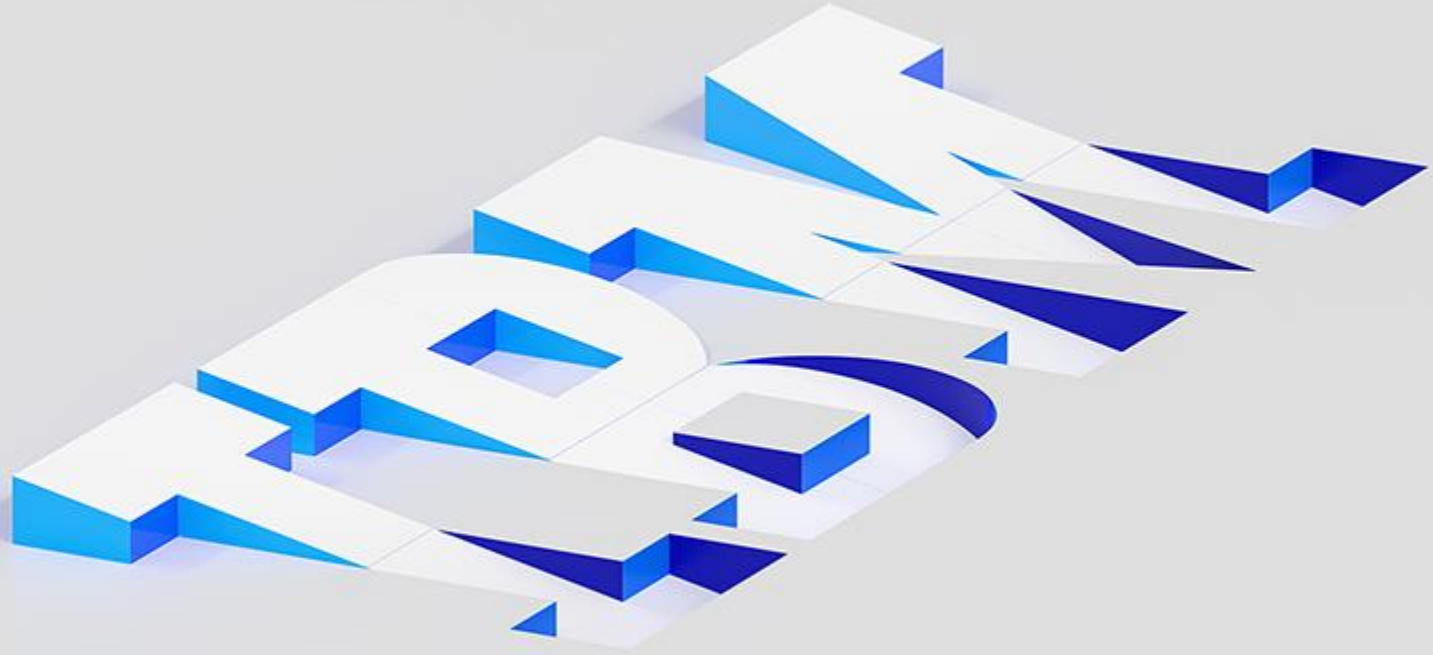
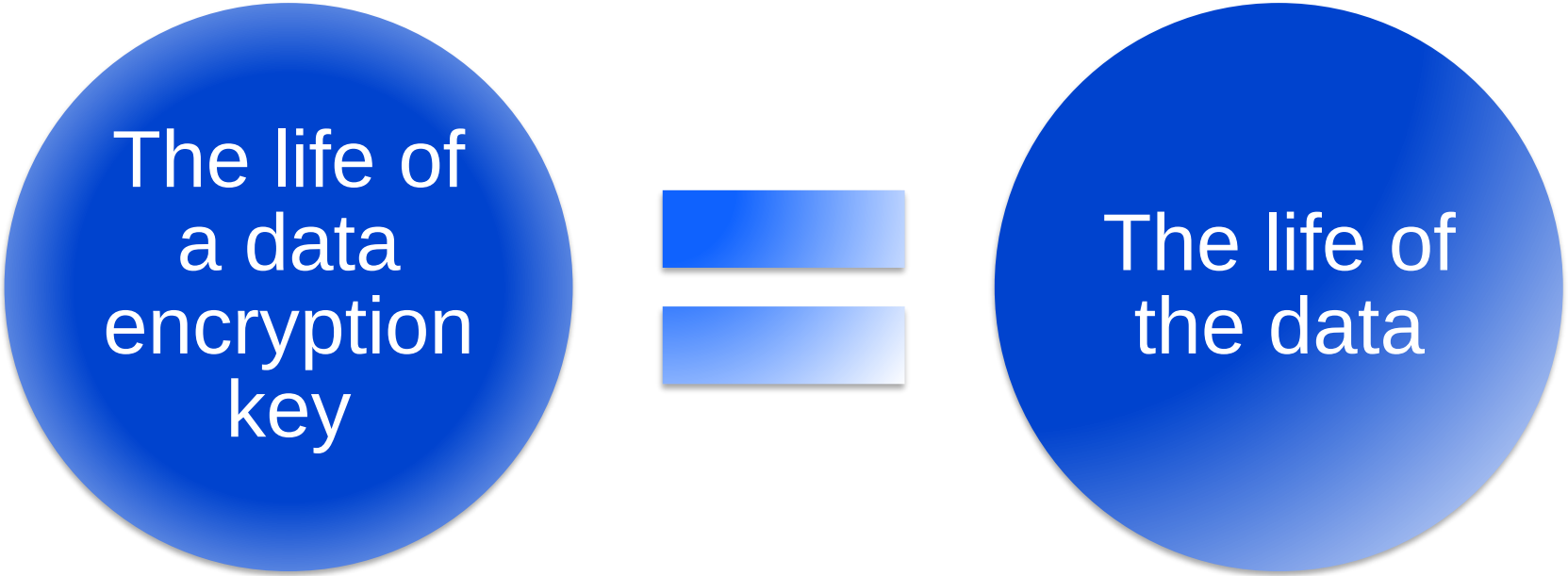
Key Management Strategy



