Wisecure
Technologies

MICRO HSM

— µSD/X

Features
Use cases
Security and cryptographic features
Hardware specification

high-speed encryption optimizing secure communication

> *Typical HSM (hardware security modules) come in the form of a PCIe card, used in PKI environments and mission-critical infrastructures, for cryptographic functions and digital key protection. However, the module is mostly applied to servers, not available for mobile devices or end-to-end environments.*
>
> *µSD/X is a hardware security module coming in the form of a microSD card. It provides security services driven by hardware-based crypto engines, including encryption, key generation and life cycle management, digital signature, authentication and other crypto functions. The groundbreaking design accelerates customizable storage encryption reaching 7MB/s, surpassing all the other competitive products on the market.*

Features

Interface compatibility

With SDIO (secure digital input/output) interfaces and common access modes, it is compatible with mobile devices.

Physical security

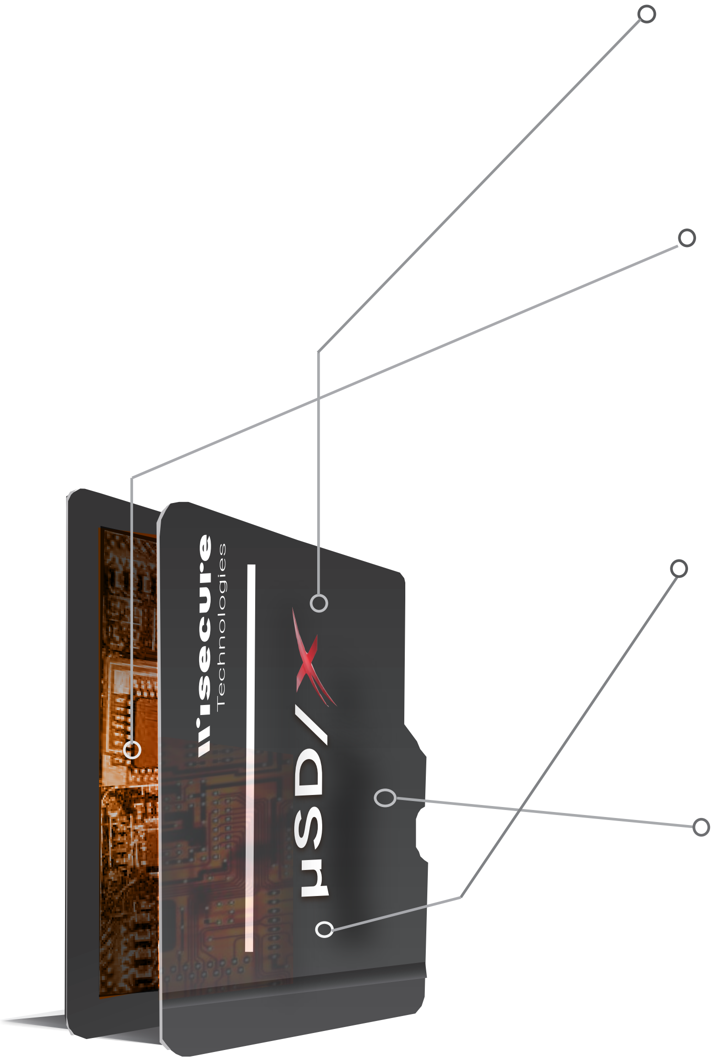
Robust internal circuit design, CC EAL 5+ certified components commensurate with military-grade security, and cutting-edge countermeasures to cyberattacks ensure thorough protection of keys and resistance to side-channel attack.

System security

With well-defined firmware architecture design giving priority to security, the system operates in a secure environment where sensitive data are thoroughly protected during operation and at rest.

Crypto service and performance

With symmetric and asymmetric cryptographic algorithms, the performance of storage encryption using AES reaches 10MB/s. As cryptocurrency is gaining more and more popularity, EdDSA is also adopted to support digital signature.



Use cases

Network authentication

The mechanism built for μSD/X can be used for firmware OTA (over-the-air) upgrade, parameter update, device management and other applications. It provides end devices with cryptographic services, featuring public key certificates or private key verification to mitigate risks of counterfeit or hijacking.

Data storage encryption

μSD/X enables flexible space usage, allowing users to set open areas and encrypted areas. Only when authentication succeeds are data inside encrypted areas accessible. Customizable hardware cryptographic engines are adopted for disk encryption, ensuring optimal encryption service. Some competitive products are vulnerable to cyberattack due to software-based security design. Still some are equipped with hardware-based security design but deficient in performance, failing to satisfy the need for smooth data operation. μSD/X resolves the dilemma by accelerating storage encryption based on hardware-based security, intensely protecting users' digital assets without compromising performance.

End-to-end secure communication

μSD/X's feasibility enables high-speed data encryption. Its protocol can also be tailored for private messengers such as Telegram and Signal in order to meet users' communicative security requirements. In software-based secure communication exist risks and vulnerabilities while the hardware-based one built inside μSD/X strengthens the client side's resistance to spoofing or tampering attacks. To make the solution more user-friendly and accessible, ***software development kits* (*SDK*)** are available for Telegram and other applications. Onto every platform and device can it be deployed with easy adjustment, saving considerable time and operation cost.

Cryptocurrencies' private key protection

μSD/X protects cryptocurrencies' private keys and operates digital signature for transaction. Inserted into a mobile device, μSD/X makes it function as a cold wallet, enabling users to transact without physical tokens in the form of cards or USB. As to security level, it is equipped with a CC EAL 5+ certified secure element, effectively resisting side-channel attack and reverse engineering.

Security and Cryptographic Features

Supported Algorithms

- Message digest：SHA-2, SHA-3, HMAC
- RSA 2048
- ECC with prime-field curves (up to 521 bits) and Edward curve
- ECC protocols：ECDSA, EdDSA, ECIES, ECMQV, ECDH
- AES 256 with modes：ECB, CBC, OFB, GCM, XTS
- Random number generator：AIS-31 (class PTG2) certified TRNG with NIST SP800-90A Hash-DRBG
- Customizable crypto-engine for ECC and AES

Application Protocols

- Cryptocurrency：BIP32, BIP39, BIP44
- Authentication：Fido U2F

APIs

- PKCS#11
- Android Key Store Provider
- Native API

Hardware Specification

Standards

- Fully compliant with SD3.0 (UHS-I) and SD2.0 specifications
- Fit micro SD card dimension
- Capacity：8/16/32GB

Power Consumption

- Working mode：160mA
- Idle mode：85mA~90mA
- Sleep mode：20mA~25mA

Temperature

- Storage temperature：-40°C ~ 125°C
- Operation temperature：0 °C~ 70°C

Flexible customization, speedy deployment

> *Flexible hardware structure design of µSD/X enables implementation of any algorithm and customization of standard ones, followed by efficient deployment in your systems without extra hardware refinement. We also provide professional service to help customers build their own asymmetric curves, hardware cryptographic engines, hardware accelerators for µSD/X. Faced with the era of quantum computing, we devote ourselves to post-quantum cryptography (PQC), applying cutting-edge techniques to µSD/X, expecting to meet customers' long-term security requirements.*

In hardware-based security lies the core belief of WiSECURE Technologies. Focusing our solutions on the new economic era (the Fourth Industrial Revolution), we protect users' precious yet vulnerable digital assets through hardware security modules, mitigating the threat posed by malicious attack or data corruption.

wisecure Technologies