Redbooks
ibm.com/redbooks

TKE for Managing CryptoExpress

Mona Bagare
Divya K K
Anil Pasupuleti
Garry Sullivan
Eric Weinmann

IBM

TKE for Managing Crypto Express

Cryptography is the foundation of trust in modern digital enterprises. Financial transactions, personal data, digital identities, certificates, and critical business applications all rely on cryptographic systems to protect information from unauthorized access and manipulation. At the heart of these systems are Hardware Security Modules (HSMs), specialized security devices designed to safeguard cryptographic keys and perform sensitive cryptographic operations within a highly protected, hardware-based environment.

As organizations expand their use of IBM Z® and LinuxONE platforms, the management of cryptographic infrastructure becomes increasingly important. Enterprises often operate large environments consisting of multiple HSMs, numerous cryptographic domains, distributed administration teams, and stringent regulatory requirements. Managing these environments requires more than simply protecting keys; it requires secure processes, separation of duties, dual control, auditability, and operational consistency on a large scale. IBM® Trusted Key Entry (TKE) was created to address these challenges.

IBM TKE is IBM's solution for delivering compliant, hardware-based HSM management mechanisms for IBM Z and LinuxONE environments. TKE contains wizards that guide users through all primary HSM management tasks, while streamlining the user experience needed to meet stringent regulatory standards and guidelines.

IBM has introduced IBM HSM Manager, the next generation of HSM management. This tablet-based application connects to TKE appliances, enabling authorized administrators to securely manage IBM Z and LinuxONE HSMs from different locations. By eliminating the requirement for administrators to be physically co-located, IBM HSM Manager streamlines routine HSM administration, helping organizations reduce operational delays, lower travel expenses, and improve overall administrative efficiency.

This IBM Redbooks® Redguide introduces the concepts, architecture, capabilities, and operational practices associated with TKE and IBM HSM Manager. It is intended for security administrators, system programmers, security architects, compliance specialists, operations teams, technical decision makers, and anyone responsible for managing cryptographic infrastructure on IBM Z and LinuxONE systems.

By first establishing a solid understanding of HSMs, master keys, cryptographic domains, and regulatory requirements, this guide provides the context necessary to understand the purpose of TKE and how it delivers secure, scalable, and compliant HSM management. Subsequent chapters explore TKE architecture, key lifecycle management, remote administration through IBM HSM Manager, operational best practices, and deployment considerations.

Whether you are evaluating TKE for the first time, modernizing existing cryptographic management processes, or implementing remote HSM administration capabilities, this guide provides practical insight into the role of TKE within IBM Z and LinuxONE cryptographic environments.

Authors and Contributors

This paper was produced by a team of specialists from around the world working with the IBM Redbooks team.

Mona Bagare is a Hardware Developer for IBM Z Crypto in India with more than 9 years of experience in system testing and hardware validation. She has worked at IBM for more than 4 years. Her areas of expertise include IBM Z cryptographic technologies, Linux system testing, hardware validation, test automation, and security testing of cryptographic solutions. She has contributed to the validation of IBM Z Crypto hardware and security technologies in compliance with enterprise requirements.

Divya K K is a Senior Software Engineer at IBM India with more than 12 years of experience. Her expertise includes IBM Z cryptography, TKE workstation development, and HSM management solutions.

Anil Pasupuleti is the IBM Z Firmware Test Architect in Bangalore, India. He has 21 years of experience in system firmware testing and security. He has worked at IBM for 15 years. He has experience in HMC/SE, zRSF, Secure Service Containers, Hyper Protect services, and most recently serves as the Test Architect of HSM firmware. He has written about IBM Z, firmware testing, and PQC web samples.

Garry Sullivan is the Trusted Key Entry (TKE) Product Architect in the US. He has 38 years of experience in security. He has worked at IBM for 43 years. He has experience in IBM RACF®, IBM i Security, leading Common Criteria evaluation, and most recently serving as the technical product owner of TKE. He has written extensively on IBM Z and LinuxONE HSM management.

Eric Weinmann is a Senior Software Engineer in the US. He has 39 years of experience in IBM Z architecture, UX design, and engineering fields.

Thanks to the following people for their contributions to this project:

Lydia Parziale, Certified IT Specialist, PMI Certified Project Manager, IBM Redbooks® Project Leader, IBM Redbooks, Poughkeepsie Center.

Christina Pomeroy, Product Manager, Cryptographic Security, IBM.

Introduction to Hardware Security Modules and Trusted Key Entry

Trusted Key Entry (TKE) is an IBM Z and LinuxONE feature that provides a dedicated appliance for managing Hardware Security Modules (HSMs) on IBM Z and LinuxONE systems. Before discussing TKE and HSM management, it is important to first understand what an HSM is and the role it plays in cryptographic security.

Definition of HSM

An HSM is a specialized, physically secure device that provides a place to do cryptographic operations quickly, efficiently, and securely.

HSMs have these characteristics:

- **Dedicated cryptographic processing** – HSMs perform standardized cryptographic algorithms. They use specialized hardware to deliver high performance and efficiency, particularly for computationally intensive cryptographic operations.
- **Master key protection** – HSMs maintain one or more highly protected master keys. These keys are used to encrypt sensitive information, ensuring that protected data and keys can be decrypted and accessed only within the secure physical boundaries of the HSM.
- **Tamper-resistant and tamper-responsive design** – The HSM's hardware is enclosed within a secure physical boundary designed to detect attempts at physical attack or manipulation. If tampering is detected, the HSM responds by automatically erasing sensitive keys and secrets, preventing their compromise.

HSMs serve as a trusted root of security for critical applications and infrastructure, including payment processing, digital certificate management, encryption and decryption services, and key management systems.

HSM Master Keys

The typical workflow and usage is as follows:

1. The master key(s) of the HSM are set.

> **Note:** A master key is a high-level secret key that never leaves the physical boundaries of the HSM. It encrypts and protects all other keys in the system. The master key is sometimes referred to as a **Master Wrapping Key (MWK)** because it is used to "wrap" (encrypt) other keys.

2. An operational key is created and wrapped by the master key.
   - The master key encrypts a key that will be used by one or more applications to perform specific cryptographic functions.
   - When the key is wrapped, it is assigned a label that is subsequently used to identify and reference the key.

> **Note:** An **operational key** is a key derived from a master key and used by applications to encrypt, decrypt, or sign data.

3. After being wrapped, the encrypted operational key is stored in a **key store** or **key vault** outside of the HSM.
   - A key store or vault may contain anywhere from a single key to millions of keys.
4. An application calls an HSM API to do a cryptographic operation.
   - When an application needs to run cryptographic operations on data, it will retrieve the wrapped operational key from the key store or vault.
   - It then passes that key and data to the HSM for processing through the HSM's API commands.
5. The HSM performs the cryptographic operation.
   - The HSM unwraps or decrypts the operational key internally.
   - The operational key is used to perform the requested cryptographic function, such as encryption, decryption, signing, or other operations.
   - The result of the operation is returned to the application.
6. The operational key is discarded.
   - Once the operation is complete, the HSM removes the operational key from working memory.
   - To use the key again, the wrapped key must be provided to the HSM so that the operational key can be recreated and used for another cryptographic operation.

Master Keys Are Special

Master keys protect every operational key stored in a key store or vault. **The master key is the key that protects all other keys.** If a master key is stolen, every key protected by that master key is at risk. If a master key is lost, you lose the ability to use your keys.

Because of their critical role, industry standards and regulatory requirements often impose strict controls around how HSMs and specifically master keys are managed. IBM provides the ability to manage an HSM's master keys in a way that conforms to industry standards and regulatory requirements.

HSM Management Standard and Regulatory Management Requirements

Most standard and regulatory HSM management requirements include the need for separation of duties, dual controls, split knowledge, key part integrity, process auditability, and processes that require the use of human actors.

In practical terms, compliant-level HSM management requires:

- **Separation of duties:** A control principle that divides management tasks among multiple distinct roles. It ensures no single administrator possesses unchecked power to create, export, recover, or use keys entirely on their own.
- **Dual control:** A security procedure requiring two or more distinct, authorized roles to act together to complete a high-risk task. All HSM management activities on the TKE must be performed under dual control.
- **Split knowledge:** A method where a key is divided into multiple unique components. Each individual component reveals nothing about the actual key on its own. Reconstructing or activating the complete key requires combining these components.
- **Key part integrity:** Ensures the individual components of a split key remain uncorrupted, authentic, and correctly ordered during multi-person assembly. It prevents tampering or injection of false data when a master key is loaded into the secure hardware via split-knowledge procedures.
- **Process auditability:** The TKE has the built-in capability to independently record, verify, and trace every administrative action, state change, and cryptographic operation inside the secure hardware boundary. It ensures complete accountability by tracking who did what, and when.
- **Processes use human actors:** Requires that HSM management activities be driven by manual and human-based duties, authorizations, and operational controls.
- **Non-exportability:** Key material must never exist outside that protected environment in the clear.

In addition to operational controls, compliance requirements may restrict the cryptographic algorithms, key wrapping methods, and minimum key strengths that can be used. HSM management processes must support and enforce these requirements.

HSM Environments

Cryptographic environments in IBM Z and LinuxONE are complex. To begin, IBM provides a multi-domain HSM with 85 different spaces (called domains) where you can set master keys.

In addition:

- Environments typically consist of many HSMs running on different IBM Z and LinuxONE servers.
- Environments often contain a mixture of server and HSM levels.
- HSMs and their domains can operate in three different modes:
  - CCA normal mode
  - CCA compliant mode
  - EP11 mode

IBM must provide a way to simplify the management of large, complex HSM environments.

Trusted Key Entry

Because HSMs protect an organization's most sensitive cryptographic assets and serve as the foundation of the cryptographic environment, their administration requires trusted processes and controls that can withstand rigorous security, audit, and compliance requirements.

TKE provides the hardware-based controls and management capabilities that clients require to securely administer IBM Z and LinuxONE HSMs in accordance with regulatory and industry requirements. At the same time, TKE simplifies HSM management in complex cryptographic environments wherever possible.

