WiSECURETECH

KEYVAULT

FIPS 140-2 validated
Certificate #4409

KeyVault Hardware Security Module

Fulfilling applications with agility and flexibility

KeyVault Hardware Security Module (kvHSM), as the name implies, is a physical device, a vault that stores and manages cryptographic keys. It is a powerful and invincible box. When its flesh acts like a shield, the womb brings cryptographic keys to life; it governs the entire life cycle of keys, including generation, distribution, storage, destruction and archiving, and its spirit inside drives these keys to fulfill encryption, decryption, signing, verification.

kvHSM provides a robust environment for cryptographic operations. It is designed in reaction to compromising, physical intrusion, tampering, etc. The military-grade secure element, with CC EAL 5+ certification, mitigates risks of key leakage and dismisses the threat posed by side channel attack (SCA).

Cryptocurrency Exchange Key Management & Shopping Mall Key Management (Cryptocurrency)

Cryptocurrency transactions have taken the world by storm. Securely storing one's private key used for signing is the least frivolous matter to consider. For the exchange and shopping malls, money stored across multiple accounts engenders the need for robust key management, which concerns not only security but also availability and cost efficiency; they should not maintain the quality of service at the expense of security.

kvHSM provides a highly customizable platform, leaving room for flexible application design. It manages the entire life cycle of private keys, including generation, distribution, storage, destruction and archiving, and the core engine executes encryption, decryption, signing, verification and hashing for cryptocurrency transactions.

It also strikes a commensurate balance between security and performance; the performance of digital signature can reach 10,000 times per second, yet the process of which complies with military-grade security level. Furthermore, kvHSM can detect physical intrusion and activate countermeasures in response; side-channel attack, reverse engineering, tampering are within the scope of data protection.

Supported Algorithms

- Hashing: SHA-2, SHA-3, HMAC
- RSA 2048
- ECC with prime-field curves (up to 521 bits) and Edward curve
- ECC Protocols: ECDSA, ECIES, ECDH, EdDSA (FIPS186-5)
- AES 256 with modes: ECB, CBC, CFB, OFB, GCM, XTS
- Random: AIS-31 (class PTG2) certified TRNG with NIST SP800-90A Hash-DRBG
- FPGA-based customizable crypto-engine for ECC and AES

Performance

- AES (256 bits XTS mode) data encryption/decryption up to 1.6GB/s
- ECDSA (256 bits) up to 10,000 tps

Certificates and Compliance

- FIPS 140-2 Level 3
- CAVP: AES (ECB, CBC, CFB, OFB, GCM, XTS), ECDSA, HMAC, DRBG, SHA-2, SHA-3
- CE/FCC

*The actual order specifications will be based on customer's requirements.

Authentication Server (IoT Ecosystem) & Cloud Crypto Service

Internet of Things (IoT) ecosystem comprises a data center (public or private cloud), gateways (intermediary communication gateways), and endpoint devices (distributed IoT devices). As a proverb goes that security is only as strong as your weakest link, three levels mentioned above should be paid equal attention.

As to the data center, it receives collected data communicated by gateways, in the path of which lies two conspicuous risks, eavesdropping and tampering; hackers may intercept messages or gain unauthorized access to the cloud. In this regard, data encryption prior to communication and authentication are integral to secure and sustainable operation.

Supported Middleware

- △ PKCS#11
- △ Native API

Physical Security

- △ SPA/DPA Countermeasures
- △ CC EAL 5+ Security Chip
- △ Tamper Response

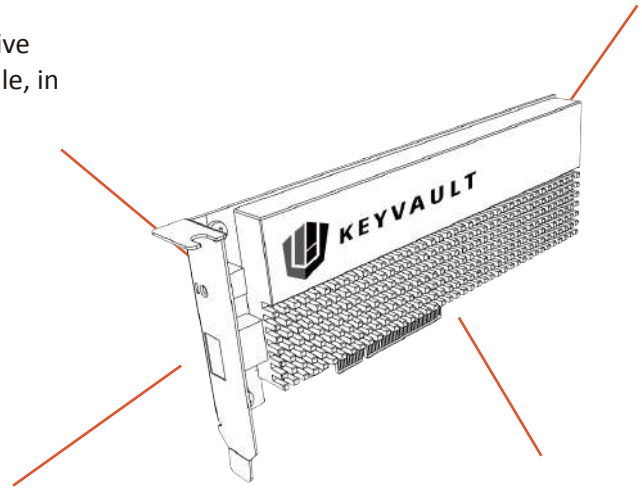
Embedded onto the cloud in the form of PCIe cards, kvHSMs' services include AES encryption, ECC-based signature/verification and key establishment, and SHA2, SHA3 hash calculation, for data protection, identification, and blockchain respectively. It also serves as the certificate authority, signing certificates for authorized devices, manages firmware update and master keys' life cycle.

Data Clearance Button

The button activates sensitive data clearance in the module, in case of any emergency.

Data Protection Shell

Once physical intrusion occurs or the shell is destroyed, the sensitive data will automatically be erased.



Cryptographic Accelerator

The accelerator enhances the performance of cryptographic operation; the speed of digital signature can reach up to 10,000 times per second; the speed of encryption exceeds 1.6GB/s.

Security Chip

The security chip embedded in the module complies with CC EAL 5+, which is tantamount to military-grade security level. Its sophisticated design precludes the possibility of side-channel attack and reverse engineering.

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