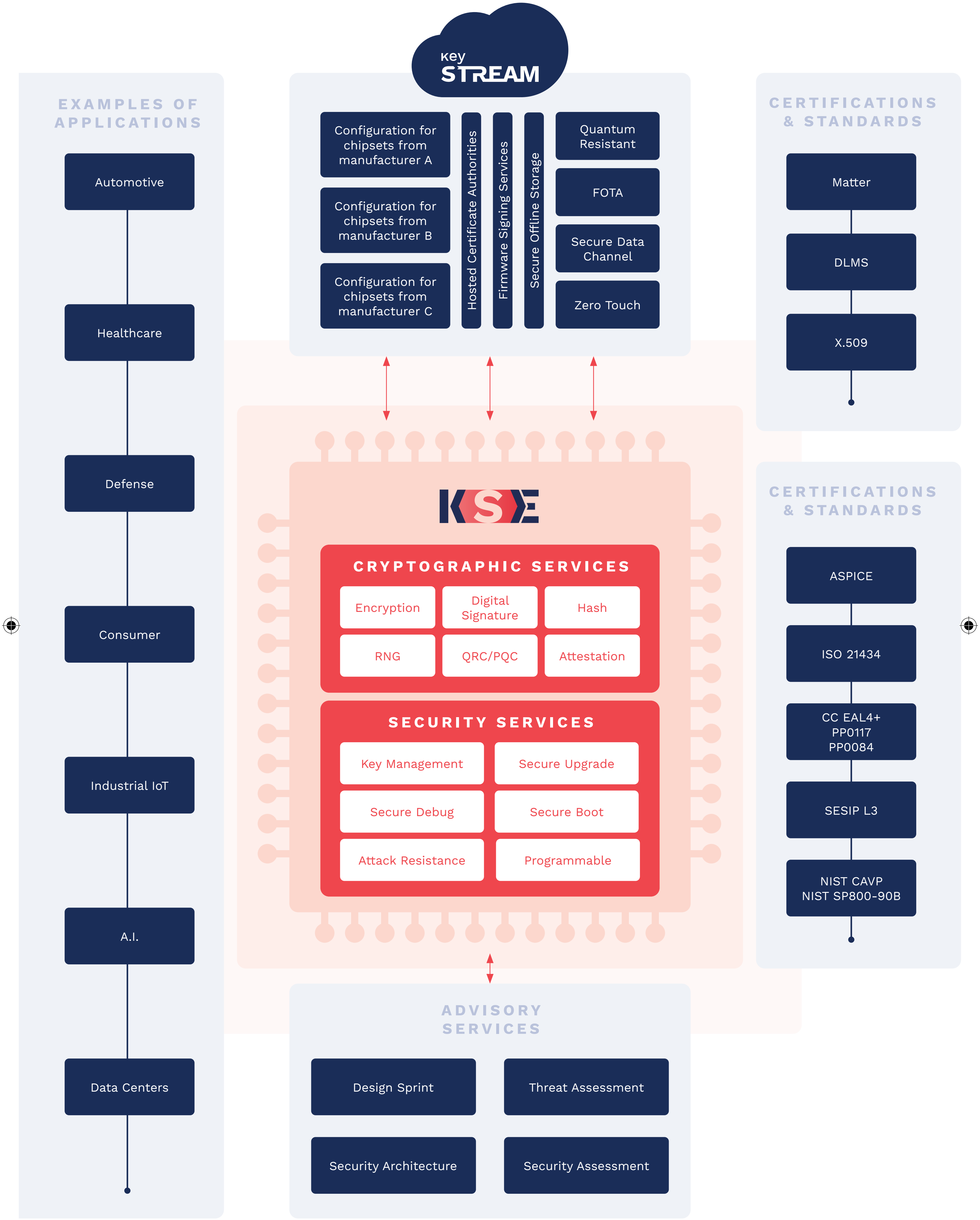
IoT security LABS
Compliance & Assessment

keySTREAM
Security Lifecycle Management

KSE
Security IP

keySTREAM
Signing Services & FOTA

keySTREAM
Provisioning



EXAMPLES OF APPLICATIONS

- Automotive
- Healthcare
- Defense
- Consumer
- Industrial IoT
- A.I.
- Data Centers

keySTREAM

- Configuration for chipsets from manufacturer A
- Configuration for chipsets from manufacturer B
- Configuration for chipsets from manufacturer C
- Hosted Certificate Authorities
- Firmware Signing Services
- Secure Offline Storage
- Quantum Resistant
- FOTA
- Secure Data Channel
- Zero Touch

KSE

CRYPTOGRAPHIC SERVICES

- Encryption
- Digital Signature
- Hash
- RNG
- QRC/PQC
- Attestation

SECURITY SERVICES

- Key Management
- Secure Upgrade
- Secure Debug
- Secure Boot
- Attack Resistance
- Programmable

ADVISORY SERVICES

- Design Sprint
- Threat Assessment
- Security Architecture
- Security Assessment