In short, TKE streamlines the HSM management process without compromising the security controls required to manage HSMs.

Overview of TKE Architecture

Today, Hardware Security Module (HSM) management is performed by multiple security administrators using a Trusted Key Entry (TKE) console located within a secure area or on a raised floor. Security administrators must be physically co-located with the TKE console, together with their smart cards and smart card readers, to authenticate and perform HSM administration tasks. Figure 1 shows a secure HSM key management process in which multiple security administrators, each holding a portion of the cryptographic key on a smart card, collaborate through a TKE workstation (also known as the TKE console). The TKE securely distributes and manages cryptographic keys for IBM Z and LinuxONE systems, ensuring that no single administrator has complete control of the master key material.

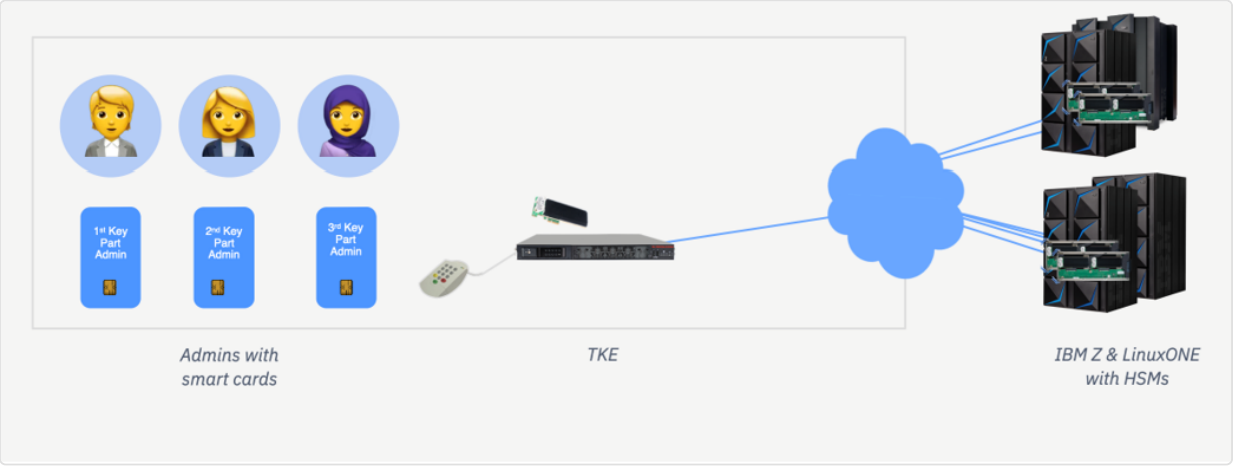

Figure 1: TKE with Security administrators on the raised floor within a secure area

For geographically distributed organizations, this operational model can be costly and time-consuming because business travel may be required, introducing scheduling constraints and operational delays.

The TKE, paired with the IBM HSM Manager app, extends this operational model by enabling geographically distributed security administrators to participate in HSM configuration and master key management procedures without being physically co-located with the TKE console. Administrators can securely perform controlled operations by using existing smart cards while continuing to enforce hardware-based security controls, dual control, and separation of duties. Figure 2 illustrates the high-level TKE architecture and the interaction between its key components.

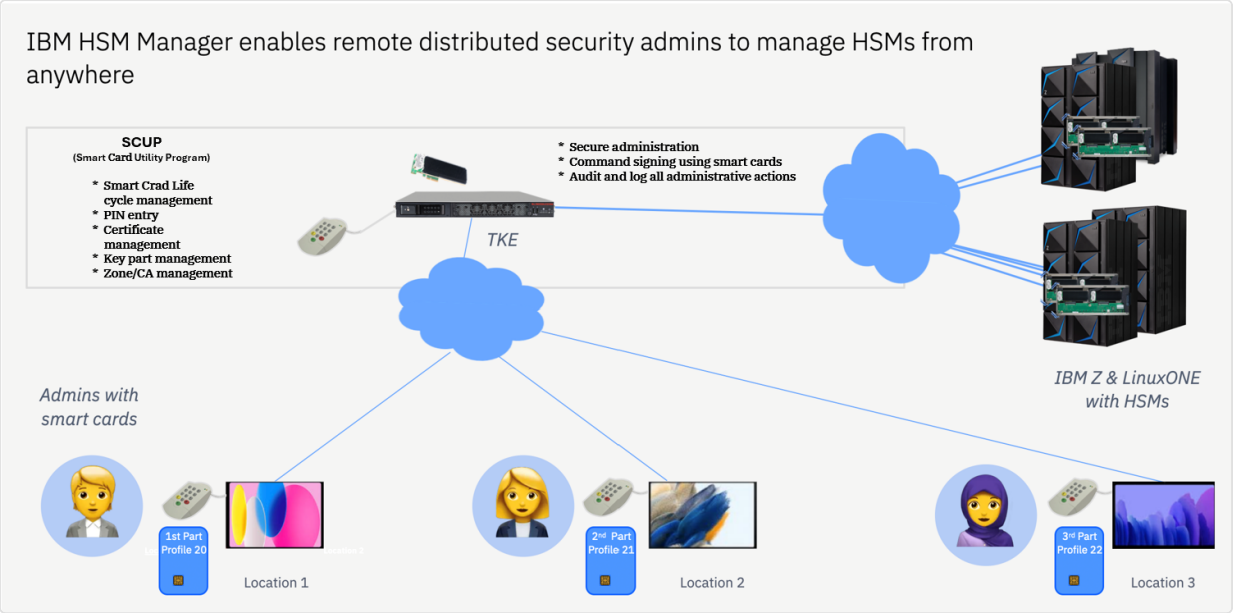

Figure 2: TKE with Security administrators in their secure and remote locations

Key Components and How They Interact

Master keys form the cryptographic root of trust for Crypto Express domains and are fundamental to protecting operational key material. Although Common Cryptographic Architecture (CCA) and Enterprise PKCS #11 (EP11) use different master key architectures and management procedures, both environments follow controlled workflows to establish, activate, and maintain master keys under strict security controls. Those workflows adhere to standards directed by non-IBM governing agencies, such as the National Institute of Standards and Technology (NIST). The following sections provide a high-level overview of the key management processes for each domain type and illustrate the major steps involved in master key lifecycle operations.

Overview of key components

The TKE environment consists of the following major components:

- Security administrators
- Smart cards
- Smart card readers
- TKE workstation
- Secure management network

Together, these components provide the secure administrative infrastructure required to manage HSMs in IBM Z and LinuxONE environments.

Security administrators use smart cards through smart card readers attached to the TKE workstation to authenticate and participate in controlled key management procedures. A Smart Card Utility Program (SCUP) manages the lifecycle of the smart cards and the card-resident objects required for these procedures. The TKE workstation sends the approved management operation over the secure management network to the host cryptographic environment, where the target HSM domain performs the requested key management action.

IBM HSM Manager enhances HSM administration by providing centralized management and coordination capabilities across the enterprise. Administrators can participate in key-management and configuration activities from distributed locations by using their existing smart card credentials, enabling organizations to manage cryptographic resources more efficiently while maintaining established security and compliance controls.

Smart card considerations

Attention: TKE introduces a redesigned SCUP, based on a newer framework for smart card administration. Existing smart card environments and associated operational procedures should be reviewed before TKE is deployed in production. The SCUP delivered with TKE does not support all older smart card and applet operations in the same manner as earlier workflows. Smart cards currently in use should be inventoried, and any dependencies on legacy card types, applets, or administrative procedures should be identified. Procedures such as initialization, personalization, backup, copy, and migration should be validated before rollout. Validation in a preproduction environment is recommended to confirm smart card compatibility and operational readiness.

Integration with IBM Z and Crypto Express

Figure 3 shows the Trusted Key Entry (TKE) architecture used to securely manage cryptographic domains and keys across IBM Z and Linux environments. The TKE workstation communicates over a TLS-encrypted management network with IBM z/OS® and Linux systems, enabling centralized and secure administration of Crypto Express adapters operating in either CCA or EP11 mode.

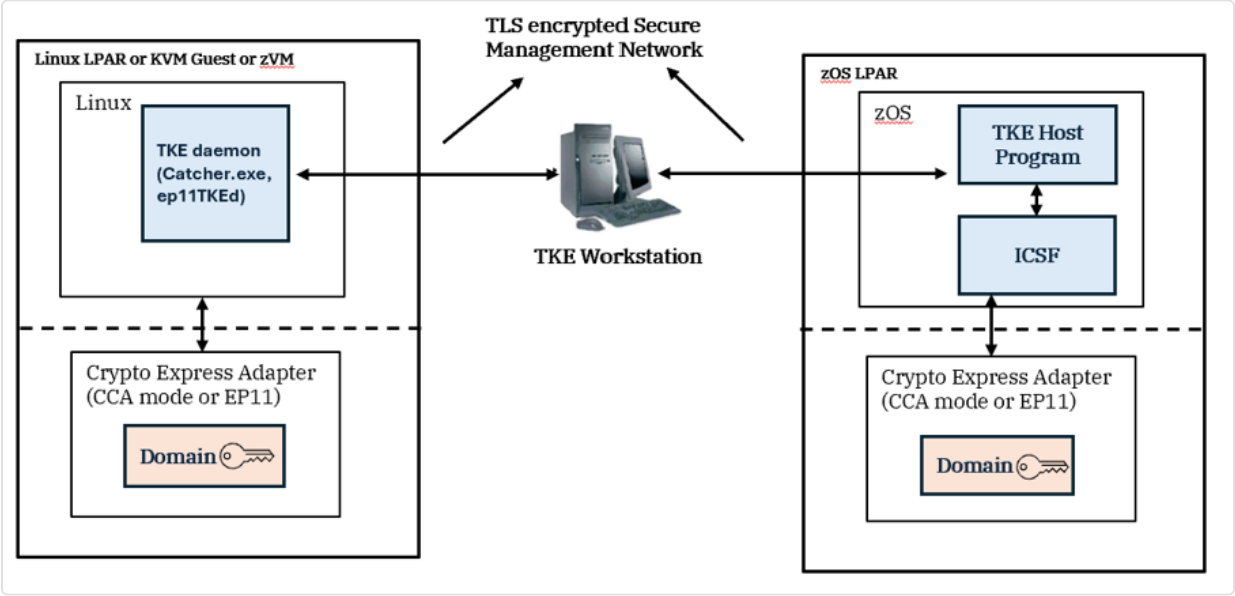

Figure 3: TKE Integration with IBM Z and Crypto Express

z/OS

In a z/OS environment, TKE communicates with the host cryptographic environment through the z/OS TKE Host Program and Integrated Cryptographic Service Facility (ICSF). The TKE workstation sends management requests over the secure management network to the z/OS LPAR, where the TKE Host Program receives and processes the request. The Host Program works with ICSF, which provides the host cryptographic services layer for z/OS. ICSF then interfaces with the target Crypto Express adapter and domain to perform the requested key management or HSM administration operation. In this model, TKE does not interact directly with the Crypto Express adapter; instead, the interaction is mediated by the z/OS host software stack. This path is used for operations such as domain administration, master key loading, key register management, and other controlled HSM procedures.

