JISA®
Creating Secured Ecosystem

JISA Softtech Pvt. Ltd.

www.jisasoftech.com

CryptoBind® HSM

Key Backup-Restore with External Hardware Backup Drive

v1.1

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.

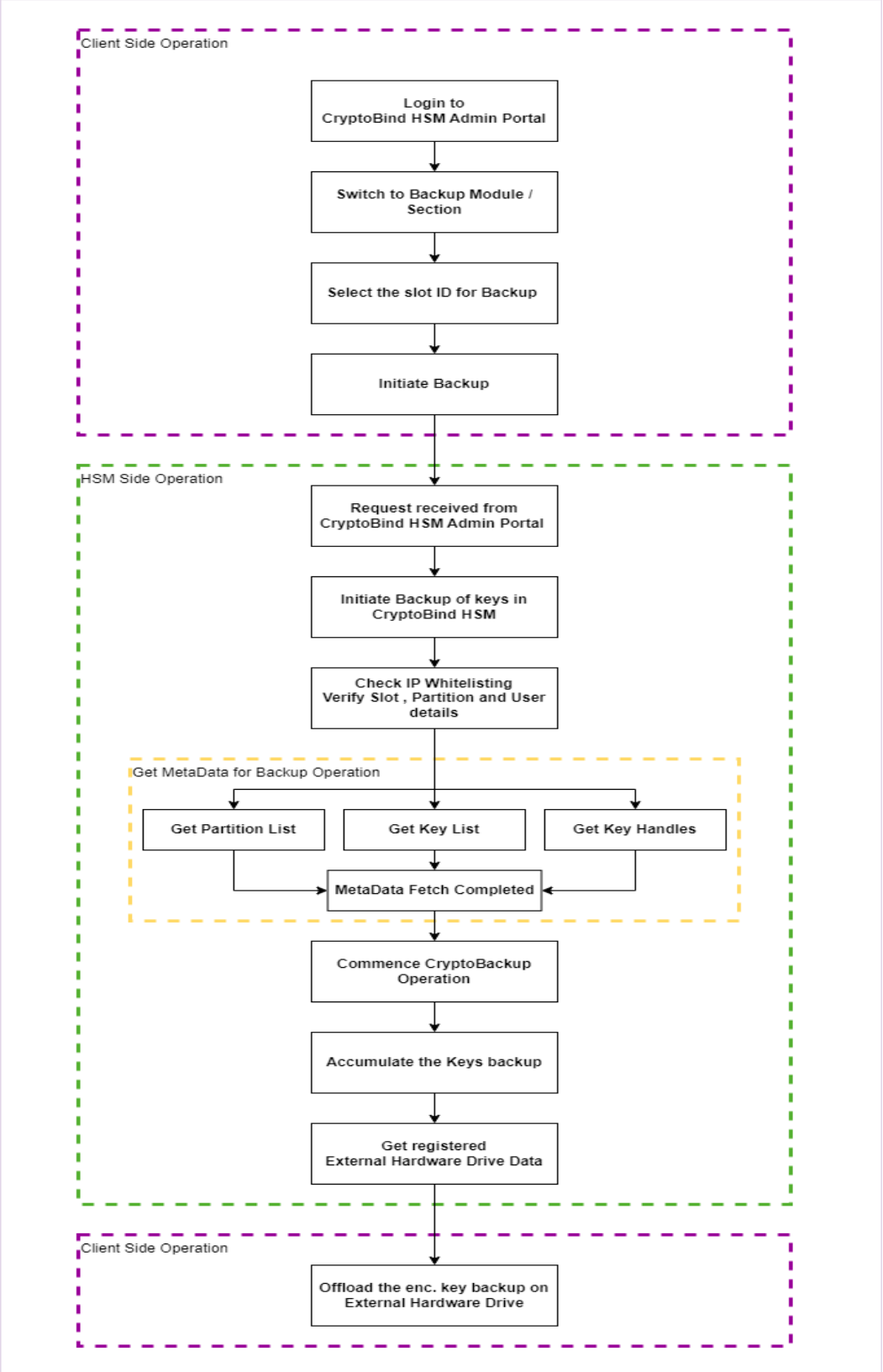
ABOUT DOCUMENT

In the realm of cryptographic operations, the security and availability of cryptographic keys are paramount. Ensuring that these keys are securely backed up and can be restored efficiently is crucial for maintaining the integrity and continuity of cryptographic services. This document provides a detailed overview of the key backup and restore operations process using external hardware backup drives within the CryptoBind Hardware Security Module (HSM) ecosystem.

