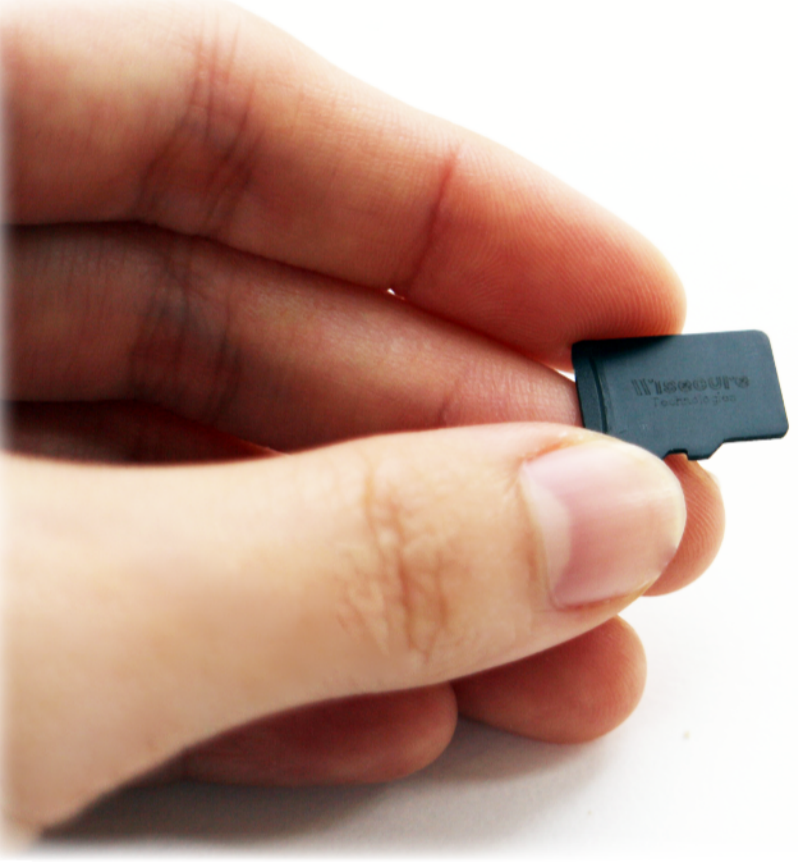
wisecuretech

VeloCrypt™ MicroSD HSM
SA Series

Features
Use cases
Security and cryptographic features
Hardware specification



high-speed encryption
optimizing secure communication

> *Typical HSMs (hardware security modules) come in the form of a PCIe card or a LAN box, used in PKI environments and mission-critical infrastructures for cryptographic operations and digital key protection. The module is mostly applied to servers, not available for mobile devices or end-to-end environments.*

VeloCrypt™ MicroSD HSM - SA Series 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, key life cycle management, digital signature and authentication. The groundbreaking design accelerates storage encryption reaching 7MB/s.

Features

Interface compatibility

With the SDIO (secure digital input/output) interface and common access modes, SA Series is purpose-built for mobile devices.

Storage encryption

Considering invasive attack unearthing information stored in the memory, SA Series enables at least 8GB up to 32GB encrypted data at rest, the access to which requires mandatory authentication underpinned by the secure channel resistant to overhearing and tampering.

Physical security

Robust internal circuit design, CC EAL 5+ certified components commensurate with military-grade security and cutting-edge countermeasures against passive attacks ensure holistic key storage.

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 in transit and at rest.

Crypto service and performance

The performance of storage encryption using AES reaches 10MB/s. As cryptocurrency is gaining popularity, SA Series supports blockchain applications.

Use cases

Network authentication

SA Series empowers the PKI system fulfilling secure OTA (over-the-air) upgrade, parameter update, device management, etc. Built with public key certificates and private key verification, SA Series enables mitigation of risks concerning counterfeit and hijacking.

Data storage encryption

SA Series features adjustable space allocation, allowing users to set unencrypted and encrypted areas. Access to the encrypted area requires mandatory authentication. Considering cryptographic processing that introduces latency, SA Series accelerates data decryption with purpose-built crypto engines, protecting users' digital assets without compromising performance. The feature is applicable to healthcare systems, industrial smart machines, production facilities, mobile devices, payment systems, etc.

End-to-end secure communication

SA Series is a "blade and chassis" platform for makers or developers. With software development kit (SDK), they can devise a new application or integrate an existing one leveraging the military-grade, hardware-based secure key storage. Having integrated the private messaging tool, Signal, for our customer, we ensure increased privacy strength lying in key storage.

Cryptocurrencies' key protection

As digital assets increase, so too will the need to manage private keys in isolation and against hardware attack. Designed for cryptocurrency transaction, SA Series provides military-grade key storage with CC EAL 5+ certification and cryptographic services required for the scenario, such as ECDSA, EdDSA, hashing, etc.

Security and Cryptographic Features

Supported Algorithms

- Message digest：SHA-2, SHA-3, HMAC
- RSA 2048, 4096
- ECC with prime-field curves (up to 521 bits) and Edward curve
- ECC protocols：ECDSA, ECDH
- AES modes：ECB, CBC
- Random number generation：AIS-31 (class PTG2) certified TRNG with NIST SP800-90A Hash-DRBG

APIs

- PKCS#11
- Native API

Compliance

- Module: CC EAL 4+ (ongoing)
- Security chip: CC EAL 5

Hardware Specification

Standards

- Fully compliant with SD3.0 (UHS-I) and SD2.0 specifications
- Fit micro SD card dimension
- MLC NAND Flash/ SLC NAND Flash
- Capacity：512MB/8GB/32GB

Power Consumption

- Working mode : 160mA ± 35mA
- Idle mode : 80mA ± 15mA
- Sleep mode : 23mA± 5mA

Temperature

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

Firm, fit, fast
Bulky vault at your fingertips

> *VeloCrypt™ MicroSD HSM - SA Series is intended for a wide range of use case applications concerning protection of digitized bits, enabling client-side high-performance data encryption in transit and at rest, digital rights management (DRM), transaction verification, etc. Both developers and nontechnical users can easily perform cryptographic operations without additional configuration.*

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.