Linux

In a Linux environment, TKE communicates with the host cryptographic environment through the TKE daemon running in the Linux LPAR, KVM guest, or IBM z/VM® guest. The TKE workstation sends management requests over the secure management network to the Linux system, where the TKE daemon, such as catcher.exe or ep11TKEd, receives and processes the request. The daemon then interacts with the target Crypto Express adapter and domain

configured in CCA mode or EP11 mode, depending on the deployment model. This provides the host-side path for TKE management operations in Linux environments. As with z/OS, TKE remains part of the management plane rather than the application cryptographic path, and is used for secure HSM administration, master key procedures, and domain-level configuration tasks.

High-Level Workflow of Key Management

Master keys provide the cryptographic foundation for securing operational key material within Crypto Express domains. Although CCA and EP11 implement master key management differently, both environments use controlled processes to load, activate, and maintain master keys. The following sections summarize the high-level workflows for each model.

CCA master key workflow

Figure 4 illustrates the high-level workflow for establishing and activating new CCA master keys within a Crypto Express domain. The process includes selecting the master key type, loading and validating multiple key parts, transitioning the new key into service, and finally re-enciphering key repositories (CKDS and PKDS) to protect existing cryptographic assets under the new master key.

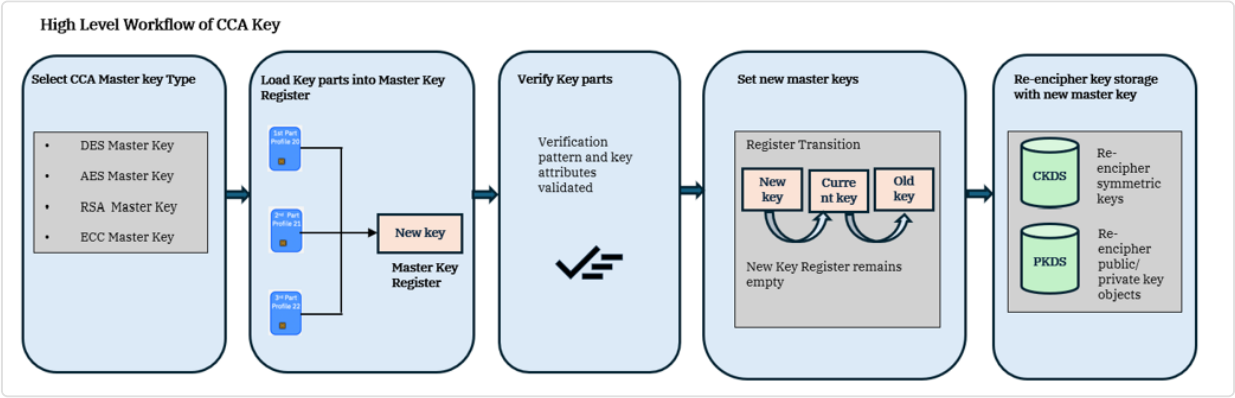

Figure 4: CCA master key workflow

In a CCA environment, master key management is performed through controlled TKE procedures that load, set, and activate master keys for the target Crypto Express domain. CCA supports multiple master key types, including DES, AES, RSA/PKA, and ECC/APKA master keys. Each master key can be loaded as multiple key parts to enforce dual control and separation of duties.

During a master key change, security administrators use TKE smart cards to load the key parts into the new master key register of the target domain. After verification, the new master key is set. When the set operation completes, the current master key moves to the old register, the new master key becomes the current master key, and the new register is cleared.

The master key remains securely within the CCA domain and is used to protect operational key material rather than being used directly by applications. In general, DES and AES operational keys stored in the CKDS, and RSA/PKA or ECC key objects stored in the PKDS, are encrypted under the active master key. After the master key is changed, the affected key storage must be re-enciphered under the new current master key so that the operational keys remain consistent with the updated domain state.

EP11 master key workflow

Figure 5 illustrates the high-level process for establishing and activating an EP11 master key within a Crypto Express EP11 domain. Unlike CCA, EP11 uses a single master key; the workflow involves loading multiple key parts, verifying the assembled key, and activating the new master key so it becomes the active cryptographic root for the target domain.

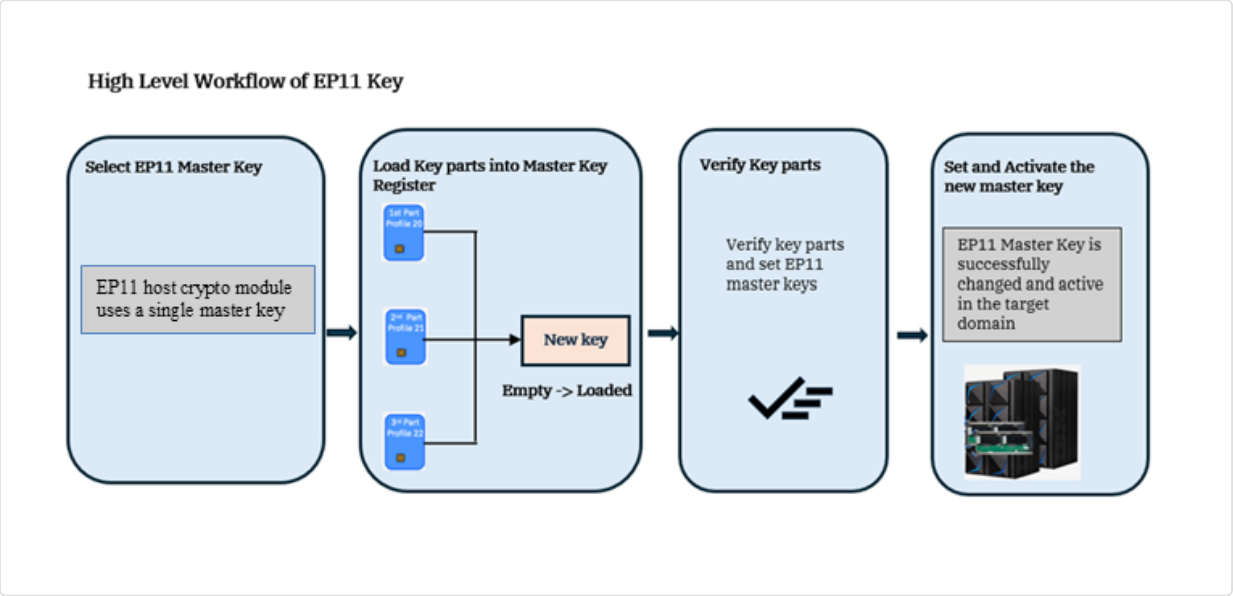

Figure 5: EP11 master key workflow

In an EP11 environment, master key management is performed through controlled TKE procedures that load, set, and activate the EP11 master key for the target Crypto Express EP11 domain. EP11 uses a single master key model, and the master key can be loaded as multiple key parts to enforce dual control and separation of duties.

During a master key change, security administrators use TKE smart cards to load the EP11 master key parts into the target domain. After verification, the new master key is set and activated for that EP11 domain. The EP11 master key remains securely within the EP11 domain and is used to protect EP11 operational key material rather than being used directly by applications. As in the CCA model, master key change procedures should be followed by the appropriate operational steps to ensure that key material managed by the domain remains consistent with the newly activated master key.

Core Capabilities of TKE

In this chapter, we discuss:

- Key lifecycle management
- Secure access controls and separation of duties
- Guided workflows and administrative assistance

Key lifecycle management

A primary role of the Trusted Key Entry (TKE) workstation is to provide a secure administrative interface for managing the lifecycle of cryptographic keys in CCA and EP11 environments. TKE is used to control sensitive key management operations such as master key part handling, secure key distribution, master key loading, and master key rotation. In the TKE model, the Smart Card Utility Program (SCUP) is used to prepare and manage the smart cards that hold key parts and administrative credentials, while TKE is used to execute the corresponding HSM-side key management procedures for the target crypto domain.

Master key creation and key part handling

TKE supports the controlled creation and handling of master key parts used during HSM key management procedures. Rather than treating a master key as a single clear value, TKE procedures allow the value to be divided into multiple parts and assigned to different security administrators. This approach helps enforce dual control and

separation of duties for sensitive key management operations. Smart cards prepared through SCUP are used to securely hold these key parts, together with the associated administrative credentials required for TKE operations. In this way, SCUP provides the smart card preparation layer of the process, while TKE provides the secure operational interface for using those cards in HSM administration.

Smart card–based distribution and administrative control

TKE also supports the secure distribution of master key material by using smart cards as the protected transport mechanism for key parts, authority keys, and administrative credentials. In this model, individual key parts are distributed across authorized administrators and are presented only during controlled TKE procedures. This design helps ensure that the complete key value is not exposed outside the trusted smart card and HSM environment. It also allows geographically distributed administrators to participate in controlled key management procedures while maintaining the procedural safeguards required for HSM administration.

