QASIC™

Quantum Resistant Custom Integrated Circuit

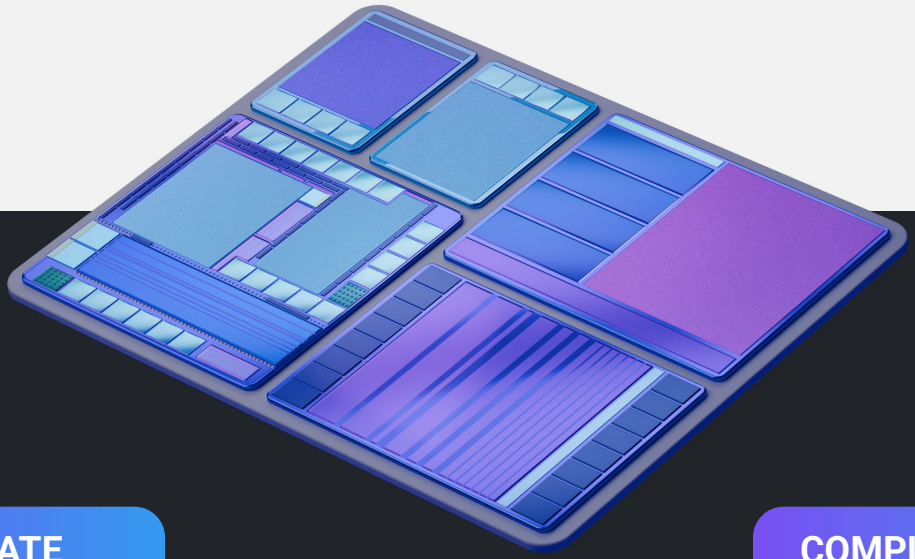
A turnkey ASIC design service accelerating the design and supply of quantum-resistant integrated circuits with a customizable microcontroller platform embedding a pre-validated post quantum security module, functional safety hardware mechanisms and efficient power management.

Post-Quantum Security
Hardware accelerated eRoT and eHSM

Functional Safety
Transient and latent fault detection with safe-state management

Efficient Power
Ultra-low power and always-on management

Microcontroller Platform
RISC-V based infrastructure, ready to customize



ACCELERATE

Fast-track your secure ASIC development. Build on proven IP, design flows and security expertise to reduce development time, risk and time-to-market.

CUSTOMIZE

Make security fit your application. Tailor architecture, interfaces, performance, power, safety and security features to the exact requirements of your product and market.

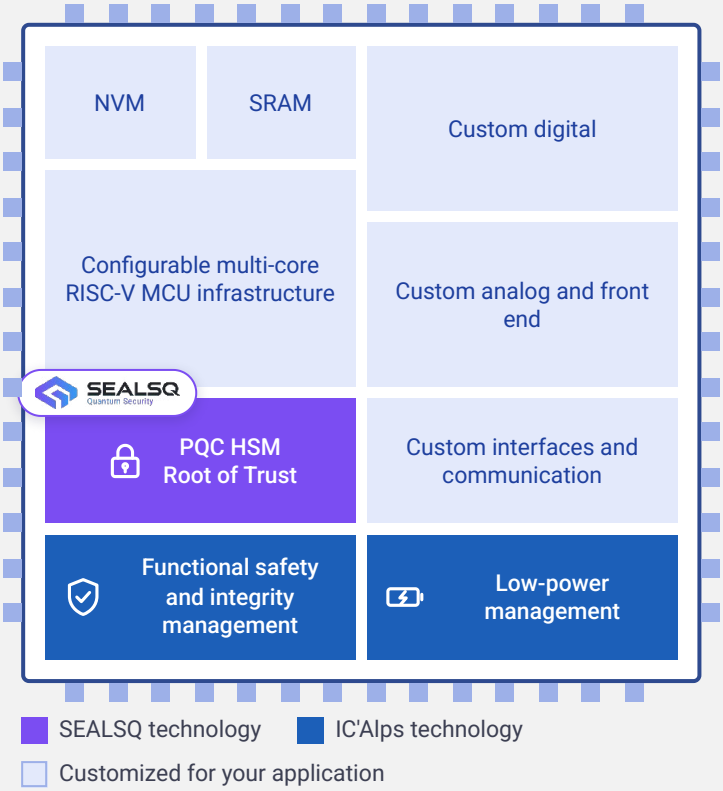
COMPLY & CERTIFY

Design for certification from day one. Embed security, safety and compliance requirements early to streamline certification against ISO 26262, ISO 26262, IEC 62443, SESIP or FIPS 140-3.

IC'ALPS

SEALSQ

Get your quantum-resistant and safe chip faster with QASIC



From high-level system requirements or a defined specification, IC'Alps customizes and tailors the platform to your expectations in features, performance, power consumption, security assurance, safety integrity, reliability and end-product certification objectives. Different levels of security services and integration options are possible with QASIC. Ask us for details.

You get

- A custom ASIC designed and supplied by IC'Alps, from specifications to production parts
- A starting microcontroller platform, already integrated and validated, with:
  - SEALSQ post-quantum cryptography secure Root of Trust (ML-KEM, ML-DSA) and services (RSA, ECC, AES, SM3, SM4)
  - A secure channel to an external EAL5+ secure element for chiplet integration
  - Functional safety support up to ISO 26262 ASIL-D and IEC 61508 SIL 3
  - Low-power management down to a few nanowatts
- Custom digital, analog and mixed-signal design
- Security and safety work products

Why Now

Quantum computers will break RSA and ECC, which protect firmware updates, device identity and communications. For long-lifecycle devices, the migration to quantum resistance must happen now. The longer a product stays deployed, the stronger the need for crypto-agility, quantum-resistant trust anchors, secure update mechanisms and sustained lifecycle management.

Platform Features

- **Security:** secure boot • identity and attestation • lifecycle • key management • crypto and PQC • isolation and filtering • secure communications
- **Safety:** lockstep • fault detection and containment • QoS and partitioning • safe-state management
- Power domains and always-on logic
- Dual-core RISC-V with standard peripherals: memory controller, DMA, interrupt controller, UART, SPI, GPIOs and more

Mission-Critical Applications

Long lifetimes amplify exposure to the quantum threat. QASIC is suited to:

- Automotive MCUs, SoCs and smart sensors
- Active implantable medical devices
- Aerospace, defense and avionics devices
- Industrial automation and robotics

Turnkey Services

- From requirements and design to qualified chips in volume
- Embedded software: low-level security firmware, CSP, BSP, RTOS
- Security aligned with ISO 21434, IEC 62443 and Common Criteria
- Safety aligned with ISO 26262, IEC 61508 SIL 3 and DO-254
- Quality certified to IATF 16949, ISO 13485 and EN/AS/JISQ 9001
- A unique identity injected in every chip by SEALSQ