JISA®
Creating Secured Ecosystem

JISA Softech Pvt. Ltd. *www.jisasoftech.com*

CryptoBind Data Security Server

Replication, Synchronization and High Availability

Copyright

Disclaimer

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between JISA Softech Pvt. Ltd. and the customer.

However, JISA Softech Pvt. Ltd. has made all reasonable efforts to ensure that the instructions contained in the document are adequate for in-depth description of the product.

JISA Softech Pvt. Ltd. will, if required explain queries related to specific product.

TABLE OF CONTENTS

ABOUT JISA

We are a young Information Technology company providing various Authentication products and Solutions.

All our Public Key Infrastructure (PKI) & Cryptographic solutions are sold under brand name JISA. With strong core competencies in Cryptography and PKI, JISA offers solutions built around Public Key Infrastructure (PKI), the framework that brings confidentiality, authentication, privacy, and non-repudiation.

“JISA has an entire range of software applications based on cryptographic algorithms and protocols”

We at JISA are focused on the design, develop, sales and support of various Hardware and Software solutions. We have done an extensive market research on various requirement of market and included suitable solution in our Solution Portfolio.

JISA India R&D centre situated in Pune, is a core of a team with excellent technicians and think-tankers with the only objective of delivering simple, efficient and powerful device that meets one’s, particularly routine requirements on technological front. It is our endeavour to provide our consumers, a taste of the technology ahead.

INTRODUCTION

We are a young Information Technology company providing various Authentication products and Solutions.

All our Public Key Infrastructure (PKI) & Cryptographic solutions are sold under brandname JISA. With strong core competencies in Cryptography and PKI, JISA offers solutions built around Public Key Infrastructure (PKI), the framework that brings confidentiality, authentication, privacy, and non-repudiation.

“JISA has an entire range of software applications based on cryptographic algorithms and protocols”

We at JISA are focused on the design, develop, sales and support of various Hardware and Software solutions. We have done an extensive market research on various requirement of market and included suitable solution in our Solution Portfolio.

JISA India R&D centre situated in Pune, is a core of a team with excellent technicians and think-tankers with the only objective of delivering simple, efficient and powerful device that meets one’s, particularly routine requirements on technological front. It is our endeavour to provide our consumers, a taste of the technology ahead.

Our solutions include:

- Encryption Solutions
- Aadhaar Data Vault
- Two factor Authentication
- Hardware Security Module
- Asset Management and Tracking Solution
- Fingerprint devices
- Biometric Tablet PC

KEY MANAGEMENT SYSTEM

WHY KEY MANAGEMENT IS NEEDED?

Security of the sensitive data which is protected by cryptography directly depends on the strength of the keys, protocols associated with keys and protection of the keys. Managing an increasing number of cryptographic keys across business applications is evolving as ever more challenging. Inappropriate and poor key management may easily compromise strong algorithms. Keys may be managed manually, but in many cases, an automated system is required to oversee, automate, and secure the key management process. An automated system that performs key management is commonly known as a (cryptographic) key management system. Most business organizations lack encryption key management strategy which consumes their lot of time, it is error prone, costly and security audits become very difficult. The top three challenges of key management are frequently cited as: lack of clear ownership of processes; lack of skilled personnel and the existence of isolated and fragmented systems.

JISA's Key Management Solution (J-KMS) directly addresses all of these. It enforces specific roles and clear responsibilities for sets of keys; it frees staff from manual, repetitive tasks and allows them to concentrate on policy decisions; it can orchestrate the delivery of keys between disparate systems supporting standard key formats.

WHAT IS J-KMS?

J-KMS is a centralized key management system that delivers automated key updates and distribution to a broad range of applications. J-KMS manages the entire lifecycle of all keys (symmetric and asymmetric), supports robust business processes and allows you to confidently comply with and pass internal & external audits. Take control of cryptography and achieve compliance with centralized and automated application key management. J-KMS allows you to stay competitive by improving business efficiency, while reducing costs and risk.

J-KMS comes with Admin UI which is hosted on client's location and this portal will work in sync with HMS & tokenization engine services.

