# TROPIC01

Cryptographic Coprocessor and Secure Storage IC

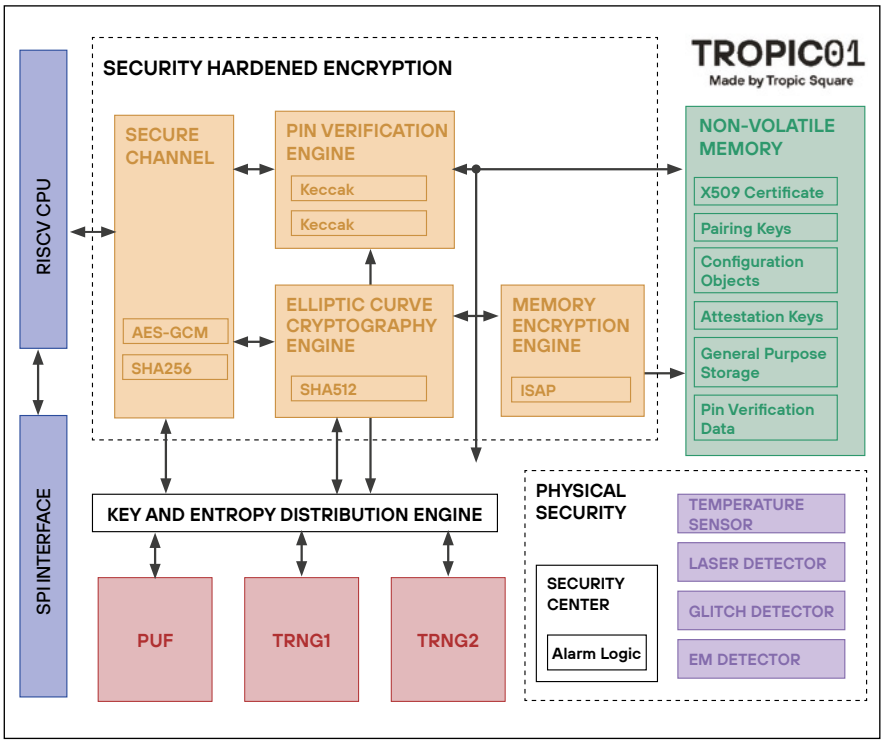
Product Brief

TROPIC01 is an open architecture secure element that serves as a foundational security component for embedded systems – providing a hardware Root of Trust to ensure security.

Within its secure perimeter, TROPIC01 enables cryptographic key management, digital identity, and secure data storage for critical applications.

TROPIC01 offers transparency by having security design details, source files, and documentation available for independent security auditing.

Implementing the secure element enables use cases such as secure boot, firmware updates, key management, and device identity.




## Security Highlights

### Tamper Resistance

- Voltage glitch detector
- Temperature detector
- Electromagnetic pulse detector
- Laser detector
- Active shield

### Cryptographic Accelerators

- Elliptic curve cryptography
  - Ed25519 EdDSA signing
  - P-256 ECDSA signing
  - Diffie-Hellman X25519 key exchange
- Keccak based PIN authentication engine
- SHA256 and SHA512
- AES256-GCM
- ISAP

### Entropy Source

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

## Features

### Onchip RISC-V IBEX Controller Core

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

### Memory

- OTP to store x.509 certificate and keys
- Flash to store general purpose and PIN verification data
- Memory address scrambling
- On-the-fly encryption
- Error correction code protection

### Communication Interface

- SPI application control
- Encrypted channel with forward secrecy

### Integration Support

- SW driver for the external host to communicate with TROPIC01
- SDK available

## Target Applications

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. The unique physical properties of the chip, combined with its security features, enables a cryptographically secured chain to TROPIC01.

**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 to meet specific requirements
- SDK for easy and flexible integration into user applications
- Reference applications

***Get TROPIC01 Samples for Evaluation and Prototyping Now***

Sign Up Here