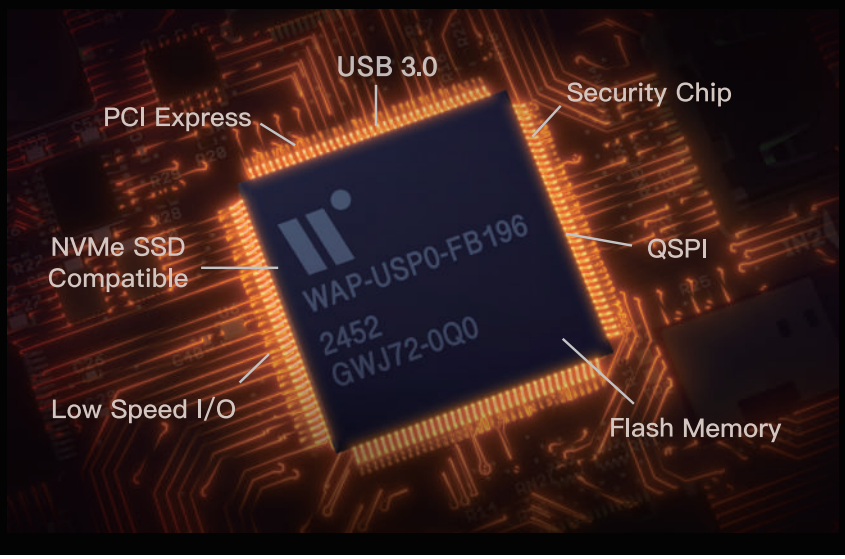
WAP - The Next-Gen High-Performance Crypto Application Processor



A Next-Generation Cryptographic Platform Balancing Security, Performance, and Flexibility

The WAP is a high-performance cryptographic application processor purpose-built to meet the evolving cybersecurity demands of the post-quantum era. Designed with a hardware-based Root of Trust, it supports the deployment of customizable application firmware or dedicated ASIC implementations. Positioned between rigid traditional security chips and less-secure MCUs, WAP delivers the ideal blend of robust security, exceptional performance, and architectural flexibility. Perfectly suited for edge devices such as drones, secure boot processes, blockchain cold wallets, hardware authenticators, and Hardware Security Modules (HSMs), WAP is the foundation for mission-critical, future-proof security systems.

Future-Ready with Seamless Post-Quantum Migration

As quantum computing continues to accelerate, legacy encryption methods like RSA and ECC face increasing vulnerabilities. The global cybersecurity community is entering a transformative period—referred to as Y2Q (Year to Quantum)—requiring immediate adoption of quantum-safe technologies.

To address this, the U.S. government's NSA CNSA 2.0 mandate requires all federal systems and supply chains to adopt post-quantum cryptographic (PQC) algorithms by 2025. In response, WiSECURE proudly introduces WAP—a fully PQC-ready processor supporting the latest NIST-standard algorithms ML-KEM (for key encapsulation) and ML-DSA (for digital signatures), while remaining backward-compatible with RSA and ECC. This hybrid model ensures smooth, low-risk migrations to quantum-resilient infrastructure.

Key Features

Supports International PQC Standards

- Complies with NIST PQC algorithms:
  - Kyber (ML-KEM) – Key Encapsulation Mechanism
  - Dilithium (ML-DSA) – Digital Signature Algorithm
- Hybrid Signature Support for seamless interoperability with existing RSA/ECC systems

Hardware-Level Security & High-Speed Processing

- PUF (Physical Unclonable Function) technology ensures a unique, tamper-resistant master key
- Built-in high-speed AES engine for symmetric encryption (up to 1 Gbps), optimized for low-power edge applications

Flexible Architecture for ASIC Customization

- Modular chip design supports tailored cryptographic solutions for specific applications
- Accelerates development while reducing R&D costs and deployment risks

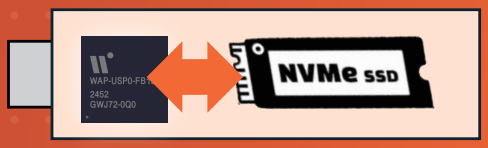
Custom ASIC

Designed for a Broad Range of Applications

- FIDO-compliant authentication devices
- Hardware Security Modules (HSMs)
- Blockchain cold wallets and hardware wallets
- Smart meters and industrial IoT security
- Online payments and financial cybersecurity
- Encrypted drone communication links
- Portable secure communication terminals

HSM / FIDO secure authenticator

Secure Boot and Cryptographic Accelerator for Edge Device SoCs



Storage Protection

Payment Terminal

Technical Specifications

Supported Cryptographic Algorithms

- Symmetric Encryption:
  - AES-128 / 192 / 256 (Supports ECB, CBC, GCM, and all NIST modes, throughput up to 1 Gbps)
- Traditional Public-Key Encryption:
  - RSA (up to 4096-bit)
  - ECC (Elliptic Curve Cryptography)
- Post-Quantum Cryptography (PQC):
  - Kyber (FIPS 203 / ML-KEM)
  - Dilithium (FIPS 204 / ML-DSA)

Hardware Interfaces

- USB 3.0
- QSPI / SPI
- GPIO
- PCI Express (PCIe)
- NOR Flash

Architecture

- 32-bit ARM Processor
- 512 KB SRAM
- No internal persistent storage

Advanced Security Features

- SP 800-90B compliant True Random Number Generator (TRNG)
- Tamper detection and physical environment monitoring
- Sensitive circuit shielding
- Secure interface binding
- Embedded PUF technology for master key protection

Compliance & Certification

- CNSA 2.0 compliant
- FIPS 140-3 Level 3 (Certification in progress, including CAVP validation)

WiSECURE Inc.
15F, CIC Tokyo, Toranomon Hills Business Tower,
1-17-1 Toranomon, Minato-ku, Tokyo 105-6490, Japan
https://wisecure-tech.jp

Leading the Future of Cybersecurity
WiSECURE is at the forefront of secure computing, with deep expertise in post-quantum cryptography and secure chip architecture. The WAP processor is engineered to meet the next decade's cybersecurity challenges across government, finance, manufacturing, and ICT sectors.
The launch of WAP not only reflects a technological leap for Taiwan in the field of PQC security chips, but also cements WiSECURE's role as a trusted innovator and global leader in quantum-resilient cybersecurity.