TROPIC01

Security through
open hardware

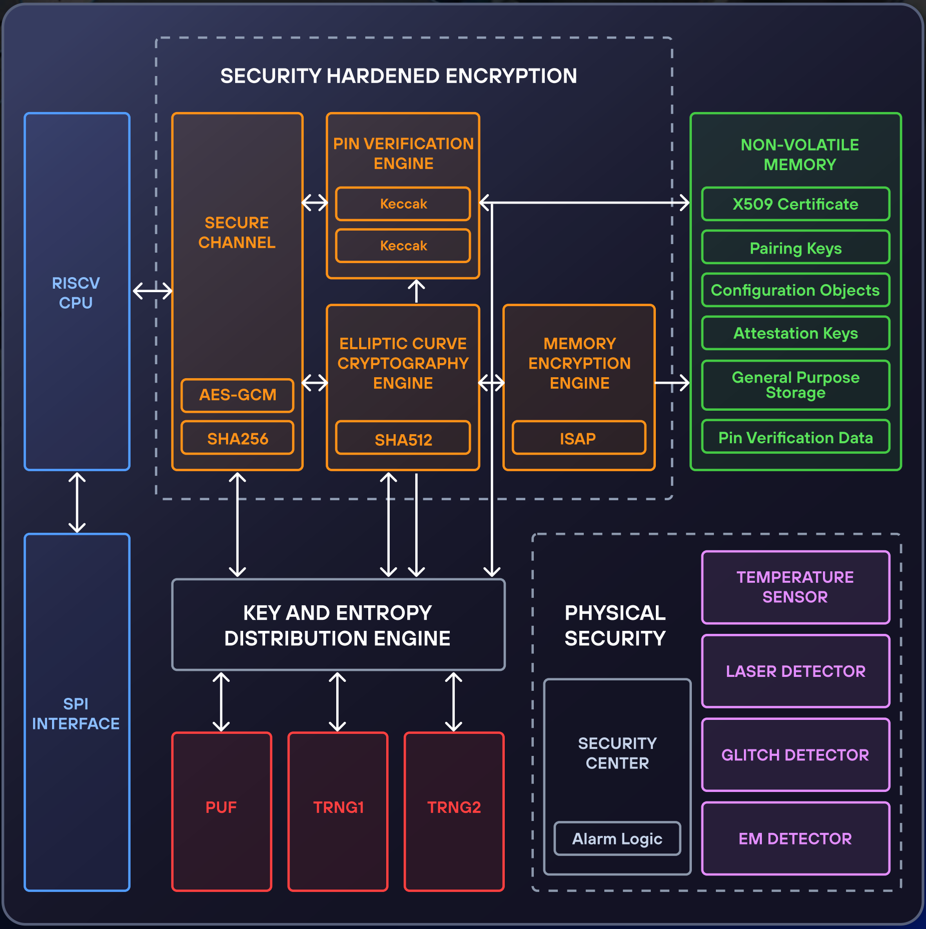
Data Brief

TROPIC01 is a truly open secure element that supplies and enhances the cryptography of your secure Hardware.

The security design details provide visibility into the implementation, enabling independent security audits that can be shared.

Our Integrated Circuit (IC) provides a more secure means of protecting your private keys from both physical and logical attacks – even when the chip is powered off.

Implementing this secure element in your hardware devices delivers identity, authentication, data protection, and a hardware root of trust.



Security Highlights

Tamper Resistance

- Voltage Glitch Detector
- Temperature Detector
- Electromagnetic Pulse Detector
- Laser Detector
- Active Shield

Cryptographic Accelerators

- State of the Art Elliptic Curve Cryptography
  - Ed25519 EdDSA signing
  - NIST P-256 ECDSA signing
- MAC & Destroy pin authentication scheme

Entropy Source

- Physically Unclonable Function (PUF)
- True Random Number Generator (TRNG)

Integration Support

- SW driver for the external host to communicate with TROPIC01

Features

Onchip RISC-V IBEX CPU

- Secure Firmware (FW) update
- Customizable FW available upon request

Memory

- OTP Memory:
  - Stores x.509 certificate and keys
  - Secure Anti-fuse technology
- Flash Memory:
  - Stores general purpose and PIN verification data and ECC keys
  - On-Encrypted with ISAP
- Both memories protected by Error Correction Code

Communication Interface

- SPI application control
- Noise protocol Secure channel
  - Forward secrecy
  - AES-GCM encryption
  - X25519 Diffie-Hellman key exchange
- SDK available for internal RISCV CPU

Unique Advantage

TROPIC01 delivers a new standard in secure elements – open to inspection, hardened against attacks, and designed for customization. At its core is a verifiable Hardware Root of Trust, ensuring ultimate device integrity and setting a new benchmark for transparency in embedded security.

Core Capabilities:

- Auditable
- Large secure non-volatile storage (memory 237 kB)
- Physically Unclonable Function (PUF)
- Mac & Destroy patented solution (PIN verification)
- Secure channel (NOISE Protocol)
- Customization readiness (incl. vendor key and FW updates)
- Designed in the European Union

Target Application

Having a strong security system is crucial for protection against hacking attacks. Use TROPIC01 as a building block in your embedded secure system to protect your privacy at a hardware level.

TROPIC01 enables security for solutions such as:

- Hardware Wallets
- IoT Device Communications
- Security Systems
- Hardware authenticators
- Smart Infrastructure
- Industrial Machines

Use Case with TROPIC01

Hardware Root of Trust

The private keys never leave the chip and are protected by hardware enforced security boundaries & anti-tamper features. The chip is secure by design and can be independently audited to verify the level of protection it provides.

Hardware-based Digital Identity

User's identity, keys, and assets are securely stored inside the chip. The unique physical properties of the chip, combined with its security features, enables a cryptographically secured chain.

Data Authenticity

TROPIC01 signs user data with Ed25519 EdDSA and P-256 ECDSA algorithms. These algorithms are implemented in side-channel resistant hardware accelerators and enable cryptographic verification of the signed data's authenticity.

Software Support & Customization

- Customization available to meet specific requirements
- Full SDK support for easy and flexible integration into user applications
- Reference applications

Explore TROPIC01 technical library on GitHub

visit our GitHub ⟶