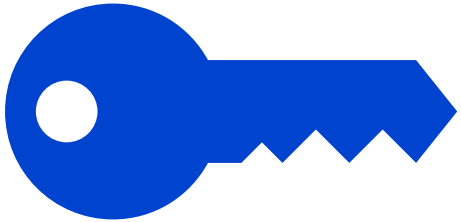
Eysha Shirrine Powers
IBM Senior Technical Staff Member
Chief Architect, IBM Z Cryptographic Portfolio
eysha@us.ibm.com

What is the life of a cryptographic key?



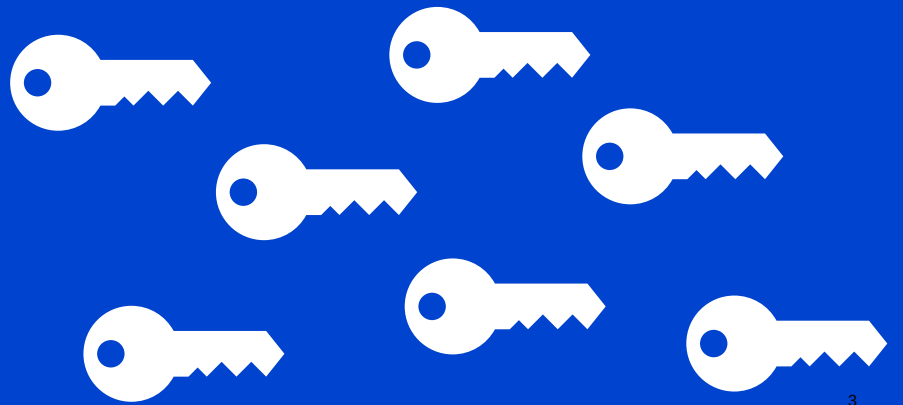
Master Keys

- Master keys are used only to encipher and decipher keys.
- Master keys are stored in secure, tamper responding hardware.
- Master keys should be changed periodically.



Operational Keys

- Operational keys are used in various cryptographic operations (e.g. encryption).
- Operational keys may be stored in a key store (e.g. data set, file, database) or returned back to the calling application.
- Operational keys encrypted by a master key are considered secure keys



Data Encryption Requires Cryptographic Keys

Planning

- Number of Keys
- Key Label Naming Conventions
- Key Access Control
- Key Life Cycle & Rotation
- Key Backup and Recovery
- Key Management Tools

Preparing

- Number of Crypto Express adapters
- Key Data Set format
- Installation options
- Master Key load
- Configuration verification

Deploying

- Key Generation
- Key Assignment to data sets
- Key Access Control
- Key Rotation

Auditing

- Key Access Control
- Key Life Cycle Transitions
- Key Usage Operations
- Crypto Engine, Service and Algorithm Usage
- Crypto Hardware Activity

Integrated Cryptographic Services Facility (ICSF)

Supports Master Keys and Operational Keys*

** ICSF can load only CCA Master Keys*

Trusted Key Entry (TKE) Workstation

Supports Master Keys and limited Operational Keys

Enterprise Key Management Foundation (EKMF)

Supports Operational Keys

Security Key Lifecycle Manager (SKLM)*

Supports Operational Keys for self-encrypting devices only (i.e. disk, tape, flash).

