Code Signing with the KMES Series 3

The KMES Series 3 is a FIPS 140-2 Level 3-validated solution used to centralize the storage and management of digital signing certificates for secure code signing by globally dispersed development teams. Our turnkey code signing solution seamlessly integrates with popular code management and automation technologies, including Java Jar Signer, Microsoft Authenticode, Jenkins, and other popular code development platforms.

**Digital signing platform for secure code signing and certificate management**

The KMES Series 3 is a FIPS 140-2 Level 3-validated solution used to centralize the storage and management of digital signing certificates for secure code signing by globally dispersed development teams. Our turnkey code signing solution seamlessly integrates with popular code management and automation technologies, including Java Jar Signer, Microsoft Authenticode, Jenkins, and other popular code development platforms.

---

**Code Signing with KMES Series 3**

- FIPS 140-2 Level 3-validated HSM
- Cryptographically sign firmware and software for IoT device security
- Reliably access certificates and digitally sign code on-demand
- Store millions of keys and certificates
- Supports standards-based libraries PKCS#11, Java, and CNG

**More Than Code Signing**

The KMES is an all-in-one versatile management platform capable of executing a wide variety of cryptographic techniques including key management, data protection, and digital signing.

- Generate, manage, and track all keys and certificates to maintain a public key infrastructure
- Enhance database security by devaluing data-at-rest using Vaultless Tokenization
- Blockchain-based timestamping, message and document signing
Secure Code Signing with KMES Series 3

Generate keys, store certificates, and manage the full code signing workflow.

Integration with Microsoft Authenticode

- Guarantee integrity of Microsoft Authenticode certificates
- Transmit logs for internal or external audits
- Utilize SignTool, CertMgr, and MakeCert Crypto APIs

Integration with Java JarSigner

- Supports Java signature and other unstructured signatures
- Use JarSigner to secure JAR files preventing unauthorized access to Java class files
- Generate keys & export certificates with Java Keytool

Functionality & interfaces

Supported key types & algorithms:

3DES, RSA, AES, ECC, SHA-1, SHA-2, DSA, and HMAC

Interfaces:

Encrypt API, Java JCA/JCE, PKCS #11, and MS CAPI/CNG

Industry Compliance Standards

- FIPS 140-2 Level 3 Validated
- PCI HSM 2.X
- FCC Part 15 - Class B