The SDK Datasheet for miniEVB integrated with PQC KAP01 Chip PoC

2025.02 Evaluator Version

Overview

The PQC (Post-Quantum Cryptography) KAP01 chip family is designed as an cryptographic application processor (AP processor), not merely a cryptographic module, yet it delivers powerful cryptographic capabilities. Beyond hardware-based security, it integrates built-in application functionalities and versatile hardware interfaces for seamless integration.

The firmware platform of KAP01 chip can make the chip as a powerful SoC (System-on-Chip). KAP01 owners can develop on the USB3 host side application-specific login inside the firmware platform which will create the chips for the application unqiue to the customers' requirements.

The Mini EVB SDK streamlines evaluation, prototyping, and deployment of the KAP01 chip, enabling developers on the USB3 host side to accelerate proof-of-concept (PoC) development and fast-track quantum-resistant security solutions.

For the mission-critical applications which need the talor-made functionalities within KAP01, please contact WiSECURE sales to get the customization services.

The SDK Features

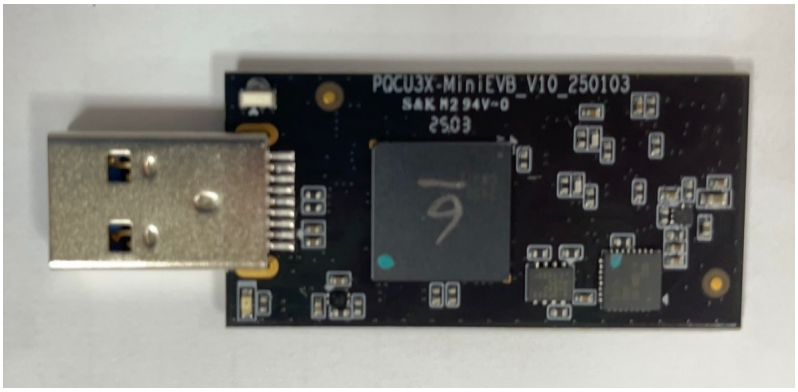
The miniEVB SDK (Evaluator Version) use the plugin interface in USB3.0, allowing users to evaluate both Classic cryptographic and PQC operations use cases, which include:

- Classic cryptographic operations
  - ECDSA (P256, P384, P521)
  - ECDH (P256, P384, P521)
  - AES (128, 192, 256)
    - Modes of Operation:
      - SP 800-38A: ECB, CBC, OFB, CFB, CTR
      - SP 800-38D: GCM
      - SP 800-38E: XTS

- Post Quantum cryptographic operations
  - FIPS 203 ML-KEM
    - Key Generation
    - Encaps
    - Decaps
  - FIPS 204 ML-DSA
    - Key Generation
    - Sign
    - Verify

SDK Deliverables

- MiniEVB hardware (KAP-USP0-MiniEVB Board)
- MiniEVB firmware
- MiniEVB CLI Tool
- KAP01 verification Tool
- KAP01 API SDK (PC Host-side)
- User Document



Reference Photos of Mini EVB Hardware

Note: The name printed on the EVB board is an internal designation.
The actual product is equivalent to the official product name KAP-USP0-MiniEVB Board

Revision History

Revision	Date	Author	Description
1.0	2025/02/01	Chris	Initial Version
1.1	2025/03/01	Rose	Update Official Name of EVB