J-KMS BENEFITS

- *Tamper proof records*
  Whenever any organization is handling sensitive data, it needs to meet data protection regulation and comply with various industry standard in order to meet security needs. Compliance needs to be proved with the help of reports. J-KMS provides tamper evident records for proof of compliance. J-KMS also supports centralized management, tamper proof audit logs, encryption, role-based access control, tokenization, and plugins to support data security and privacy requirements. These solutions help organization to meet compliance.
- *Manages Key lifecycle*
  J-KMS manages numerous keys throughout their lifecycle. It helps organization to streamline key management processes, control keys. J-KMS enables system-wide key control to manages any key type and format. It also enables key revocation and deletion for smooth operation.
- *Cost Reduction*
  J-KMS eliminates repetitive tasks, inefficient process, manual work. It reduces human errors and automates processes. It provides centralized management which helps to optimize resources. Reduce time spent on compliance and audits. These opportunities enable organization to reduce their cost.
- *Automate Process*
  J-KMS allows Automatic key updates and rotation to any end-point. It ensures secure key distribution within the processes.
- *Reduce Risk*

J-KMS comes with admin console where admin can set configurations like who should have access, user details, IP whitelisting. This helps to reduces the risk of human errors.

- *Dual control with asynchronous workflows*
- *Simple backup and recovery*

  J-KMS allows simple backup and recovery architecture. In case a key in use is lost due to system failure, backup copy is made available.
- *Maximize efficiency*

  J-KMS comes with Admin UI which makes admin configurations easy and efficient. Automated process also helps to reduce repetitive tasks, errors. With the help of J-KMS, data security can be applied quickly. This helps to maximize staff efficiency and productivity.
- *Strengthen security and compliance*

  J-KMS provide capability to encrypt, mask and tokenize the sensitive data. This makes sure that unauthorized users don't get access to this data. J-KMS provide necessary tamper proof audit logs. J-KMS is compliant with data protection standards like Payment Card Industry Data Security Standard (PCI-DSS), General Data Protection Regulation (GDPR). This strengthens the security and compliance
- *BYOK*

  J-KMS supports cloud security which helps cloud users to use their own encryption software
- *High availability and scalability*

Organization not only need to protect the sensitive data but also protect encryption keys from temporary unavailability, permanent loss, destruction, and accidental or malicious deletion. High availability and high scalability of J-KMS is ensured through clustering of servers, HSMs, increasing the number of cryptographic keys. It provides necessary power supplies, components to guard appliance from loss and destruction.

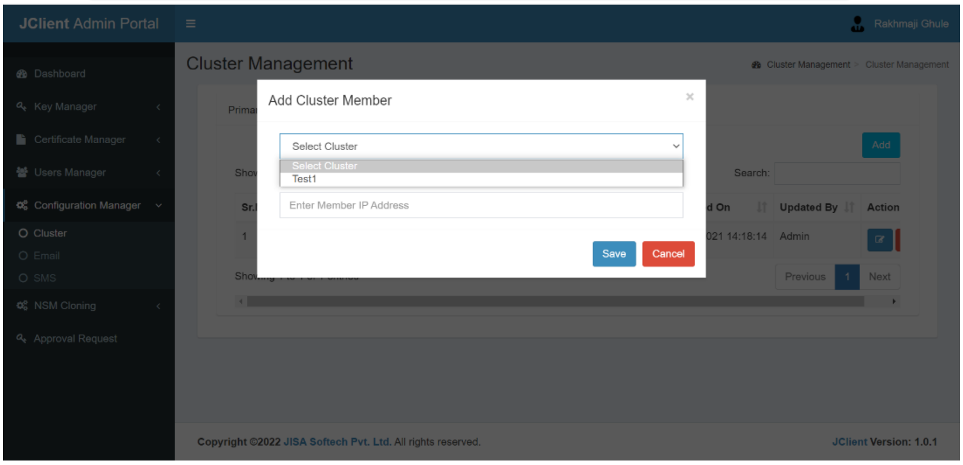
CLUSTER CONFIGURATION

Cluster is created in order to support High Availability. When configured in Cluster, all participating nodes continuously synchronize respective databases with each other.

Members of the cluster must have bi-directional access to each other on port

The Cluster members synchronize key, certificate related data and not all. Data like Backup files, Backup keys, NTP configuration is not considered for synchronization.

In CryptoBind DSS, the replication and synchronization is taken care by proprietary Replication Service. The members i.e. DSS, participating in cluster can be configured on Centralized Admin Portal.



Add Cluster Member

Select Cluster
Select Cluster
Test1

Enter Member IP Address

Sr.	d On	Updated By	Action
1	021 14:18:14	Admin	

Copyright ©2022 JISA Softech Pvt. Ltd. All rights reserved.

JClient Version: 1.0.1

Under Cluster Management, User has to register all members. Cluster member DSS are configured with replication certificates using which the member DSS encrypts-decrypts the replication data.

