CryptoAir+

Light-weight USB-based Hardware Security

**Built-in
Crypto Engine**

**Key Management
Interface**

**Agile Crypto
Platform**

**Passwordless & MFA
(FID02 &U2F)**

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

Data Safeguard for Clouds and Ends

CryptoAir®+ is an advanced encryption engine featuring password-less/ multi-factor authentication. The product covers entry-level authentication and protection of data at rest. tI provides crypto services for enterprises 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 the customization of cryptographic algorithms. Post-quantum cryptography (PQC) can operate on the platform.

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

SNAS (Secure Network Attached Storage)

The risk of data leakage comes from internal and external factors. Internal
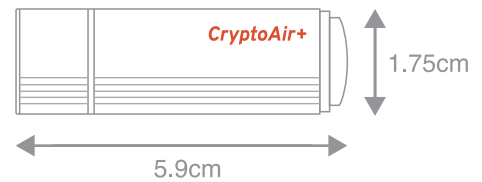
factors include insider thefts. NAS (Network Attached Storage) commonly used ni enterprises, fi without any protection, is prone to data breaches. Since insiders can directly exchange disks without leaving any trace, data stored on the disk may be accessed through another machine. CryptoAir®+ enables data stored in the disk to be bullet-proof. tI 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 the laboursome work of access control setting.

FileAegis®
- Remote/branch/enterprise secure data sharing
- File-based encryption
- FIDO authentication framework
- Zero trust with FID02 strong authentication

FileAegis® - Zero Trust Architecture Infra

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. FileAegis® 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 rights of the file. Only those who possess CryptoAir®+ or AuthTron® can attain access rights.

FileAegis® 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 audits, AI-based threat detection, code signing, and others to enforce rigorous policy.

CryptoAir+

1.75cm

5.9cm

Specification

Supported Applications	File Protection Application Package Key Sharing Application Package FIDO External Authenticator (U2F, FIDO2) QNAP NAS Application (QPKG) WiSECURE Touch Pattern User Presence WebUSB (Package installation required)
Authentication Features	Crypto-based authentication Security policy for limited login attempt Touch pattern for user presence
Crypto Algorithms and Services	AES GCM/ECB/CTR/CBC ECDSA/EdDSA ECIES/ECDH/ECMQV RSA 2048/4096 MAC/HMAC SHA256/SHA3/SHA384 Key Wrapping and Unwrapping Key Derivation Function - PBKDF/KBKDF Random Number Generation - DRBG with AIS-31 Certified TRNG (SP 800-90A)
Performance	AES (CTR) 7MB/s ECDSA signing 48 tps(P-384), 102 tps (P-256)
Cryptographic API	PKCS#11 Native API
Certification	CE FCC RoHS VCCI
Hardware Specification	USB 2.0 Composite HID, Mass storage USB classes Chip Card Interface Device RBG LED Indicator Electronic Touch Sensor - 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 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 ground 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 costs.
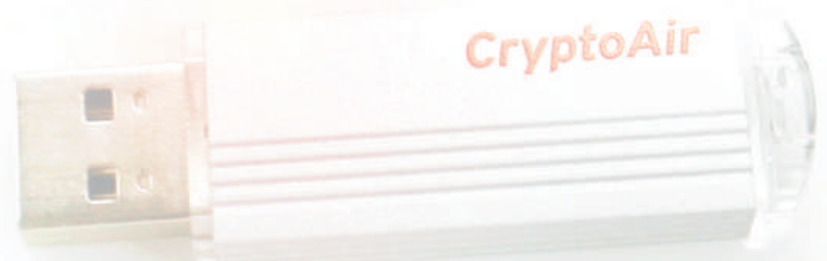
Speedy Deployment and High Adaptability

Faced with the quantum threat brought by quantum computers, CryptoAir®+ possesses a quantum-safe and future-proof crypto core. It satisfies the need to customize algorithms, 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).

Contact us
WiSECURE Technologies Corporation
4F., No. 218, Sec. 6, Roosevelt Rd., Wenshan Dist.,
Taipei City 116, Taiwan R.O.C.
+886-2-29343166
support@wisecure-tech.com