CCA master key rotation and key-store transition

For CCA host crypto modules, TKE is used to support the loading and change of DES, AES, RSA/PKA, and ECC/APKA master keys. In a typical CCA workflow, administrators load new master key parts into the new master key register, verify the loaded value, and then set the new master key. When the change is completed, the current master key is moved to the old master key register, the new master key becomes the current master key, and the new register is cleared. Because the active CCA master keys protect operational key material in host key data sets, the master key change is normally coordinated with re-encipherment of the CKDS or PKDS, depending on the key type, so that the stored keys remain consistent with the newly activated master key. In this model, TKE controls the HSM-side master key procedure, while ICSF coordinates the associated host key-store update and activation activities.

EP11 master key rotation and TKDS transition

For EP11 host crypto modules, TKE is used to support the loading and change of the P11 master key for the target EP11 domain. As in the CCA model, the master key can be handled as multiple parts under dual control and loaded through controlled TKE procedures. The EP11 master key protects operational key material associated with the TKDS, and a master key change is normally coordinated with the corresponding TKDS update or re-encipherment activity through ICSF. TKE therefore provides the secure administrative interface for the EP11 domain master key lifecycle, while ICSF coordinates the host-side transition of the associated key data set to the new protection state.

Secure access controls and separation of duties

Another core capability of TKE is the enforcement of secure administrative access controls for HSM management operations. TKE provides the control framework used to restrict access to sensitive cryptographic administration functions through administrator roles, smart card–based authentication, dual control, and separation of duties. These controls help ensure that only authorized personnel can perform operations against the target crypto module or domain.

TKE supports role-based administrative control so that security responsibilities can be assigned according to function, such as domain administration, authority management, master key handling, or audit-related tasks. Access can therefore be limited to the specific functions required by each administrator role, reducing the risk of unauthorized or unintended changes to the cryptographic environment.

A key part of this capability is separation of duties. Sensitive procedures, such as master key loading or authority administration, can be structured so that no single administrator has full control over the complete operation. Instead, different administrators can hold separate smart cards, credentials, or master key parts, allowing the procedure to be completed only through coordinated participation. This model helps reduce operational risk and supports compliance with established security practices.

TKE also supports dual control for high-impact HSM operations. Multiple authorized administrators can participate in the same controlled procedure, and smart cards are used to securely hold the credentials, authority keys, and key parts required for those operations. In this way, TKE combines role-based access control, smart card authentication, and procedural separation of duties into a single administrative security model for CCA and EP11 environments.

Guided workflows and administrative assistance

TKE also provides guided workflows to simplify complex HSM administration procedures. In addition to direct notebook and utility interfaces, TKE provides guided experiences for selected administrative tasks so that administrators can perform sensitive operations in a structured and repeatable manner. This approach helps reduce operational errors, improve consistency, and make complex configuration tasks easier to execute in controlled environments.

TKE guided workflows are particularly useful for activities that involve multiple dependent steps or require careful sequencing. Examples include role creation, authority setup, workstation logon profile preparation, smart card initialization, and smart card migration or replacement. By guiding the administrator through the required inputs and expected sequence of actions, TKE helps ensure that prerequisite information is collected and that the procedure is completed in a predictable way.

These guided functions do not replace the underlying HSM security controls. Rather, they provide an administrative layer that makes those controls easier to apply correctly. In this way, guided workflows complement TKE's broader capabilities for key lifecycle management, smart card–based administration, and secure access control, while helping organizations standardize operational procedures across distributed administration teams.

IBM HSM Manager

IBM HSM Manager is a tablet-based iOS and Android application that allows security administrators to manage Hardware Security Modules (HSMs) on IBM Z and LinuxONE systems remotely. HSMs are tamper-resistant hardware devices that safeguard and manage cryptographic keys. On IBM Z and LinuxONE systems, HSMs are managed through a dedicated appliance called the **Trusted Key Entry (TKE) console**. IBM HSM Manager extends TKE capabilities onto tablets, enabling fully remote, hardware-backed HSM administration without requiring physical co-location with the TKE. IBM HSM Manager supports the full HSM management lifecycle — from initial configuration of an HSM in its factory state all the way through to master key loading — using the same smart cards already provisioned for TKE console use. No new smart cards or credentials are needed.

Existing Pain Points Faced by Customers

HSM management on IBM Z and LinuxONE is an inherently physical process — multiple security administrators must be simultaneously present at a TKE console, inside a secure area or on the raised floor of a data center, each bringing their own smart card or cards.

- **Geographic constraints:** A typical enterprise spans multiple physical sites, each requiring its own co-located security administrators. Any HSM change demands coordinated business travel across cities and countries, which is costly.
- **Scheduling bottleneck:** Because all required administrators must be physically present together, a single unavailability can delay an entire HSM operation, deferring both planned and unplanned work, creating scheduling risks.
- **Duplicate infrastructure:** Each site must maintain its own TKE console, smart card setup, and trained personnel, duplicating hardware investment and overhead.
- **Poor scalability:** Expanding to additional data centers or hybrid cloud environments requires proportionally more physical infrastructure and co-located staff.

How IBM HSM Manager Alleviates the Existing Problems

IBM HSM Manager enables fully remote, hardware-authenticated HSM management from a tablet, preserving all TKE security features while eliminating the need for physical co-location. Security administrators can manage IBM Z and LinuxONE HSMs from any location — administrators at different sites each use their own tablet to contribute smart card key parts to a joint operation, removing the need for travel entirely. Security is not compromised: smart card authentication is preserved end-to-end, key parts are AES-256 encrypted (ECDH-derived, with future Hybrid-Kyber support), all HSM commands are signed on the smart card and verified by the target HSM, and nine layered security controls are enforced from VPN through to host login. IBM HSM Manager works with existing TKE smart cards — no re-provisioning is required.

How to Get IBM HSM Manager

Getting started with IBM HSM Manager is straightforward once the required hardware, software, and connectivity prerequisites are in place. Before installing the application, verify that your TKE environment and client devices meet the following requirements.

Ensure hardware prerequisites are met

- A TKE running TKE version 10.1 with the latest MCLs and the IBM HSM Manager feature enabled.
- Customer-procured tablets running iPadOS 16 or newer, or Android tablets running Android OS 12 or newer, with network connectivity to the TKE.
- Identiv SPR332v2 PIN Pad smart card readers (same model used with TKE consoles).
- USB-C to USB adapters to connect the tablet to the smart card reader.
- Smart cards created using the TKE Smart Card Wizard on the TKE.

Install the IBM HSM Manager app

- Download and install the IBM HSM Manager app on the tablet(s) from the appropriate app store or enterprise distribution channel.
- Verify that the tablet can communicate with the TKE and that the required smart card reader and smart card are available.

You are now ready to get started.

Steps on How to Use IBM HSM Manager

This section walks through the complete end-user flow for IBM HSM Manager, from initial enablement on the TKE through loading master keys across a domain group.

1. Enable IBM HSM Manager on the TKE

Enablement is performed once by a TKE administrator. Figure 1 shows the IBM HSM Manager settings.

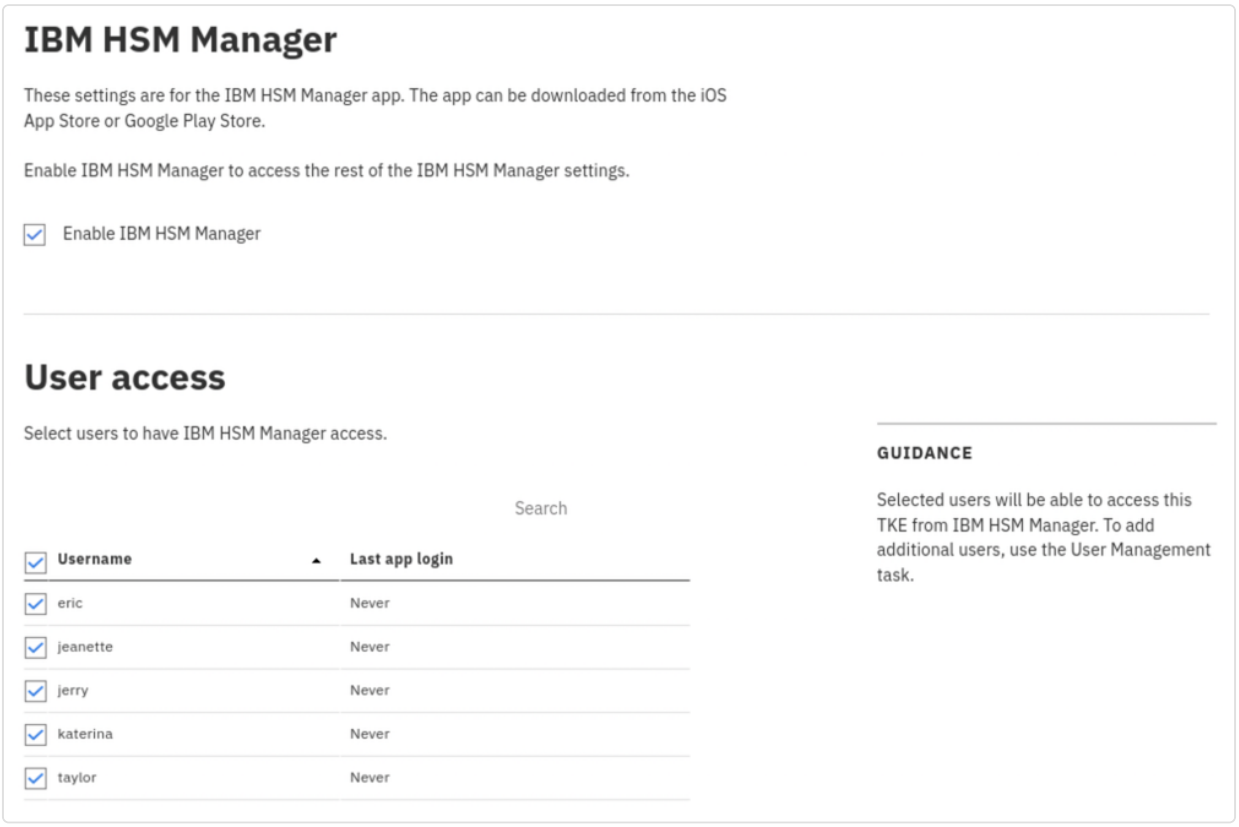

Figure 1 HSM manager settings

a. Log in to the TKE console with an administrator ID using **Privileged Mode Access** from the Welcome view.

b. Navigate to **Service Management** and launch the **IBM HSM Manager Settings** task.

c. **Enable IBM HSM Manager access** and select which TKE users are permitted to connect via the app.

d. (Optional) Create additional TKE users via the User Management task if needed.