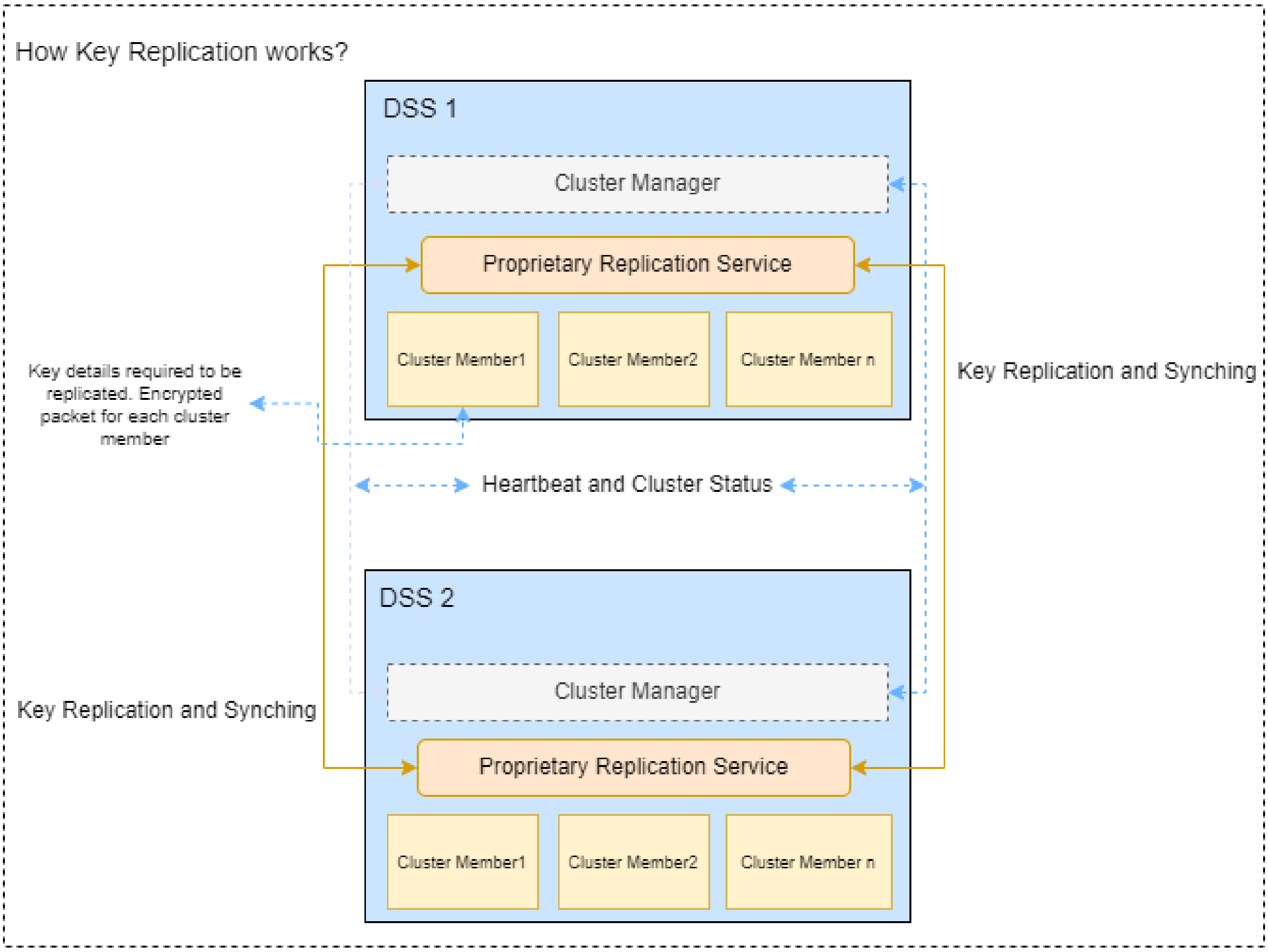
Once cluster members are configured, the cluster Manager running in background in each of the cluster members understands the details of all participating members.

The cluster manager keeps track of all members using some probing packets i.e. heartbeats. If any DSS node is disconnected, an alert message is generated.

Any operations can be performed on any of the members.

HOW REPLICATION WORKS?

Whenever any Key Generation, Key Import or Key Deletion request is performed on any of the cluster member, an encrypted data packet with key details is created for each cluster member is created on that node.


