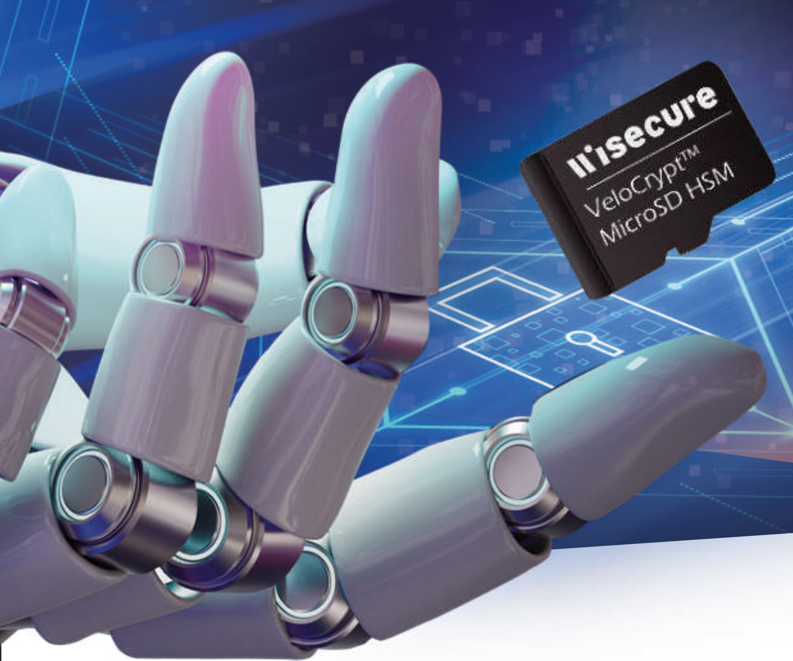
wisecuretech



VeloCrypt® MicroSD HSM

High-Speed encryption
optimizing secure communication

Typical HSMs (hardware security modules) come in the form of a LAN-based card or a PCle 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.
VeloCrypte 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 high-speed data encryption storage, key generation, lifecycle management, digital signature, authentication and other cryptographic functions. Leveraging these advanced capabilities, VeloCrypt MicroSD HSM empowers customers to seamlessly integrate secure authentication, secure boot, encrypted storage of confidential data, and protected communications. Designed to meet the rising security demands of emerging applications, it provides a robust foundation that ensures business operations remain secure, efficient, and resilient.

Interface Compatibility

With an SDIO (Secure Digital Input/Output) interface and a common access mode, it seamlessly integrates with a wide range of embedded systems and devices.
This significantly reduces hardware design complexity and software development time, accelerating the product development lifecycle and helping businesses bring their products to market faster.

Crypto Service and Performance

Equipped with a variety of standard encryption algorithms to meet the security requirements across different industries. With AES encryption storage speeds of up to 10MB/s, it provides outstanding security and high-performance computing, ensuring a strong and resilient defense.

Storage Encryption

Supporting encryption of data-at-rest, providing encrypted storage ranging from 512MB to 32GB, with access controlled through strong authentication mechanisms.

Physical Security

Combining Common Criteria EAL 5+ certified security chips with advanced internal circuit design, it effectively safeguards against hardware attacks (such as side-channel attacks) and implements advanced, military-grade key protection strategies.

System Security

With a security-driven firmware architecture, the system ensures robust protection of sensitive data and keys, whether stored at rest or in transit.

WiSECURE Inc.
15F, CIC Tokyo, Toranomon Hills Business Tower, 1-17-1
Toranomon, Minato-ku, Tokyo 105-6490, Japan

https://wisecure-tech.jp

Secure Boot

VeloCrypt® SA Series delivers hardware-based Root of Trust (RoT) security, featuring tamper resistance and high-level certifications to safeguard device keys. It ensures boot integrity by allowing only trusted firmware and operating systems to run, effectively preventing malware injection and mitigating the risk of botnet hijacking. From startup to operation, it maintains a continuously trusted environment.

FIDO Device OnBoard (FDO)

VeloCrypt® SA Series integrates with the kvFDO service solution, enabling seamless deployment on existing IoT devices. Leveraging the FDO standard protocol, it connects to enterprise SaaS device management systems for fast and automated provisioning. This enhances operational efficiency and ensures comprehensive device lifecycle management.

Data Storage Encryption

VeloCrypt® SA Series combines high-speed encrypted storage with military-grade security provided by a dedicated security chip. Its configurable encryption and decryption partitions provide robust data security and seamless performance across diverse applications, ensuring the protection of critical digital assets in connected devices.

End-to-End Secure Communication

VeloCrypt® SA Series is built on hardware-based protection and offers a Software Development Kit (SDK) to assist device manufacturers in integrating existing applications. This ensures secure data transmission across various protocols, enhancing the device's ability to resist eavesdropping and tampering.

PRODUCT SPECIFICATIONS

Appearance：SD card | Capacity：512 Mbytes / 8 GBytes / 16GBytes / 32 GBytes

Flash Type：SLC / MLC NAND flash

Temperature：Operating Temperature：-0°C to 70°C | Storage Temperature：-40°C to 125°C

Electrical：Operating Voltage：2.7V ~ 3.6V | Power Consumption：160 mA±35mA

Hardware Features :

- Compliant with SD Default speed / SD High speed / SD UHS-I
- With a CC EAL 5+ security chips
- Certificate：CE / FCC / VCCI / BSMI
- API：PKCS#11 / Native API

Supported Algorithms :

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