2. Add TKE to the App and Authenticate

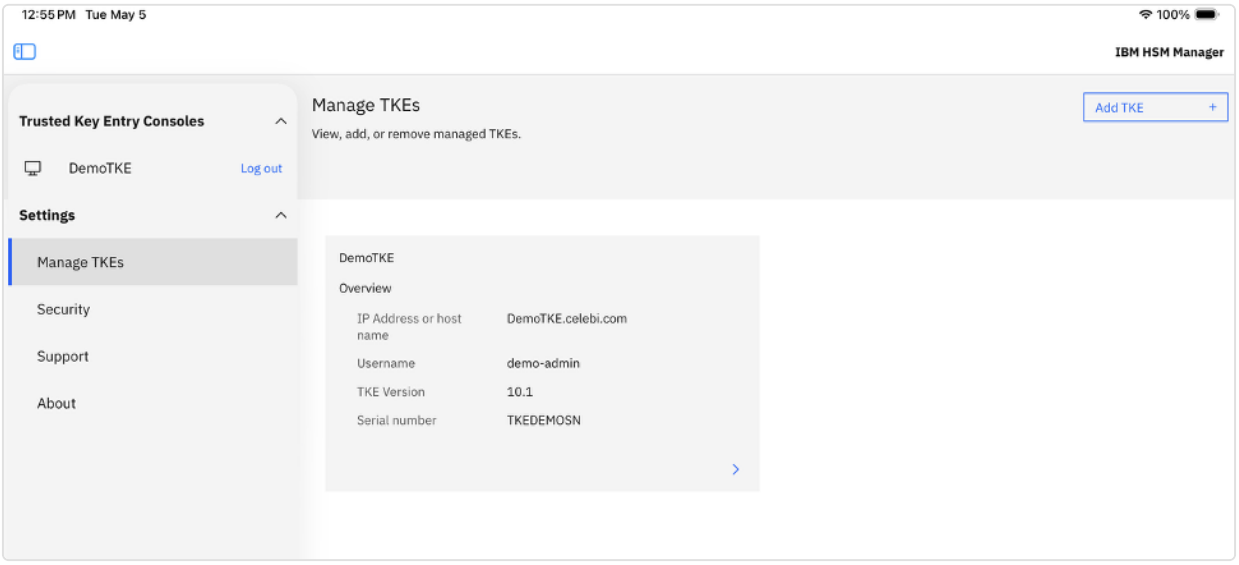

Figure 2 Manage TKE

a. Open the IBM HSM Manager app on the tablet; accept Terms & Conditions and optionally take the introductory tour.

b. Tap the sidebar → Settings → Manage TKEs → Add TKE.

c. Enter the TKE hostname or IP address and the TKE user credentials.

d. Review and import the TKE certificate.

e. If required by the TKE's IBM HSM Manager settings, set an App password.

f. Tap Add TKE to complete the workflow.

3. Log In to the TKE HSM

All users in the TKE HSM group profile must authenticate before HSM management can begin.

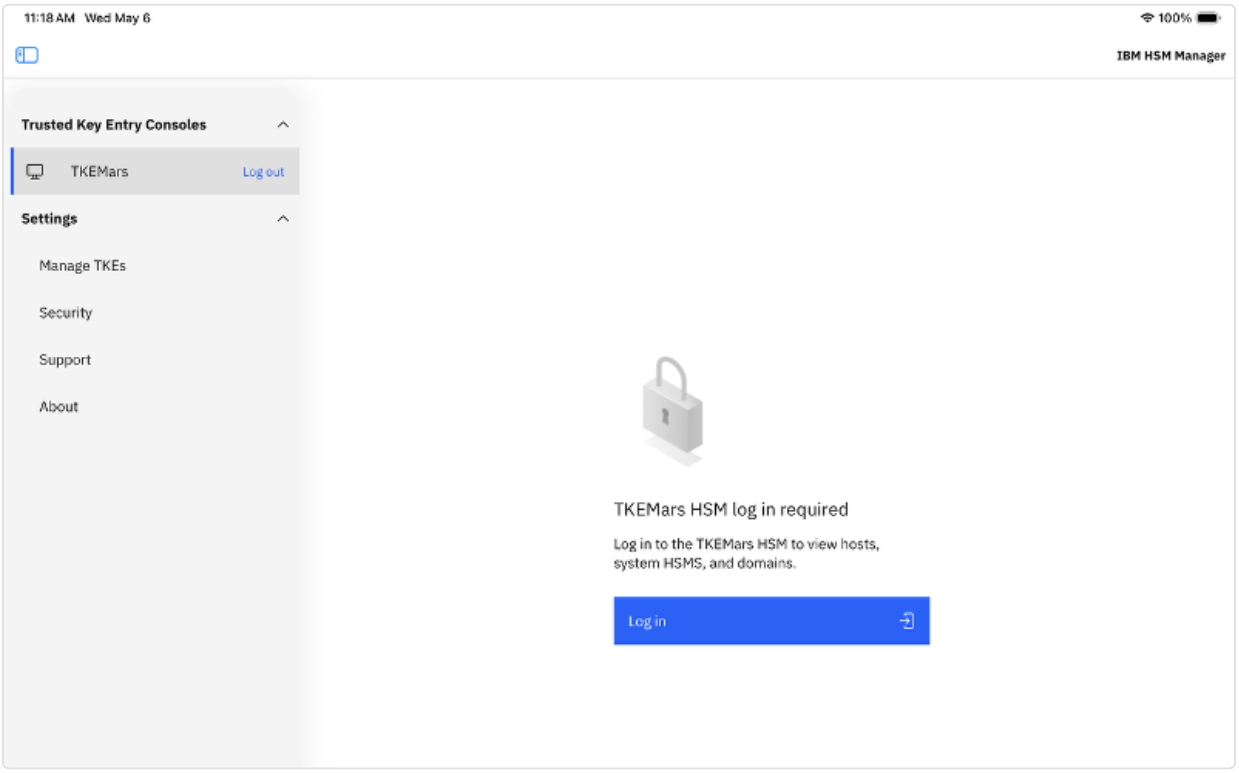

Figure 3 TKE Login

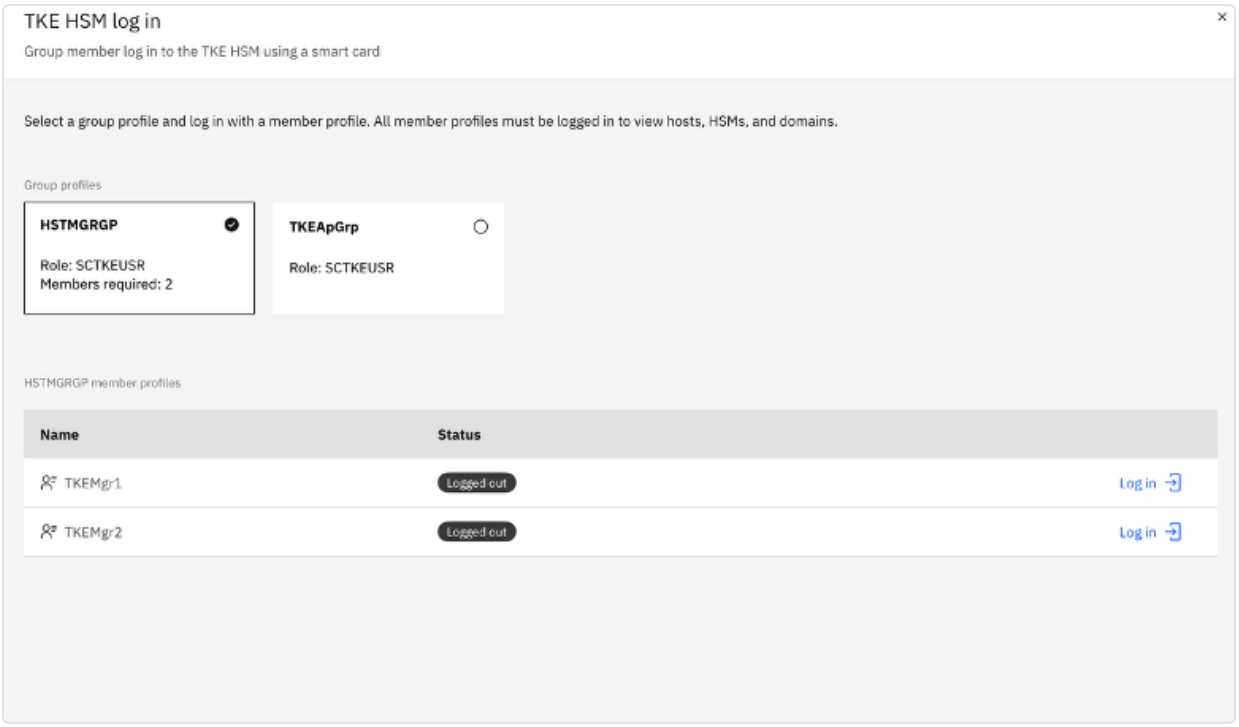

Figure 4 TKE Admin

a. Tap the Log in button for the TKE.

b. Select the appropriate group profile to view its members.

c. Security Admin 1: insert TKEMgr1 smart card → log in.

d. Security Admin 2: insert TKEMgr2 smart card → log in (may use a separate tablet or share the same tablet).

e. Once all members are logged in, HSM management is unlocked.

View Hosts, HSMs, and Domain Groups

IBM HSM Manager provides a centralized view of the hosts, HSMs, and domain groups that are available within your environment. After logging in to a host, you can navigate through its associated HSMs, inspect domain information, and review master key status details.