How Key Replication works?
DSS 1
Cluster Manager
Proprietary Replication Service
Cluster Member1
Cluster Member2
Cluster Member n
Key details required to be replicated. Encrypted packet for each cluster member
Key Replication and Synching
Heartbeat and Cluster Status
DSS 2
Cluster Manager
Proprietary Replication Service
Cluster Member1
Cluster Member2
Cluster Member n
Key Replication and Synching

The Replication Service, understands these packets and replicates it to the desired cluster member. Upon receiving successful acknowledgement, it marks this packet for destruction source. Now the Key Operation can be of new Key Addition or Key Deletion. Based on the metadata available in the packets i.e. replicated data, desired operation is performed on that particular DSS. After successful operation, the Replication service fetches the key status and same will be updated on portal.

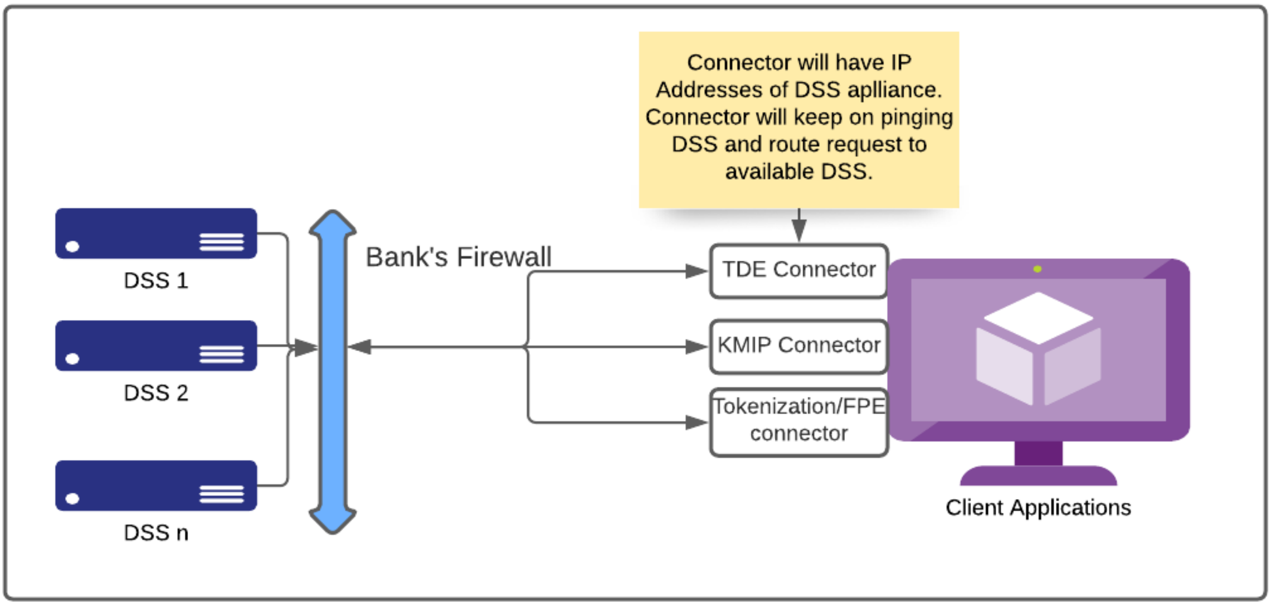
If any Key Synchronization activity fails, then the DSS from where the Keys are supposed to be replicated, keeps this data till the time, the member DSS comes online. Once the member DSS is online, the Replication Service, starts synchronizing this data with that node.

HIGH AVAILABILITY

High Availability with DSS can be achieved with or without Load Balancers. If Load Balancers are configured, then VIP (Virtual IP) has to be configured on LB with IP Addresses of all DSS configured along with it. This VIP will be configured with KMIP Connectors on client-side.

In case LB is not configured then IP Addresses of DSS has to be listed in connector's configuration file. Client connectors keeps probing the DSS status with custom protocol i.e. Heartbeat.

If the connector is not able to get active connection with DSS, it will generate a log message and try to connect with other DSS IP.


Connector will have IP Addresses of DSS aplliance. Connector will keep on pinging DSS and route request to available DSS.
DSS 1
DSS 2
DSS n
Bank's Firewall
TDE Connector
KMIP Connector
Tokenization/FPE connector
Client Applications

JISA®
Creating Secured Ecosystem

Contact:

sales@jisasoftech.com , support@jisasoftech.com

Phone: 020-25888445, 022-49727513

JISA Softech Pvt. Ltd.
5, Shree Building, Kotbagi Hospital Lane,
Near IndusInd Bank, DP Road, Aundh, Pune – 411007

www.jisasoftech.com