CERTIFICATIONS & STANDARDS

- Matter
- DLMS
- X.509

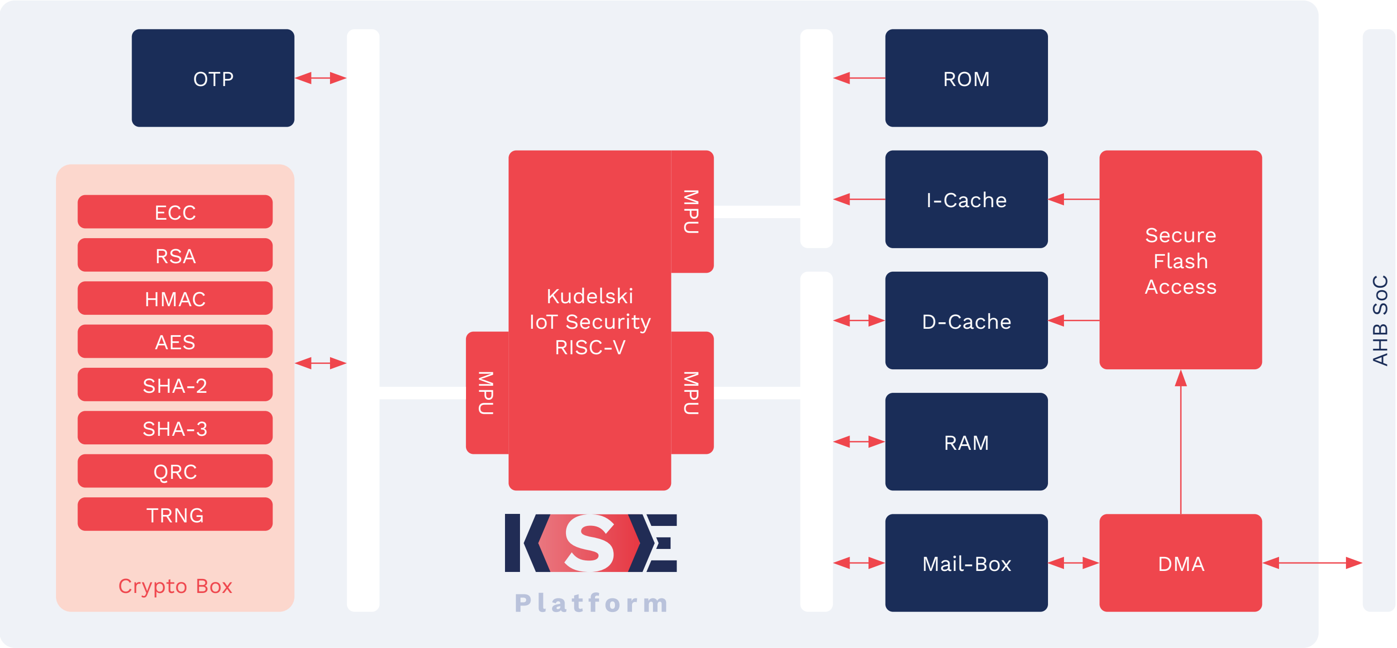
CERTIFICATIONS & STANDARDS

- ASPICE
- ISO 21434
- CC EAL4+ PP0117 PP0084
- SESIP L3
- NIST CAVP NIST SP800-90B

OVERVIEW OF OUR OFFERS

Ensuring the system security by safeguarding the integrity, authenticity, freshness, and confidentiality of assets

The KSE portfolio, Kudelski IoT's hardware security IP, provides SoC manufacturers with robust, modular, and advanced security and cryptographic capabilities. Our solutions address IoT security requirements, with upgradable cryptographic capabilities to adapt to evolving conditions. The KSE Portfolio provides a diverse range of proven, certification-ready embedded security features, compliant with key governmental and industry standards.



KEY BENEFITS

Built-in HW security – Combining a proprietary RISC-V processor with a robust and resilient security foundation, our solutions offer physical attack protection and anti-tampering capabilities to safeguard sensitive data and operations within the enclave.

Programmable Trust Application (TA) – Proprietary TAs are developed securely, isolated by the secure platform. The IP's secure debug can be utilized to facilitate TA development and integration.

Multiple use cases & verticals – Meets the security requirements and standards of multiple vertical markets and use cases.

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.

Cryptographic, Random Number Generation, and Key Protection Services – Seamlessly integrated cryptographic solution, including Quantum-Resistant Cryptography (QRC), secure provisioning, storage, and usage of secret keys.

Built-in advanced security services – Including secure device lifecycle, secure boot, secure debug, data and communication. The integration of these security services is simplified through the Kudelski Secure Services Library (KSSL).

KSE SOLUTIONS PORTFOLIO

Offering SoC manufacturers flexibility according to their specific needs for security, performance, and gate count

At Kudelski IoT, we acknowledge the multifaceted landscape of security standards, regulations, requirements, and services that are mandated by various use cases. In response to this complex environment, our product portfolio has been structured into two distinct product series, the KSE5 and KSE3, and complemented by a modular architecture. Each of these series is designed to meet a specific security level while providing a common core feature set.

Our portfolio organization reflects our dedication to delivering tailored solutions that serve diverse applications needs, offering SoC manufacturers flexibility according to their specific requirements for security, performance, and gate count. As part of our offering, we provide full support for integrating the KSE and obtaining certifications. Our products adhere to strong coding standards and undergo comprehensive assessments and audits.

FEATURES FOCUS	KSE5	KSE3
Security Robustness	AVA-VAN.5	AVA-VAN3
Targeted Certifications	CC EAL4+ PP0084, PP0117	SESIP L3, PSA RoT Components L3
Example of Applications	Highly Secure Applications, GSMA iSIM	General IoT, Automotive
Embedded CPU	Dual-core RISC-V	Single-core RISC-V
Cryptographic Primitives (Keys Gen & Mngt, HW Accelerators)	✓	✓
Secure Lifecycle Mngt (Perso, Provisioning, Return, Decommissioning)	✓	✓
Secure HW & SW Features (Secure Boot, Update, Debug, Anti-Replay, Isolation)	✓	✓
In-field Security Monitoring (Anomaly & System Events Mngt)	✓	✓
Secure Storage	✓	✓
Secure Communication	✓	✓
Options	Quantum Resistant Cryptography, Java OS Support, ISO21434, ASPICE	Quantum Resistant Cryptography, ISO21434, ROM-Based or Programmable

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

V3.6

www.kudelski-iot.com