CryptoBind®
Data Security  Server
Key Management Solution
Data Security Server provides built-in HSM with encryption and tokenization solutions. It enables organizations to neutralize the data breach impact for data at rest, in motion and in use by de-identifying sensitive information.

Data Security Server enables advanced format-preserving encryption, secure Stateless tokenization, and stateless key management to protect enterprise applications, data processing infrastructure, Data Encryption API etc.

Data Security Server provides built-in HSM with encryption and tokenization solutions. It enables organizations to neutralize the data breach impact for data at rest, in motion and in use by de-identifying sensitive information. Data Security Server solves the industry's biggest challenge by simplifying data protection across complex legacy and modern IT.
Enhance your data security with CryptoBind® Data Security Server

Model Information:

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Performance</th>
<th>Concurrent Key Usage</th>
<th>Key storage in Appliance</th>
<th>Key storage Upgradable in Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA1000</td>
<td>1000</td>
<td>1G &amp;/or 10 G Fiber</td>
<td>10,000 Keys</td>
<td>1,00,000 Keys</td>
</tr>
<tr>
<td>DSA5000</td>
<td>5000</td>
<td>1G &amp;/or 10 G Fiber</td>
<td>5,000 Keys</td>
<td>5,00,000 Keys</td>
</tr>
<tr>
<td>DSA2000</td>
<td>2000</td>
<td>1G &amp;/or 10 G Fiber</td>
<td>2,000 Keys</td>
<td>10,000 Keys</td>
</tr>
<tr>
<td>DSA100</td>
<td>1000</td>
<td>1G &amp;/or 10 G Fiber</td>
<td>1000 Keys</td>
<td>10,000 Keys</td>
</tr>
<tr>
<td>DSA500</td>
<td>500</td>
<td>1G &amp;/or 10 G Fiber</td>
<td>500 Keys</td>
<td>10,000 Keys</td>
</tr>
</tbody>
</table>

Types of data to protect can include:

- Credit card and other payment card numbers
- Bank account numbers, Tax File Numbers
- Post codes and IP codes
- Currency amounts, salaries, bank account amounts, transaction amounts
- Phone numbers, mobiles and landlines
- Dates, birth dates, join dates
Social security, national security and Medicare account numbers

Names — surnames, first names, street names, suburbs

Identification numbers — driver’s license and passport numbers

**Supported Environment:**

Operating Systems: Windows, RHEL, CentOS, Ubuntu, Suse Linux, Linux, Unix, HP UX, IBM AIX

The virtual appliance is available in VMware, HyperV, KVM and Azure compatible formats.

Application Middleware Support: IIS, JBOSS, Oracle, IBM, Nginx, Apache, WSO2

Hardware Acceleration: Intel AES-NI and IBM POWER8

Database Support: MSSQL, MySQL, Oracle, DB2, MongoDB, Maria DB, PostgreSQL

Container: Docker, Red Hat OpenShift

**Hardware Specifications:**

### Physical specifications network appliance

- **Height**: 89 mm
- **Width**: 437 mm
- **Depth**: 647 mm
- **Weight**: 23.59 kg
- **Packaging** (W x H x L): 678 mm x 290 mm x 876 mm

#### Power Supply

- **Certified Hot Swappable Power Supply**
- **Power Efficiency**: 94%
- **Output and Input**: 400W/550W/740W with Input 100 - 240Vac
- **AC Input Freq.**: 50 - 60Hz
- **Power Distributor**: O/P: 12V/75A, +5V Max: 30A, +3.3V Max: 24A, -12V Max: 0.6A
- **Mean Time Between Failure**: 1,83,421 hours

#### Operating Environment / Compliance

- **Operating temperature**: +10°C to +35°C (+50°F to +95°F)
- **Storage temperature**: -10°C to +55°C (+14°F to +131°F)
- **Relative humidity**: 10% to 95% non-condensing

#### Network Interface

- **Dual network Interface of 1 G port** &/or **Dual network Interface of 10 G Optical Fiber port**

