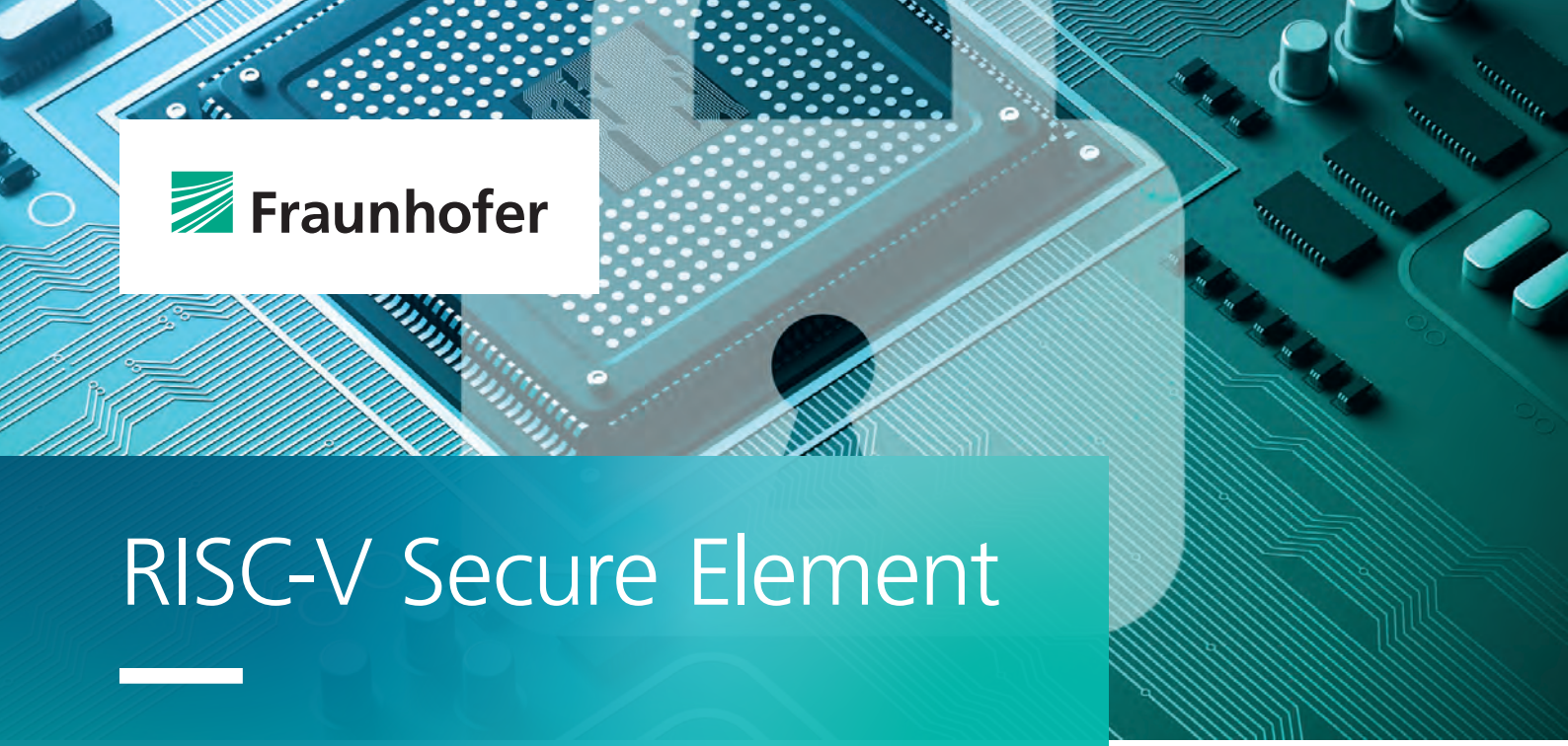


RISC-V Secure Element

Customized System-on-Chip Solutions for Sovereign and Future-Proof Security

© denisismagilov - stock.adobe.com / Fraunhofer IIS

The European Cyber Resilience Act introduces mandatory cybersecurity requirements for products with digital elements, fundamentally reshaping the design criteria for semiconductors and embedded systems. It obliges manufacturers to ensure security by design, vulnerability handling, lifecycle support, and demonstrable compliance from development through operation. For tomorrow's SoC and custom ASIC designs, this means that cybersecurity can no longer be treated as an add-on at software level – it must be anchored in hardware. Robust root-of-trust architectures, secure key storage, cryptographic acceleration, secure boot, lifecycle management, and tamper resistance become essential building blocks.

A dedicated secure element – available as silicon chiplet, IP, or fully integrated within custom SoC and ASIC solutions, provides the hardware-based trust anchor required to meet regulatory expectations while protecting intellectual property, sensitive data, and system integrity across the entire product lifecycle.