Individual host HSMs:

1. Tap the Hosts tab → tap a host from the list → tap Log in and enter host credentials.

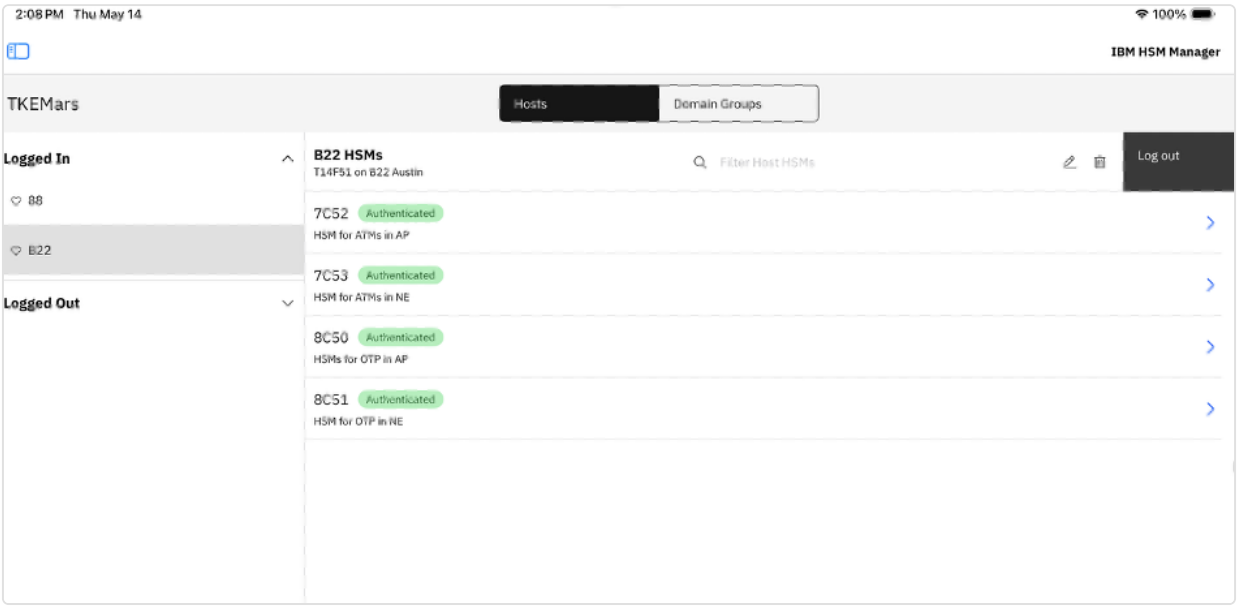

Figure 5 View Hosts

2. Review the HSMs listed for the host.

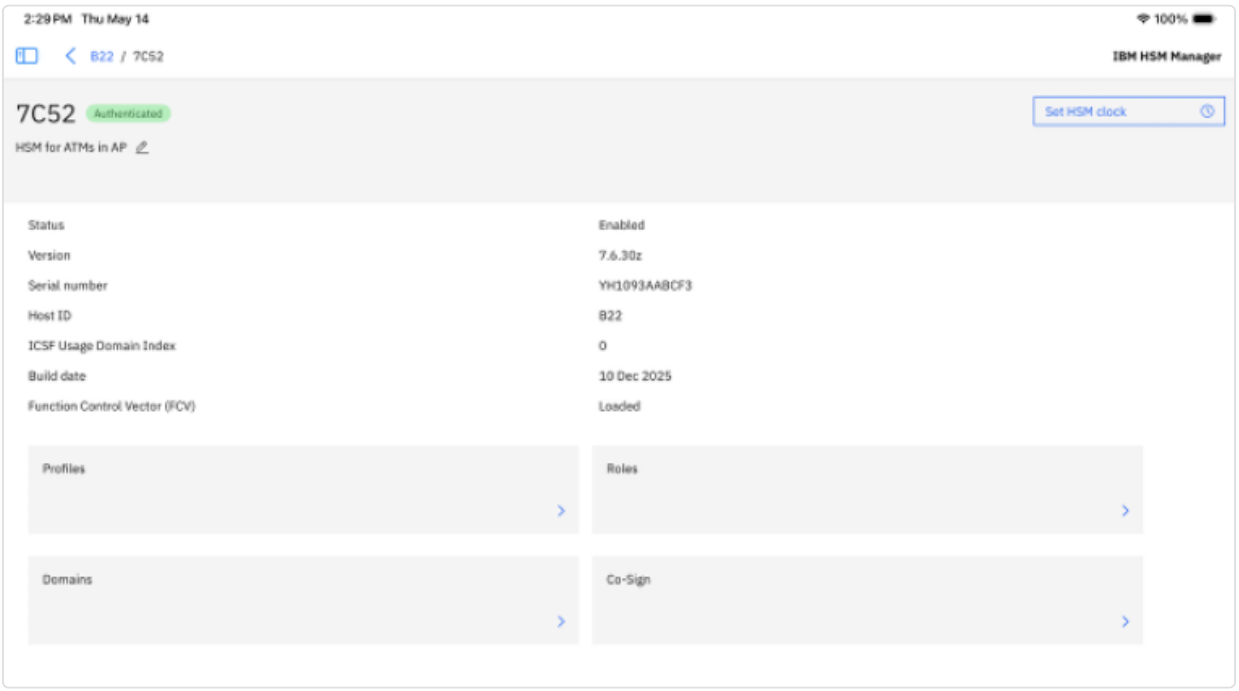

Figure 6 View HSM Details

3. Tap an HSM to view its details; tap Domains to view domains; tap a domain to see its details.

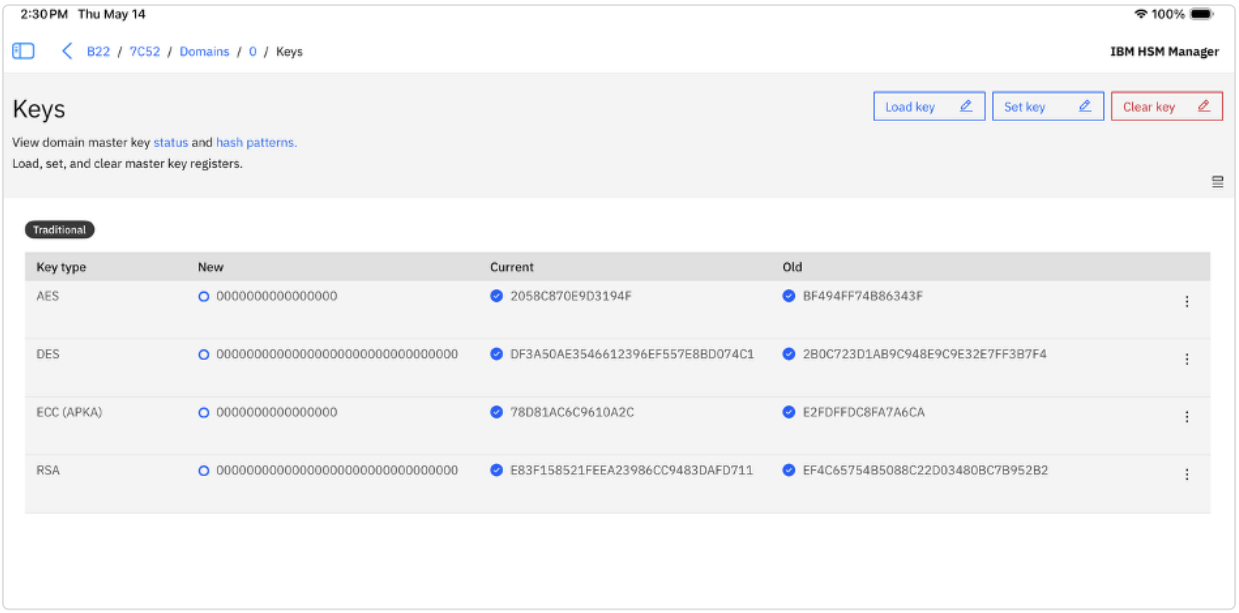

Figure 7 View MK Details

4. Tap Master keys to view domain master key register values and status.

Domain Groups:

1. Tap the Domain Groups tab → tap an existing group.
2. Tap Open group to view the primary HSM and all member HSMs and domains.
3. Tap the Domain card → Master keys card to review master key register state.

Load Master Keys Across a Domain Group

Domain groups allow master key operations to be applied simultaneously across all member HSMs and domains.

Security Admin 1 (first key part)

1. Open the domain group → tap Domain card → Master keys card → Load key.
2. Select total number of key parts (e.g., 3).
3. Choose to load the first master key part.
4. Insert the smart card containing the first key part; select the key parts for the New Master Key Registers.
5. Tap Load keys; confirm to clear registers if non-empty.
6. Enter signing PIN; verify first key parts are loaded.

Security Admin 2 (second and third key parts)

1. (Separate tablet) Open the domain group → navigate to the Keys view; or continue on the shared tablet.
2. Tap **Load keys** → select **second** key part → insert smart card → tap **Load keys** → enter PIN → verify.
3. Repeat for the **third/last** key part: select third part → insert smart card → tap **Load keys** → enter PIN → verify.

Final Verification

Both administrators confirm that New Master Key Registers are fully loaded across all domains.

Set Master Keys:

1. Tap Set key → select the master key types to set.

2. Sign with your smart card and PIN.

3. Confirm the operation; verify keys transferred from New to Current Master Key Register.

Summary

IBM HSM Manager modernizes HSM lifecycle management for IBM Z and LinuxONE by transforming a traditionally on-premises, co-location–dependent process into a fully remote, mobile-enabled operation — without compromising security. IBM HSM Manager supports the complete HSM management lifecycle:

- **Enable** — A TKE administrator enables the feature once on the TKE console.
- **Connect** — Security administrators add the TKE to the app and authenticate using smart cards.
- **View** — Administrators browse hosts, HSMs, domains, domain groups, and master key register state.
- **Configure** — New HSMs can be configured from initial state: create domain groups, IBM recommended roles, and profiles — all from the tablet.
- **Load Keys** — Master key parts held on separate smart cards are loaded across all domains in a group by administrators working from different geographic locations.
- **Set Keys** — Optionally promote loaded keys from the New to the Current Master Key Register.