The process outlined herein covers both client-side and HSM-side operations, offering a comprehensive guide for administrators and security officers tasked with managing key backups. The steps involved are designed to ensure that backups are securely created, stored, and can be reliably restored when necessary.

This document serves as a critical resource for understanding the end-to-end process of key backup and restore operations, emphasizing the importance of secure and redundant storage solutions. By leveraging external hardware backup drives, organizations can achieve a higher level of security and resilience, thereby fostering a secure and robust cryptographic environment.

PROCESS FLOW - KEY BACKUP AND RESTORE OPERATIONS EXTERNAL HARDWARE BACKUP DRIVE



The accompanying diagram provides a visual representation of the comprehensive process involved in key backup and restore operations using external hardware backup drives within the CryptoBind Hardware Security Module (HSM) framework. This diagram illustrates the sequential steps taken to securely back up cryptographic keys and ensure their reliable restoration, highlighting the distinct roles of client-side and HSM-side operations.

Key Sections of the Diagram:

Client Side Operation:

- This section details the initial steps carried out by the user through the CryptoBind HSM Admin Portal. It covers the process from logging in and navigating to the Backup module, to selecting the slot ID for backup and initiating the backup process with proper authentication.

HSM Side Operation:

- Once the backup is initiated from the client side, the HSM performs critical tasks such as verifying the request, checking IP whitelisting, and fetching necessary metadata. This ensures that the backup process adheres to stringent security protocols.

Metadata Fetch and Backup Accumulation:

- This part of the process involves gathering essential information like partition lists, key lists, and key handles. After fetching this metadata, the HSM accumulates the encrypted keys backup, ensuring that all data is securely encrypted and organized.

External Hardware Backup Drive Integration:

- The diagram also highlights the verification and usage of external hardware drives for storing the encrypted key backups. This includes offloading the backups to multiple drives viz. 3/5/7 to ensure redundancy and security.

Key Restore Operation:

- The reverse process for key restoration is also depicted, illustrating how encrypted key backups can be retrieved and decrypted from the external hardware drives, ensuring the keys are restored to their respective slots and partitions within the HSM.
- This diagram serves as a crucial tool for understanding the detailed workflow of key backup and restore operations, emphasizing the importance of secure backup procedures and reliable data restoration capabilities. By following the outlined steps, organizations can ensure the integrity, availability, and security of their cryptographic keys, thereby maintaining robust cryptographic operations.

DETAILED KEY BACKUP AND RESTORE OPERATIONS PROCESS WITH EXTERNAL HARDWARE BACKUP DRIVE

Client Side Operation

Login to CryptoBind HSM Admin Portal:

- The user starts by logging into the CryptoBind HSM Admin Portal. This requires entering their credentials as a Management User. Management Users typically have the necessary permissions to perform administrative tasks such as key backups.
- Upon successful login, the user is directed to the dashboard. The dashboard serves as the central interface, providing access to various modules and functions within the admin portal.

Navigate to the Backup Module:

- From the dashboard, the user locates and selects the Backup module. This module is accessible from the left-side panel of the dashboard interface.
- Switching to the Backup section allows the user to manage backup-related operations, including selecting specific slots and initiating backups.

Select Slot ID for Backup:

- Within the Backup module, the user identifies and selects the slot ID corresponding to the partitions and keys they wish to back up.
- To proceed with the backup, the user, who is typically an admin of the portal, must enter the Security Officer (SO) ID and password. This step ensures that only authorized personnel can initiate the backup process.
- Upon successful authentication, the backup process is initiated. This ensures that all necessary security protocols are followed before any data is handled.

Initiate Backup:

- Once the authentication is successful, the backup initiation command is sent from the client side. This command triggers the backup process within the CryptoBind HSM.
- The client-side operations are crucial for setting the parameters and authorizing the backup, ensuring that the process starts with proper oversight and control.

HSM Side Operation

Request Received by HSM:

- The CryptoBind HSM receives the backup initiation request from the admin portal. This marks the beginning of the HSM-side operations.
- The HSM first performs an IP whitelist check to ensure that the request is coming from a trusted source. This security measure helps prevent unauthorized access and potential security breaches.

Verify Backup Details:

- The HSM verifies the details of the backup request, including the slot ID, partition information, and user credentials. This step ensures that the request aligns with the HSM's security policies and that the correct data is being accessed.

Fetch Metadata for Backup Operation:

- The process of fetching metadata begins. This involves gathering essential information required for the backup operation, such as:
    - Partition List: Identifying all the partitions that need to be backed up.
    - Key List: Compiling a list of all keys within the selected partitions.
    - Key Handles: Retrieving the handles associated with each key, which are necessary for managing the keys during the backup process.

