Tricryption® kS

High Speed, High Volume Centralized Symmetric Key Management Services

Data Sheet : Symmetric Key Management

Tricryption® kS preforms symmetric key generation, key storage and retrieval, key authorization, and auditing of key usage. Encryption keys are separated from the data and stored centrally.

Tricryption kS employs industry standard symmetric encryption keys to allow for real-time revocation and data ownership by the enterprise.

Benefits

- **Key Ownership -** All encryption keys are managed by the software and owned by the enterprise.
- **Key Revocation -** Keys are revoked in real-time. Thereby revoking access to all copies of the encrypted data, no matter the location of the data.
- **Centralized Key Storage -** Unified, cross-application, enterprise-wide, centralized key management with tracking.
- **High Speed / High Volume -** Supports trillions of encryption keys, connection and thread pooling.
- **Logging Key Usage -** All key access is logged which allows monitoring of encrypted data use.

Cloud-Ready

Elastic and Scalable
Horizontally and vertically to handle increased demand.

- Stateless design
- Supports multitenancy

Hypervisor Support
Tricryption kS is supported in virtual environments.

Key Storage in RDBMS
Supports current installation base. Uses backup and failover methods already familiar to enterprises.

Secure Communication
Secure TLS/SSL communications for all key exchange and server management.

Multi-OS Support
Supports multiple operating system platforms.

Multiple Instance Support
Run multiple instances of Tricryption kS for integration, failover and enterprise architecture and cloud flexibility.

Enterprise Trust
Expandable to match multi-partner collaboration & business processes while controlling key ownership.

Central Policy Management
Manage user encryption policies from a single point.

- Directory Services Support
- Certificate Users Support
- User Group Support
- User Roles
- ACL Templates
- KMIP Compliant

Certified and Validated

- Uses Industry and Government Standard Cryptographic Algorithms
- FIPS 140-2 Level 1 – 3 Compliant
- Common Criteria CC EAL2+

System Protector Security
Hardware security module and token support provides for a high level of security for entire system and encrypted data.

Crypto Module Support

ERUCES Tricryption cryptographic module (FIPS validated). Third party hardware security module support.

HSM supported:

- Safenet® Luna
- Thales® nCipher nShield [FIPS 140-2 Level 2/3]

Algorithms Supported

- AES (256 bits, 196 bits, 128 bits)
- Triple DES

System Protector Security

- Password (PKCS5)
- HSM (Safenet Luna or Thales nCipher nShield)
- K of M Secure Tokens
- Joint Authorized Initiators (Smartcards)
- Microsoft® Windows Protector

Hardware Requirements

Minimum (x86)

Processor	1 (GHz)
RAM	1 GB
Hard Disk Space	512 MB

Recommended (x64)

Processor	Dual-Core Pentium® 4, 2 GHz or greater
RAM	2 GB
Hard Disk Space	2 GB

Operating System Support

- Windows® XP Professional SP3
- Windows 2003 Server
- Windows 2008 Server
- Windows 7
- Solaris® 9
- Solaris 10
- Linux Kernel 2.6

Software Requirements for Infrastructure

Databases supported for encryption key storage:

- IBM® DB2
- Microsoft SQL Server
- Oracle®
- PostgreSQL®
- Sybase® ASE

Hypervisors Supported

VMWare® VSphere ESXi, Microsoft hyper-v, Xen, KVM, Vcenter and Oracle VirtualBox.

Visit our website
http://www.eruces.com

To speak with a Product Specialist
Call 913.310.0888 or email moreinfo@eruces.com

ERUCES Headquarters
11142 Thompson Ave
Lenexa, KS 66319-2301 USA
+1 (913) 310 0888

01.64.004 11/11

Secure Data Anywhere.™