Organizations using IBM Z or LinuxONE with distributed security administration teams stand to gain the most immediate value — eliminating the cost, delay, and scheduling risk associated with on-premises TKE console management.

Best Practices and Considerations

IBM HSM Manager extends Trusted Key Entry (TKE) capabilities to remote devices or platforms, enabling remote HSM management tasks that were traditionally performed only through physical console access. Because these operations affect cryptographic domains, master keys, and administrative control, organizations must adopt disciplined security and operational practices to maintain the same level of protection that TKE environments require.

This chapter provides guidance on security best practices, operational guidelines, and key considerations for deploying and managing IBM HSM Manager in production environments. The recommendations presented here reflect the principle that remote cryptographic administration must preserve the rigor and control expected for traditional TKE-based operations.

In this chapter, we discuss:

- Security best practices for access control, authentication, and governance
- Operational guidelines for environment readiness and master key management
- Key considerations for production deployment
- Training and rollout strategies

Security best practices

IBM HSM Manager extends the security foundation of TKE with additional layers of configurable protection for remote HSM administration. These capabilities include access controls, application authentication, TLS-based server authentication, and client-side user authentication with optional MFA, providing a defense-in-depth approach to securing HSM management operations.

Access control and enablement

The decision to enable IBM HSM Manager should be treated as a significant security control change, requiring formal approval and documentation. Organizations should approach enablement with the same discipline applied to other privileged access systems.

Key practices for access control include:

- Enable IBM HSM Manager only through controlled administrative processes with appropriate approval workflows
- Apply least-privilege principles from deployment start, granting access only to users with defined operational need
- Grant access only to users with approved roles and documented authorization
- Review user definitions before activation to confirm proper authorization and completion of required training
- Document enablement details comprehensively: who enabled the capability, when it was enabled, which systems are affected, and which users were granted access
- Treat enablement as a governed change subject to change management procedures for improved auditability

This structured approach ensures that IBM HSM Manager access is granted deliberately and that organizations maintain clear records of who has been authorized to perform remote HSM operations.

Strong authentication and multi-admin control

Multi-admin authentication is fundamental to secure cryptographic operations. IBM HSM Manager preserves this requirement while enabling remote access, ensuring that critical operations cannot be performed by a single individual.

Organizations should implement the following authentication controls:

- Require strong authentication and multi-admin participation for all sensitive operations
- Use multi-admin smart card authentication for master key operations and domain configuration changes
- Maintain separation of duties when introducing IBM HSM Manager to existing TKE environments
- Keep Admin1 and Admin2 roles distinct, with different individuals assigned to each role
- Distribute approval, execution, and audit responsibilities across different individuals to prevent concentration of control

These controls ensure that the security model remains intact even as the operational model becomes more flexible. No single administrator should have the ability to compromise the HSM environment, regardless of whether operations are performed locally or remotely.

Role-based access control and profile governance

Role-based access control (RBAC) provides the framework for managing who can perform which operations within IBM HSM Manager. Proper profile governance ensures that access rights remain aligned with organizational needs and security policies.

Best practices for RBAC implementation include:

- Implement RBAC reflecting IBM-recommended patterns and organizational security models
- Map profiles carefully to roles, smart cards, and operational responsibilities, ensuring clear alignment between job functions and access rights
- Review profiles periodically to confirm continued alignment with current staffing and compliance requirements
- Remove dormant, obsolete, or overly broad profiles promptly to reduce unnecessary access
- Subject profile changes to formal review and approval processes, treating them as security-relevant modifications

Regular profile reviews help identify access creep and ensure that users retain only the permissions necessary for their current responsibilities. This ongoing governance is essential for maintaining a secure environment over time.

Smart card governance

Smart cards are security-critical assets that enable authentication and authorization for sensitive HSM operations. Organizations must manage these physical tokens with the same care applied to other high-value security credentials.

Comprehensive smart card governance includes:

- Manage smart cards as security-critical assets with formal lifecycle controls
- Assign dedicated cards according to role and responsibility, avoiding shared assignments
- Avoid shared or informally reassigned cards that can obscure accountability
- Establish lifecycle controls covering issuance, activation, custody, replacement, suspension, and revocation
- Handle lost, damaged, or compromised cards through documented procedures that include immediate suspension and investigation
- Maintain accurate inventory and ownership records linking each card to a specific individual and role
- Reconcile assigned cards against active users periodically to identify discrepancies

Smart card governance failures can undermine the entire security model. Organizations should treat smart card management as a critical security process requiring ongoing attention and periodic audit.

Secure remote operations

Remote administration introduces network dependencies and endpoint security considerations that do not exist in traditional console-based TKE operations. Organizations must ensure that remote access channels are properly secured and monitored.

Key practices for secure remote operations include:

- Permit remote administration only within trusted, controlled connectivity models that have been explicitly approved
- Protect, monitor, and limit communication paths to approved network segments, preventing unauthorized network access
- Use only supported tablets, card readers, adapters, and operating system levels as prescribed by IBM documentation
- Enroll devices in enterprise device management systems where possible to enforce security policies and maintain visibility
- Protect devices with strong local authentication mechanisms and ensure current security updates are applied
- Govern remote access as a privileged administrative channel subject to the same controls as other high-risk access methods

Network segmentation, monitoring, and device management are essential components of a secure remote administration model. Organizations should not assume that smart card authentication alone provides sufficient protection for remote operations.

Audit, accountability, and change management

Maintaining clear audit trails and accountability is essential for both security and compliance. Organizations must be able to demonstrate who performed which operations, when they were performed, and under what authority.

Audit and accountability practices include:

- Maintain traceability to named individuals, approved roles, and documented intent for all administrative actions
- Log enablement events, profile changes, smart card assignments, and sensitive operations comprehensively
- Introduce administrative changes through formal change management procedures that include review and approval
- Review planned changes for security impact before implementation, considering both direct and indirect effects
- Validate post-change that security controls remain effective and that no unintended access has been created
- Conduct periodic audits focusing on privileged access, separation of duties, and policy alignment

These practices ensure that organizations can reconstruct the history of administrative actions and demonstrate compliance with security policies and regulatory requirements. Audit capabilities are particularly important in environments subject to external oversight or certification requirements.

Operational guidelines

Operational discipline is essential to prevent failed procedures, inconsistent key states, or unintended impact across managed domains. The following guidelines help organizations maintain reliable and predictable HSM operations.

Environment readiness

Successful deployment of IBM HSM Manager requires careful validation of the technical environment. Organizations should verify compatibility and functionality before introducing the solution into production.

Environment readiness activities include:

- Validate TKE version, tablet operating system, hardware specifications, and dependencies before rollout
- Verify compatibility of card readers, adapters, connectivity components, and prerequisite software
- Confirm that tablets can reliably reach TKE components with acceptable latency and stability
- Establish fallback procedures for connectivity interruptions or device failures
- Conduct pilot or preproduction validation before production deployment to identify and resolve issues

Thorough environment validation reduces the risk of operational failures during critical procedures. Organizations should not assume that all components will work together without explicit testing.

Domain group planning and usage

Domain groups enable administrators to manage multiple HSMs and domains together, applying configuration changes consistently across systems. However, this capability requires careful planning to avoid unintended consequences.

Best practices for domain group management include:

- Define domain groups carefully and document their intended purpose and membership
- Verify group membership and confirm the primary domain role before performing group-level operations
- Ensure administrators understand which actions propagate to group members and which affect only individual domains
- Assess downstream effects before making group-level changes, considering dependencies and operational impact
- Align domain group design with organizational boundaries and change control practices to maintain clear ownership

Domain groups are powerful tools for managing complex environments, but they can also amplify the impact of configuration errors. Organizations should approach domain group operations with appropriate caution and validation.

Master key management discipline

Master key operations are among the most sensitive procedures in HSM management. These operations require careful execution and validation to ensure that keys are loaded correctly and consistently across all affected systems.

Master key management practices include:

- Treat master key operations as tightly controlled procedures with explicit checkpoints and validation steps
- Load key parts according to established dual-control practices, ensuring that no single individual has access to complete keys
- Validate each key part entry carefully before proceeding to the next step
- Perform final verification after the complete load process to confirm that the intended key has been loaded
- Trigger a controlled pause for any discrepancy, interruption, or uncertainty, investigating before proceeding

- Maintain consistency across ICSF, Linux, and IBM HSM Manager platforms to ensure interoperability

> **Attention:** Master key errors can have severe consequences, potentially rendering encrypted data inaccessible or compromising cryptographic operations. Organizations should never rush master key procedures or skip validation steps.

Operational validation before sensitive actions

Before performing any sensitive operation, administrators should verify that all prerequisites are met and that the environment is in the expected state. This validation reduces the risk of errors and unintended consequences.

Pre-operation validation should include:

- Confirm all prerequisites before performing sensitive operations, checking both technical and procedural requirements
- Verify user authentication status, HSM visibility, domain availability, and key state
- Confirm readiness of required peer administrators for multi-admin operations
- Verify correct target environment selection to prevent operations in the wrong system
- Use documented checklists for high-impact procedures to ensure consistent execution

Systematic validation helps prevent common errors such as operating on the wrong domain, attempting operations without proper authentication, or proceeding when required administrators are unavailable.

Training, rollout, and operational readiness

Effective use of IBM HSM Manager requires that administrators understand both the technical procedures and the security implications of their actions. Organizations should invest in comprehensive training before production deployment.

Training and rollout best practices include:

- Provide administrator training before production introduction, covering both technical and security aspects
- Cover authentication workflows, smart card handling, domain groups, master key procedures, and failure scenarios in training
- Use phased rollout: demonstration environments → limited administrative group → full production deployment
- Prepare incident response procedures for failed authentication, lost cards, connectivity issues, and misconfigurations
- Establish clear escalation paths for situations that require additional expertise or approval

Phased rollout allows organizations to identify and resolve issues in controlled environments before they affect production operations. This approach reduces risk and builds administrator confidence.