#### Compliance

- **RoHS, UL, CE, BIS Compliant**
- **FIPS 140-2 level 3 Certified Cryptographic boundary** — Applicable for physical appliance for Crypto operation and Key generation
Technical Specification:

Two Factor Authentication
API Support PKCS#11, MSCAPI, MSCNG, SOAP, REST, KMIP, .NET
Supports Users and groups from LDAP, local systems, Hadoop and container environments
Network Management SNMP (v1, v2 & v3), NTP, Syslog-TCP
SIEM integration for log analysis and monitoring
Multi-tenancy support
Supports Clustering & High availability using Agents, also supports HA with external hardware or software Load Balancer
Management portal for Complete life cycle management of Cryptographic keys including Creation, Deletion, Archival, Usage and Permissions of Cryptographic keys
Separation of duties and policies
Administrative Interfaces Secure Web, SOAP, CLI, REST
Security Authentication Username/Password, RSA multi-factor authentication (optional)
Compatible with local user LDAPS, Active Directory etc.
Syslog Formats CEF, LEEF, RFC
vSphere cloud platform support
Device can be configured in High Availability with Active-Active cluster

DSS server configuration

Core: 16 cores
RAM: 32 GB
Internal storage: 1 TB
JISA's KMS is a centralized key management system that delivers automated key updates and distribution to a broad range of applications.

As your company grows, so does your data. Key Management System increase life cycle efficiency and help your departments develop proper key management policies that scale with your organization.

Strong data encryption requires encryption key management. Being able to own and manage your encryption keys is crucial to meet compliance standards.

Benefits of JISA’s KMS:

- Streamlines key management processes
- Cost effective solutions with simple backup and recovery
- System wide key control manages any key type and format
- Automatic key updates and distribution
- Scalable solution
- Provides tamper evident records for compliance
- System wide key control manages any key type and format

Features of JISA’s KMS:

- Encryption Key and certificate life cycle
- Access control for keys and certificate
- Key Manager support for direct application integration
- Flexible integration with HSM
- KMIP agent OS Support: Windows, Linux, HP UX, AIX
- Policy based key and certificate generation
- Able to function as a certificate authority
- Database for storage of keys and key metadata
- KMIP compliant (Version 1.0, 1.1, 1.2, 1.3, 1.4, 2.0)

www.jisasoftech.com

Creating secured ecosystem
Encryption Use-Cases

Encryption is the process of converting information or data into a code, especially to prevent unauthorized access. JISA KMS can be used in many encryption use-cases like TDE, Column Level Encryption etc.

The purpose of data encryption is to protect digital data confidentiality. While data encryption may seem like a daunting and complicated process, JISA’s software handles it reliably every day.

JISA KMS can be used in many encryption use-cases like TDE, Column Level Encryption etc. In most of the scenarios, JISA KMS manages keys leveraging the native encryption offered by different Databases and Applications.

Transparent Data Encryption (TDE)

- Encrypt database files.
- Addresses compliance issues such as PCI DSS which require the protection of data at rest.
- File level encryption.
- Encrypting databases on the hard drive and on backup media.

Column Level Encryption

- Flexibility in encryption of data
- Encryption is possible not just at rest but also in motion and when data is in process
- TDE is possible with this
- Retrieval speed is relatively high

Application Level Encryption

- Potential to simplify the encryption process
- Security at application level to ensure more protection
- Enables to achieve PCI DSS standards
- Data is encrypted before it is written to the database
Storage & Tape Drive Encryption

Flexible Key management (KMIP compliant)  Access control can be enforced

Provides good security and high functionality
Contact Us:
sales@jisasoftech.com  |  connect@jisasoftech.com
Phone: +919619-222-553

JISA Softech Pvt. Ltd.
A-604, Amar Business Zone, Ganraj Chowk, Veerbhadra Nagar, Baner, Pune, Maharashtra 411045

www.jisasoftech.com