Wisecuretech

# CryptoAir®+

## Hardware-based Data Protection for Enterprises


Built-in Crypto Engine

Key Management Interface

Agile Crypto Platform

FIDO2 Strong Authentication (FIDO2 & U2F)


## Data Safeguard for Clouds and Ends

**Features of CryptoAir®+**

- Comprehensive crypto service
- Military-grade secure key storage
- Resistance to side-channel attack (SCA)
- Customizable cryptographic algorithms

CryptoAir®+ is an advanced encryption engine featuring password-less/multi-factor authentication. The product covers entry-level authentication and protection of data at rest. It provides crypto service for enterprise to perform encryption, strong authentication, digital signature, etc. The secure element inside is CC EAL 5+ certified, resisting side-channel attack.

The crypto platform allows for customization of cryptographic algorithms. Post-quantum cryptography (PQC) can operate on the platform.

## SNAS (Secure Network Attached Storage)

**SNAS (Secure Network Attached Storage)**

- Secure data storage on premises
- File-based encryption
- Key management best practices (NIST SP 800-57)
- Privileged Access Management

The risk of data leakage comes from internal and external factors. Internal factors include insider thefts. NAS (Network Attached Storage) commonly used in enterprises, if without any protection, is prone to data breach. Since insiders can directly exchange disks without leaving any trace, data stored in the disk may be accessed through another machine. CryptoAir®+ enables data stored in the disk to be bullet-proof. It serves as an AES encryption engine making data ciphertexts. The secret key is stored in the military-grade secure element in the CryptoAir®+ USB device.

A management console is designed to allow for intuitive management with drag-and-drop simplicity. Users can set the privileges of each CryptoAir®+ USB device. The mechanism greatly reduces laboursome work of access control setting.

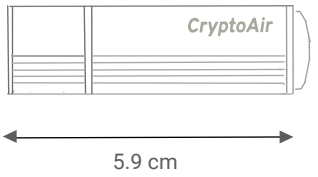
## DPX (Data Protection during/after eXchange)

**DPX (Data Protection during/after eXchange)**

- Remote/branch/enterprise secure data sharing
- File-based encryption
- FIDO authentication framework
- Zero trust with FIDO2 strong authentication

Enterprise data sharing methods such as email or uploading to clouds are prone to malware, man-in-the-middle attack and unauthorized access. Once a data breach occurs, data cannot be retrieved. DPX (Data Protection during/after eXchange) with CryptoAir®+ provides military-grade hardware-level data sharing security. Before any file is uploaded to the cloud, CryptoAir®+ will encrypt the file on the client-side laptop/desktop. The user-friendly management console enables users to set the privileges and access right of the file. Only those who possess CryptoAir®+ or AuthTron™ can attain access right.

DPX is a total data protection solution featuring crypto-based strong authentication (password-less and multifactor) under FIDO (Fast Identity Online) framework. Users can further integrate logging audit, AI-based threat detection, code signing and others to enforce rigorous policy.




# Specification

* regarding your needs

| | |
|---|---|
| Supported Applications | • File Protection Application Package<br>• Key Sharing Application Package<br>• FIDO External Authenticator (U2F, FIDO2)<br>• QNAP NAS Application (QPKG)<br>• WiSECURE Touch Pattern User Presence<br>• MS-CSP/MS-CNG<br>• Web USB |
| Authentication Features | • Crypto-based authentication<br>• Security policy for limited login attempt<br>• Touch pattern for user presence |
| Crypto Algorithms and Services | • AES GCM/ECB/CTR/CBC*<br>• ECDSA/ECIES/ECDH/ECMQV/EdDSA/ECDAA*<br>• RSA 2048/4096<br>• MAC/HMAC<br>• SHA256/SHA3/SHA384<br>• Key Wrapping and Unwrapping<br>• Key Derivation Function<br>– PBKDF/KBKDF<br>• Random Number Generation<br>– DRBG with AIS-31 Certified TRNG (SP 800-90A) |
| Performance | • AES (CTR) 7MB/s<br>• ECDSA signing 48 tps(P-384), 102 tps (P-256) |
| Cryptographic API | • PKCS#11<br>• Native API |
| Certification | • FIDO2 Level 1 and U2F Level 1 (Level 2 in progress)<br>• FIPS 140-3 Level 3 (certificate arranged)<br>• CC<br>• FCC<br>• RoHS<br>• VCCI |
| Specification | • USB 2.0<br>• Composite HID, Mass storage USB classes<br>• Chip Card Interface Device*<br>• RBG LED Indicator<br>• Electronic Touch Sensor<br>– Cognition-oriented / Thought-directed |
| Storage | • CC EAL 5+ Secure Element Key Storage 256 KB |

## Why should you choose WiSECURE data protection?

### Comprehensive Product Portfolio

With crypto modules applied to clouds and ends, WiSECURE is also engaged in deployment and consulting, expecting to help customers clarify potential risks in specific use cases so as to constitute the most cost-efficient solution.

### Crypto Implementation and ODM Service

From low-level crypto functions to hardware development, WiSECURE builds security products from the grounds up and also provides ODM service for customers requesting branded security keys.

### Cost-efficient Key Management

We provide key management best practices complying with NIST SP800-57. Customers can save technical effort and reduce cost.


## Speedy Deployment and High Adaptability

Faced with quantum threat brought by quantum computers, CryptoAir®+ possesses a quantum-safe and future-proof crypto core. It satisfies the need to customize algorithms, to employ new standards and to migrate to post-quantum cryptography (PQC). Deploying new algorithms does not require hardware replacement, which resolves the issue of end of life (EOL).

To know more about our solution or FIDO2 application, please contact us.

https://www.wisecure-tech.com/contact/

+886-2-29343166