Wisecure
Technologies

VeloCrypt™ MicroSD HSM

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 LAN-based card or a PC Ie card, used in PKI environments and mission-critical infrastructures for cryptographic functions and digital key protection. The module is mostly applied to servers, not available for mobile devices or end-to-end environments.

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

Features

Features

1. Interface compatibility

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

2. Storage encryption

Considering invasive attack unearthing information stored in the memory, VeloCrypt™ MicroSD 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.

3. Physical security

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

4. 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 intransit and at rest.

5. Crypto service and performance

The performance of encryption using AES reaches 7MB/s. As cryptocurrency is gaining popularity, VeloCrypt™ MicroSD supports blockchain applications.

Use cases

Network authentication

The mechanism built for VeloCrypt™ MicroSD is applicable to firmware OTA (over-the-air) upgrade, parameter update, device management and other applications. It enables cryptographic service on end devices, featuring public key certificates or private key verification to mitigate risks of counterfeit or hijacking.

Data storage encryption

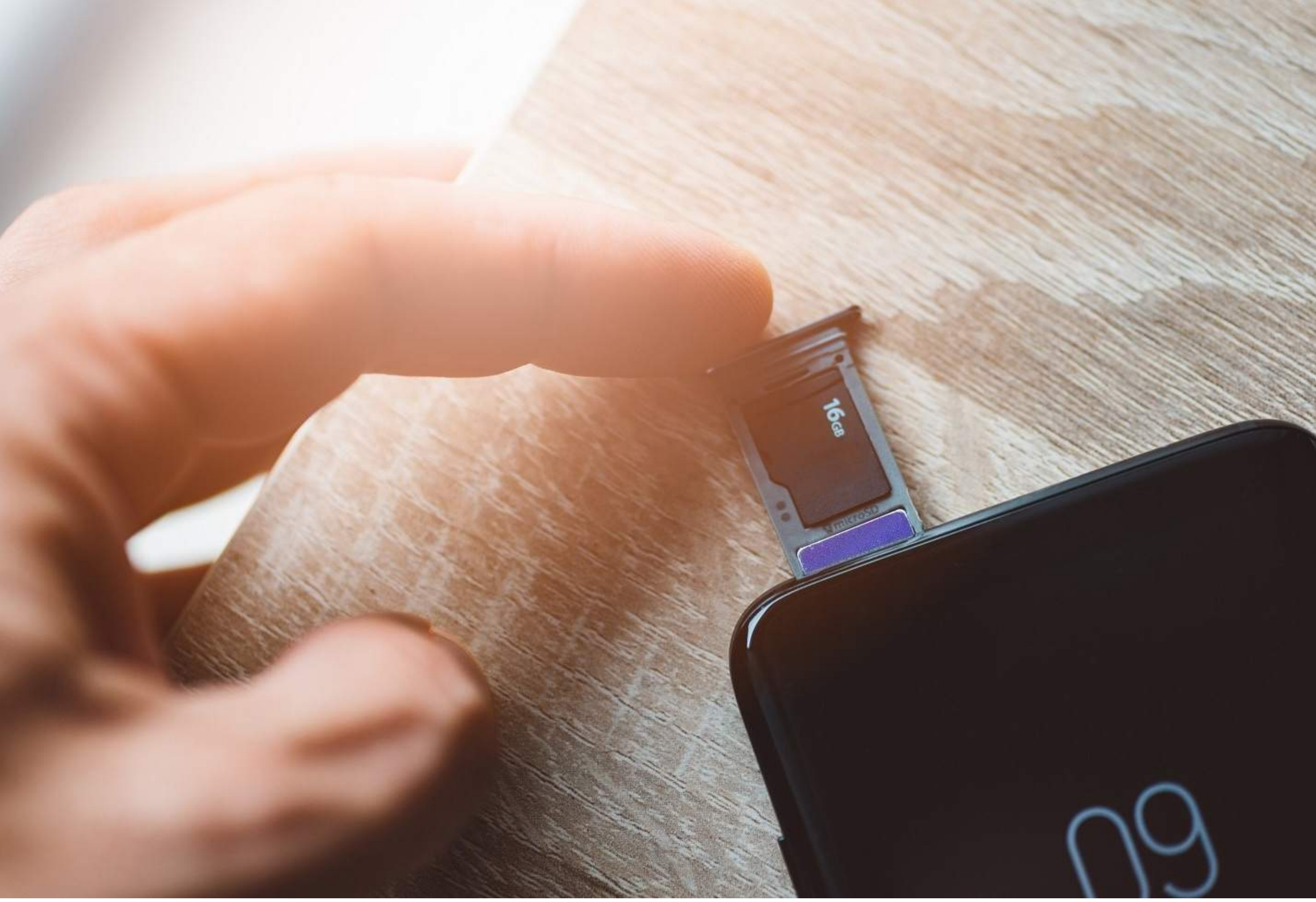
VeloCrypt™ MicroSD features adjustable space allocation, allowing users to set unencrypted and encrypted areas. Access to the encrypted area requires mandatory authentication. Considering cryptographic processing that introduces latency, VeloCrypt™ MicroSD accelerates data decryption with purpose-built 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

VeloCrypt™ MicroSD provides a flexible platform. With software development kit (SDK), developers 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, VeloCrypt™ MicroSD provides military-grade key storage with CC EAL 5 + certification and purpose-built cryptographic services, such as ECDSA, EdDSA, etc.



Security and cryptographic feature

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, EdDSA, ECIES, ECMQV, ECDH
- AES 256 with modes：ECB, CBC, OFB, GCM, XTS, CTR, CFB
- 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

API

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

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 ± 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 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.

On the other hand, the flexible hardware structure design of VeloCrypt™ MicroSD 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 VeloCrypt™ MicroSD. Faced with the era of quantum computing, we devote ourselves to post-quantum cryptography (PQC), applying cutting-edge techniques to VeloCrypt™ MicroSD, 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