Key considerations for production use

Production use of IBM HSM Manager introduces dependencies and complexities that require deliberate management. Organizations should understand these considerations before committing to production deployment.

Multi-user authentication dependencies

Multi-admin authentication provides essential security controls but can also introduce operational delays. Organizations must balance security requirements with operational responsiveness.

Key considerations include:

- **Availability requirements**: Multi-user authentication can delay operations if required administrators are unavailable due to time zones, schedules, or other commitments

- **Coordination overhead**: Coordinating multiple administrators for routine operations increases complexity and communication requirements
- **Emergency procedures**: Organizations need clear procedures for situations requiring urgent action when normal multi-admin workflows cannot be completed quickly

Organizations should establish clear expectations about response times and availability for administrators with critical roles.

Network stability and connectivity

Remote operations depend on reliable network connectivity between tablets and TKE components. Network instability can interrupt workflows and create operational uncertainty.

Connectivity considerations include:

- **Network reliability**: Instability between tablets and TKE can interrupt workflows, potentially leaving operations in incomplete states
- **Latency sensitivity**: Some operations may be sensitive to network latency, affecting usability and reliability
- **Fallback procedures**: Organizations need documented procedures for completing operations when network connectivity is lost

Network monitoring and capacity planning are essential for maintaining reliable remote operations.

Hardware compatibility and availability

IBM HSM Manager requires specific hardware components that must be available when needed. Organizations should ensure that compatible devices are readily accessible.

Hardware considerations include:

- **Device compatibility**: Supported tablets, card readers, and adapters must be available when needed
- **Spare equipment**: Organizations should maintain spare devices to handle failures or damage
- **Procurement lead times**: Replacement hardware may have significant lead times, requiring advance planning

Hardware failures should not prevent critical operations. Organizations should maintain sufficient spare equipment to handle common failure scenarios.

Operational complexity and error risk

Multi-step procedures involving multiple administrators increase the risk of errors. Organizations should implement controls to reduce this risk.

Complexity considerations include:

- **Procedure complexity**: Multi-step procedures with multiple administrators increase error risk
- **Documentation requirements**: Complex procedures require clear, detailed documentation
- **Validation checkpoints**: Procedures should include validation checkpoints to catch errors early

Simplifying procedures where possible and providing clear documentation reduces error risk.

Configuration accuracy and access control

Incorrect role or profile configuration can either block authorized work or create security exposures. Organizations must maintain accurate configuration and validate changes carefully.

Configuration considerations include:

- **Configuration accuracy**: Incorrect role or profile configuration can block authorized work or create unintended access

- **Change validation**: Configuration changes should be validated in test environments before production deployment
- **Regular reviews**: Periodic configuration reviews help identify and correct errors or drift

Configuration management discipline is essential for maintaining both security and operational effectiveness.

Balancing usability and control

Organizations should balance usability and control carefully when deploying IBM HSM Manager. The solution provides significant operational flexibility, but this flexibility must be governed appropriately to maintain security.

Deploy IBM HSM Manager only when governance, training, auditability, and operational readiness are mature enough to support it. Organizations that lack strong change management, audit capabilities, or administrator training should address these foundational requirements before introducing remote HSM management.

Summary

IBM HSM Manager requires the same rigor governing all high-value cryptographic administration. Strong authentication, separation of duties, least-privilege access, and disciplined smart card governance form the foundation of secure operations. Equally important are environment validation, careful domain group planning, controlled master key procedures, and structured administrator training.

By combining strong governance with repeatable operational discipline, organizations can use IBM HSM Manager effectively while reducing security and operational risk. The practices outlined in this chapter provide a framework for deploying and managing the solution in a way that preserves the trusted security model while enabling the operational flexibility that modern enterprises require.

Organizations should view these best practices not as optional recommendations but as essential requirements for maintaining the security and reliability of their cryptographic infrastructure. The consequences of inadequate governance or operational discipline in HSM management can be severe, affecting both security posture and business operations.

Summary

IBM HSM Manager represents a significant evolution in Hardware Security Module management for enterprise environments. Introduced with the IBM zNext Early Support Program, this solution extends the proven Trusted Key Entry (TKE) model by enabling secure remote management capabilities while preserving the hardware-based security controls that organizations depend on.

Traditionally, TKE operations required administrators to physically access secure environments with smart cards to perform critical HSM management tasks. IBM HSM Manager modernizes this approach by allowing the same operations—including HSM configuration, domain management, and master key operations—to be carried out remotely via a secure application. This transformation addresses the operational challenges of distributed teams and geographically dispersed infrastructure without compromising the trusted security model.

The solution supports the complete HSM lifecycle, from initial enablement and authentication through domain management and multi-party key operations. By maintaining the same smart card-based authentication model and multi-admin control requirements, IBM HSM Manager ensures that security governance remains intact while significantly improving operational flexibility.

Key takeaways

IBM HSM Manager delivers several fundamental capabilities that transform how organizations manage their cryptographic infrastructure:

Remote TKE operations without compromising security
HSMs can now be managed remotely using the same smart card-based authentication model that TKE users have relied on for years. This eliminates the need for physical presence at TKE consoles while maintaining hardware-based security controls. Administrators can perform critical operations from secure locations without traveling to data centers, reducing operational delays and improving response times for time-sensitive tasks.

Multi-admin control remains central
Critical operations such as master key loading continue to require multiple administrators and smart cards, enforcing strong security practices and separation of duties. This multi-party authentication workflow ensures that no single individual can compromise the security of the HSM environment. The solution preserves the principle that sensitive cryptographic operations require coordinated action from multiple authorized parties, maintaining the governance model that enterprises require for compliance and risk management.

End-to-end HSM lifecycle support
From initial setup and enablement through master key loading and ongoing configuration management, all major HSM workflows are supported within the IBM HSM Manager framework. Organizations can manage the complete lifecycle of their cryptographic infrastructure through a unified interface, reducing the complexity of maintaining multiple tools and processes. This comprehensive coverage ensures consistency in how HSMs are managed across different operational phases.

Domain group-based management
Multiple HSMs and cryptographic domains can be grouped and operated together, with administrative actions applied consistently across systems. This capability is particularly valuable in large-scale environments where maintaining configuration consistency across numerous HSMs is critical. Domain grouping simplifies bulk operations while ensuring that security policies and configurations remain synchronized across the infrastructure.

Role-based access control built-in Roles and profiles define who can perform which operations, ensuring controlled access and governance throughout the HSM management lifecycle. This structured approach to access control enables organizations to implement least-privilege principles and maintain clear audit trails of administrative actions. Role definitions can be aligned with organizational responsibilities, ensuring that access rights match operational requirements and compliance mandates.

Improved usability for distributed teams
Tablet-based access simplifies operations for teams working across multiple locations and time zones. Administrators can respond to operational requirements without being constrained by physical location, improving service delivery and reducing the coordination overhead associated with traditional TKE operations. This flexibility is particularly valuable for organizations with global operations or those implementing follow-the-sun support models.

Value recap

IBM HSM Manager delivers measurable value across multiple dimensions of enterprise operations:

Operational efficiency
The solution removes the need for physical presence at TKE consoles, fundamentally changing how HSM management tasks are executed. This eliminates travel requirements, reduces coordination effort between teams, and removes delays in executing secure operations. Organizations can respond more quickly to business requirements, reduce the time needed to complete routine maintenance tasks, and improve overall service delivery. The ability to perform operations remotely also reduces the operational cost associated with maintaining secure physical access to TKE environments.

Security continuity
IBM HSM Manager preserves hardware-based security controls while enabling remote operations. The solution

maintains multi-party authentication requirements and split-key principles that are fundamental to secure cryptographic operations. Organizations can modernize their operational model without introducing new security risks or compromising established governance frameworks. The same security controls that protected on-premises TKE operations continue to protect remote operations, ensuring that the transition to remote management does not weaken the security posture.

Scalability
Centralized management of multiple HSMs and domains enables organizations to scale their cryptographic infrastructure more effectively. As environments grow and become more distributed, IBM HSM Manager provides the tools needed to maintain operational control without proportionally increasing administrative overhead. Domain grouping and bulk operation capabilities ensure that management complexity does not increase linearly with infrastructure size. This scalability is essential for organizations experiencing growth or those consolidating cryptographic operations across multiple business units.

Governance and control
Role-based access control and structured workflows improve operational discipline and ensure that administrative actions align with organizational policies. Domain grouping simplifies the management of complex infrastructures while maintaining clear accountability for configuration changes. The solution provides the audit trails and access controls that compliance frameworks require, making it easier to demonstrate adherence to security policies and regulatory requirements. Organizations can implement consistent governance practices across their entire HSM infrastructure, regardless of physical location or operational scale.

Conclusion

IBM HSM Manager brings a more flexible operating model to TKE environments while keeping the same trusted security foundation that organizations depend on. By enabling remote operations without compromising security controls, the solution addresses the operational challenges of modern distributed enterprises. Organizations can improve efficiency, reduce operational costs, and enhance service delivery while maintaining the rigorous security governance that cryptographic operations require.

The combination of remote management capabilities, multi-admin control, and comprehensive lifecycle support positions IBM HSM Manager as a strategic enabler for organizations seeking to modernize their cryptographic infrastructure management. As enterprises continue to evolve toward more distributed operational models, IBM HSM Manager provides the foundation for secure, efficient, and scalable HSM management that meets both current and future requirements.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM® in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 United States of America

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. The following terms are trademarks of IBM in the United States, other countries, or both:

IBM®, IBM Bob™, IBM Z®, RACF®, Redbooks®, z/OS®, z/VM®

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

For information about trademarks, service marks, and other intellectual property notices, see IBM's Copyright and Trademark Information page: https://www.ibm.com/legal/copyright-trademark.

AI Attribution

This work was primarily human-created. AI was used to make stylistic edits, such as changes to structure, wording, and clarity. AI was used to make content edits, such as changes to scope, information, and ideas. AI was prompted for its contributions, or AI assistance was enabled. AI-generated content was reviewed and approved. The following model(s) or application(s) were used: IBM Bob™, Microsoft Copilot, and Google Gemini.