Metadata Fetch Completion:

- Once all necessary metadata is gathered, the system marks the metadata fetch as complete. This status update indicates that the system has all the required information to proceed with the actual backup operation.

Commence CryptoBackup Operation:

- With the metadata fetch completed, the HSM initiates the CryptoBackup operation. This involves creating secure backups of each key within the defined slots and partitions.
- The backup operation is meticulously designed to ensure that each key is encrypted and stored securely, maintaining the integrity and confidentiality of the data.

Accumulate Encrypted Keys Backup:

- The HSM accumulates the encrypted keys backup. During this process, the keys are securely encrypted and organized, preparing them for transfer to external hardware backup drive.
- The encryption ensures that even if the backup data is intercepted or accessed without authorization, the keys remain protected and unusable without the correct decryption mechanism.

Verify External Hardware Drive Data:

- The HSM verifies the data of the registered external hardware backup drives. This step is crucial to ensure that the external hardware backup drives are recognized and authenticated by the system.
- Verification of external hardware backup drives helps maintain the security and integrity of the backup process, preventing unauthorized devices from accessing sensitive data.

Offload Encrypted Key Backup:

- The final step involves offloading the encrypted key backup to the external hardware backup drives. The process ensures that the backups are securely transferred and stored on multiple external drives.
- Typically, the encrypted key backups are offloaded to sets of 3, 5, or 7 external hardware backup drives. This redundancy ensures that multiple copies of the backup exist, providing robust data recovery options in case of hardware failure.

Key Restore Operation:

- The key restore process works in a reverse manner to the backup process. If keys need to be restored, the encrypted key backups can be retrieved from the external hardware backup drives.

The restore operation involves:

- Logging into the CryptoBind HSM Admin Portal and navigating to the restore module.
- Selecting the slot ID and partition from which the keys need to be restored.
- Authenticating the restore request with the SO ID and password.
- The HSM then fetches the encrypted key backups from the external hardware backup drives, verifies their integrity, and decrypts the keys.
- The keys are then restored to their respective slots and partitions within the HSM, ensuring they are ready for use.
- This operation ensures that the key management process remains secure and reliable, allowing for quick recovery and continued operation.

EXTERNAL HARDWARE BACKUP DRIVE REFERENCE

CryptoBind External hardware backup drives play a crucial role in the secure storage and redundancy of cryptographic key backups. These drives are essential components in ensuring that key backups are not only stored securely but also readily available for restoration when needed. Below are some key points highlighting the importance and functionality of external hardware backup drives in the key backup and restore operations process:

1. **Enhanced Security:**

- External hardware backup drives provide an additional layer of security by storing key backups separately from the main system. This physical separation reduces the risk of unauthorized access and potential data breaches.
- The backups stored on these drives are encrypted, ensuring that even if the drives are intercepted or accessed without proper authorization, the data remains secure and unusable without the correct decryption keys.

2. **Redundancy and Reliability:**
    - Utilizing multiple external hardware backup drives creates redundancy, which is critical for data recovery. By storing backups on sets of 3, 5, or 7 drives, organizations ensure that multiple copies of the data exist.
    - This redundancy means that if one drive fails, the backup can still be retrieved from another drive, providing a robust solution for data recovery and business continuity.
3. **Ease of Management:**
    - External hardware drives are easy to manage and transport, making them an ideal choice for offsite storage. Regularly updating and rotating these drives ensures that the most recent backups are always secure and accessible.
    - The drives can be registered and verified by the HSM, ensuring that only authorized devices are used for storing sensitive key backups.
4. **Quick Restoration:**
    - In the event that keys need to be restored, external hardware backup drives enable quick and efficient recovery. The encrypted key backups can be retrieved, verified, and decrypted, ensuring that keys are restored to their respective slots and partitions within the HSM.
    - This capability ensures minimal downtime and disruption to cryptographic operations, allowing organizations to maintain their security posture and operational efficiency.

Below is an illustrative reference image of the External Hardware Backup Drive, which is integral to the secure and redundant storage of cryptographic key backups. This image exemplifies the type of hardware used in the key backup and restore operations.

Contact:

sales@jisasoftech.com , support@jisasoftech.com

JISA Softech Pvt. Ltd.

A-604, 6th Floor, Ganraj Chowk, Amar Business Zone Baner, Swati Park, Veerbhadra Nagar, Baner, Pune, Maharashtra 411045

www.jisasoftech.com