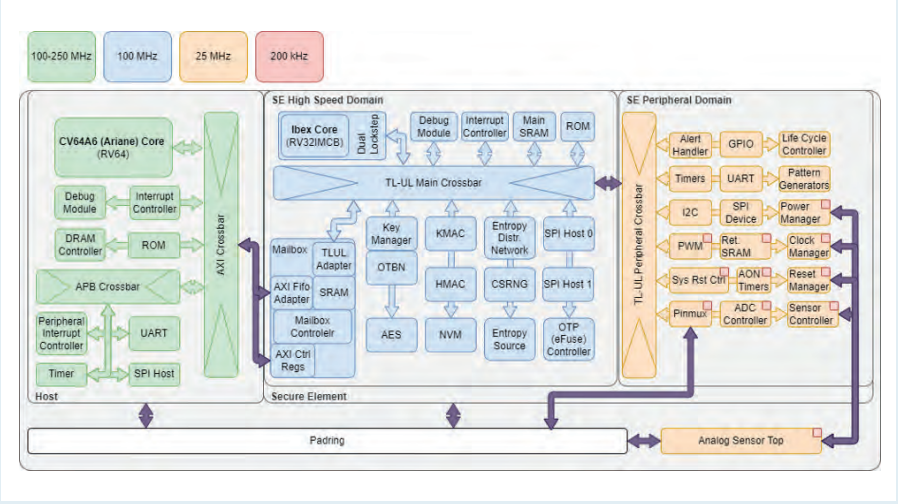
Fraunhofer's **OpenTitan-based RISC-V Secure Element** delivers precisely this: robust security features to safeguard your hardware devices against attacks. It supports both classical and post-quantum cryptography, ensuring resilience against current and future threats. With secure key storage, secure boot, secure update, and device authentication, your devices remain up to date and protected from unauthorized access.
The Secure Element also includes active monitoring for real-time threat detection and life-cycle management.

Fully sourced within the European Union for the highest possible level of technological sovereignty, the Secure Element is available as verified hard IP or as a packaged and tested stand-alone chip in GlobalFoundries 22FDX® technology. It can also be deployed in an FPGA environment for rapid prototyping or software development purposes.

Based on this development, Fraunhofer offers turnkey custom chip design services for tailored solutions according to application-specific requirements.

Key Features

- Hardened 100 MHz 32-bit Ibex Core (RV32IMCB)
- (Post-Quantum) secure boot and secure update
- Support for DICE (Device Identifier Composition Engine) and remote attestation
- Cryptographic key store and API
- Hardware accelerators for classic and post-quantum cryptography
- Designed and tested to withstand side-channel and fault attacks
- Device identity and originality checks
- Entropy source and random number generation – NIST and BSI compliance ready
- Alert handler for actively handling critical security events
- Memory and bus scrambling
- Certifiable for Common Criteria EAL 4+ security level



Block diagram of the RISC-V-based Secure Element subsystem with security functions and a comprehensive set of peripherals
© Fraunhofer IIS

Cryptographic Algorithms

- AES-128/192/256 with ECB/CBC/CFB/OFB/CTR
- HMAC / SHA2-256
- KMAC / SHA3-224, 256, 384, 512, [c]SHAKE-128, 256
- SLH-DSA (SPHINCS+) post-quantum signature accelerator
- Programmable big number accelerator for RSA, ECC as well as ML-DSA (Dilithium) and ML-KEM (Kyber)
- Cryptographically secure random number generator (CSRNG) compliant to NIST SP-800, BSI AIS31

Communication

- Host SPI
- Device SPI
- I²C
- UART
- GPIO
- Secure Debug JTAG Interface
- Mailbox interface for AXI bus connecting to larger SoC systems

Memories

- 2 MB MRAM
- 4 kB eFuse OTP
- 64 kB Boot ROM
- 256 kB SRAM

Ecosystem

- Deployable as standalone microcontroller or SoC component
- Manufactured in GlobalFoundries 22FDX® technology and packaged in the EU
- Small volume production possible
- Application and customer specific instruction set extensions and co-processors possible
- Cryptographic agility with hardware support for more algorithms, e.g. Falcon (FN-DSA) or FrodoKEM

Services

- Integration support and customer specific modifications
- FPGA Implementation available for testing and prototyping
- Chip development support
- Foundry services and chip packaging
- Application development support
- Documentation and certification support

Contact

Gerald Moser
Phone +49 9131 776-4439
gerald.moser@iis.fraunhofer.de

Fraunhofer IIS
Am Wolfsmantel 34
91058 Erlangen
www.iis.fraunhofer.de

Andreas Seelos-Zankl
Phone +49 89 32299 86-186
andreas.zankl@aisec.fraunhofer.de

Fraunhofer AISEC
Lichtenbergstraße 11
85748 Garching near Munich
www.aisec.fraunhofer.de

www.iis.fraunhofer.de/secure-elements-and-accelerators

Sponsored by

Bavarian Ministry of Economic Affairs, Regional Development and Energy