KMES SERIES 3

Key Management Enterprise Server

Enterprise-Class Key & Certificate Management Platform

Lifecycle Management, Robust User Permissions, and Full Automation Capabilities

The Key Management Enterprise Server (KMES) Series 3 is a scalable, versatile, and secure solution for managing large volumes of keys, certificates, and other cryptographic objects. Built around Futurex's proven cryptographic technology, the KMES's modular system architecture provides a custom solution to fulfill the unique needs of organizations across a wide range of industries. Full integration with Futurex's Hardened Enterprise Security Platform enables the KMES to offer unparalleled functionality expansion options alongside management of the entire Public Key Infrastructure (PKI) for the platform.

The KMES' key and certificate lifecycle management capabilities enable organizations to establish a secure PKI without foregoing manageability. A single-device PKI platform, it doubles as a certificate authority (CA) and registration authority (RA), as well as offering a wide range of expansion capabilities.

Enterprise Automation Capabilities

As an enterprise-class product, the KMES's has the ability to manage very large quantities of keys, certificates, and other such objects, and sensible automation means the process is unencumbered.

Define automatic expiration rules, for example, to remove and replace keys of all major types, algorithms, and protocols on a user-defined schedule, without need of travel to the data center. Meanwhile organizations can set automatic alerts, so they're always informed about the status of their key and certificate infrastructure.

Next-Generation Features

- FULL KEY AND CERTIFICATE LIFECYCLE MANAGEMENT
- ENTERPRISE CERTIFICATE AND REGISTRATION AUTHORITY
- TURNKEY APPLICATION ENCRYPTION
- REMOTE KEY MANAGEMENT FOR ATM AND POINT OF SALE
- ROBUST USER AND GROUP PERMISSION SYSTEM
- VAULTLESS TOKENIZATION

Versatile Functionality

- Supports mutual authentication under a trusted root certificate performed by either an existing CA or through a service provided by Futurex to establish a trusted PKI among all infrastructure components
- Capable of generating and managing self-signed certificates necessary to establish a trusted PKI
- Simplify the object management process through custom, user-defined attributes and key group format cloning for replication of data structures

EMV Certificate Authority

- All major card brands supported
- Supports EMVCo-compliant self-signed issuer certificate creation

Industry Compliance Standards

- FIPS 140-2 Level 3 compliant
- ANSI X9.24 Part 1 and Part 2—TR-39
- PCI HSM

Product Overview: KMES Series 3

Hardened, Enterprise-Class Key & Certificate Management Platform

- Key and certificate lifecycle management and establishment of an organized public key infrastructure
- Custom, user-defined attributes and key group format cloning for replication of data structures
- Support of tens of millions of cryptographic objects
- Functionality available for ATM and Point of Sale remote key loading

Enterprise Application Encryption and Data Protection

- FIPS compliant security for application-based data protection
- Centrally manage the full key, certificate, and policy lifecycle
- Easy-to-use architecture simplifies and expedites deployment
- Segregated key containers, enabling the creation of a single cryptographic resource pool for multiple independent applications
- Web-based workflow management for automation of key lifecycle tasks
- Standards-based libraries for easy integration: KMIP, C# .NET, Java

Unified Cryptographic Platform

- Full Certificate Authority (CA) and Registration Authority (RA) lifecycle management, consolidated within a single platform
- Designed for turnkey implementation
- Customized audit reports and activity logging

Scalable Integration

- Nth degree scalability with multiple KMES devices
- Automatic synchronization of keys, certificates, and other objects between connected Hardened Enterprise Security Platform devices
- Masterless Peering enables high availability architecture

Enterprise Certificate Authority Features

- Virtually limitless scalability of certificate authorities
- Supports both CRL, OCSP, and SCEP for certificate status management
- Extended validation certificates

Registration Authority Features

- Web-based RA allows for certificate signing requests to be submitted by users and validated by an authentication user group
- Automated e-mail templates for workflow management
- Custom white labeling for registration authority portal
- Integration with LDAP for auto-enrollment

Quantum-Safe Hybrid Certificate Authority Solution

- Simultaneously sign with classical and quantum-safe algorithms, eliminating the need to migrate from current system
- Mitigates the inevitable quantum computing risk

FUTUREX.COM

ENGINEERING CAMPUS / 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF/ (800) 251-5112 P/ +1 (830) 980-9782 info@futurex.com

Product Specifications

Supported Cryptographic Algorithms

Symmetric
- 3DES
- AES (128 to 256-bit)
- CBC, CFB, CFB1, CFB8, CFB64, CFB128, ECB, GCM, OFB
- CMAC
- HMAC (up to 256-bit)

Hashing: Available as a raw hash functions or in conjunction with other symmetric and asymmetric functions
- SHA (2, 256, 384, 512-bit)

Asymmetric
- RSA (512 to 8192-bit)
- DSA (512 to 4096-bit)
- Elliptic curve
  - NIST standard P Curve (192, 224, 256, 384, 521-bit)
  - Brainpool (160 to 512-bit)
  - Ed25519
- ECDSA
- ECIES
- Quantum-safe algorithms
- Padding methods
  - PKCS #1.5
  - OAEP
  - PSS
  - X9.31

Key and Certificate Data Structures
- X.509
- PKCS #1 (for public keys)
- PKCS #7, #8, #11, #12
- Java KeyStore
- TR-31, TR-34

Key Derivation Methods
- DUKPT
- SP800-108 / KBKDFVS
- ECDH

Tokenization Methods (Format Preserving)
- FF3.1

TLS Methods (Using RSA or ECC Ciphers)
- 1.0, 1.1, 1.2, 1.3

Physical and Operating Specifications

Weight: 40.5 lbs (18.4 kg)
Width: 19 inches (48.3 cm)
Height: 2U - 3.47 inches (8.81 cm)
Depth: 22.3 inches (56.7 cm)
Power: 100 - 240 VAC 50/60 Hz. 225 Watts
Operating temp: -40° to 140°F (-40° to 60°C)
Storage temp: -40° to 140°F (-40° to 60°C)
Operating relative humidity: 20% to 80%
Storage relative humidity: 5% to 95%