Tools for Master Key Management

Recommended

Trusted Key Entry (TKE) Workstation

- **Most secure**; Dual controls; Separation of duties; Key material is not displayed
- Applicable for initialization of ICSF Key Data Sets (i.e. key stores) and Crypto Express adapters
- Applicable for master key rotation
- Required for EP11 Master Key management & PCI-HSM Master Key management
- Load and administer master keys across multiple IBM Z systems and geographies; Load master keys for inactive LPARs
- Separate, priced product

Trusted Key Entry (TKE) Workstation (Tower or 1U)

Smart Cards

Smart Card Readers

Default

z/OS ICSF Master Key Entry Panels

- **Less secure than TKE**; Separation of duties; Key material is displayed on panel
- Applicable for initialization of ICSF Key Data Sets (i.e. key stores) and Crypto Express adapters
- Applicable for master key rotation
- Included with z/OS and ICSF

Discouraged

z/OS ICSF Pass Phrase Initialization (PPINIT) Panel

- **Least secure**; No separation of duties
- Applicable for initialization of ICSF Key Data Sets (i.e. key stores) and Crypto Express adapters
- **NOT** applicable for master key rotation
- Included with z/OS and ICSF

Tools for Operational Key Management (1 of 2)

Recommended

Enterprise Key Management Foundation (EKMF) Web

- **Secure key management for z/OS Data Set Encryption**; Dual controls; Separation of duties
- Applicable to z/OS Data Set Encryption and the management of AES DATA and AES CIPHER keys
- Generate and manage operational keys across multiple IBM Z systems and geographies
- Supports key distribution to z/OS ICSF key data sets which may be protected with different Master Keys
- Keys reside in a Db2 repository separate from z/OS key stores and key rings; Keys deleted from z/OS can be restored using EKMF
- View a data set dashboard showing encrypted data sets
- Separate, priced SW product (PID: 5655-EKM)

Recommended

Enterprise Key Management Foundation (EKMF) Workstation

- **Secure key management for Multi-purpose Crypto Function**; Dual controls; Separation of duties; Smart cards
- Multi-purpose; Applicable to application, database, data set, storage, network encryption, financial systems (e.g. ATMs and POS terminals)
- Generate and manage operational keys across multiple IBM Z systems and geographies; generate and manage certificates
- Supports key distribution to z/OS ICSF key data sets and SAF key rings which may be protected with different Master Keys
- Supports MQ Advanced Message Security, WAS Security, Certificate Management Protocol to Certificate Authorities
- Keys reside in a Db2 repository separate from z/OS key stores and key rings; Keys deleted from z/OS can be restored using EKMF
- Separate, priced offering

Tools for Operational Key Management (2 of 2)

Using z/OS Integrated Cryptographic Services Facility (ICSF) application programming interfaces and utilities

Default

- **Secured by SAF resources**
- Multi-purpose; Applicable to application, database, data set, storage and network encryption
- Generate and manage operational keys for a single ICSF instance and/or multiple ICSF instances shared in a sysplex
- Included with z/OS

Using the Trusted Key Entry (TKE) Workstation

Limited

- **Secure key loading**; Dual controls; Separation of duties; Smart cards
- Multi-purpose; Applicable to application, database, data set, storage and network encryption
- Generate/import and load a limited number of operational keys
- No ability to manage keys after loading them into ICSF. Must use EKMF or ICSF for additional key management
- Separate, priced product

Using IBM Security Guardium Key Lifecycle Manager (SKLM → GKLM) commands and utilities

N/A

- **Not applicable to z/OS Data Set Encryption**
- Three versions:
  - GKLM 4.0 Traditional (for distributed systems):
    - Applicable to self-encrypting devices (e.g. disk, tape, flash) and Key Management Interoperability Protocol (KMIP) clients
    - Keys reside in a Db2 repository
  - GKLM 4.1 Container Edition:
    - Applicable to self-encrypting devices (e.g. disk, tape, flash) and Key Management Interoperability Protocol (KMIP) clients
    - Option 1: Keys reside in a Db2 repository encrypted by an SKLM generated key encrypting key
    - Option 2: Keys reside in a Db2 repository encrypted by an ICSF generated key encrypting key which is encrypted by a Crypto Express master key
  - SKLM 1.1 for z/OS:
    - Only applicable to self-encrypting devices (e.g. disk, tape, flash)
    - Keys reside in z/OS key stores and/or RACF key rings
- Separate, priced product

Key Management Activities

SEDs = Self-encrypting devices

	Activity	ICSF	TKE	EKMF Workstation	EKMF Web	GKLM
Authorization Tasks	SAF Authorization (CSFKEYS and CSFSERV)	YES	YES	YES	YES	GKLM for z/OS
	Key Auditing (master keys, operational keys)	YES	YES	OPERATIONAL KEYS	AES DATA & CIPHER KEYS	YES
Master Key Tasks	Master Key Entry	YES, PANELS	YES, SECURE	NO	NO	NO
	Master Key Change	YES, PANELS	YES, SECURE	NO	NO	NO
	Master Key Zeroize	NO, HMC / SE	YES	NO	NO	NO
Basic KDS Tasks	Operational Key Record Creation (and naming)	YES	NO	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
	Operational Key Record Update	YES	NO	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
	Operational Key Record Deletion	YES	NO	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
Basic Key Tasks	Operational Key Generation, Rekey	YES	LOAD ONLY	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
	Operational Key Import	YES	LOAD ONLY	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
	Operational Key Export	YES	NO	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
KDS Metadata Tasks	Operational Key Archival	YES	NO	NON-KDS,SECURE+	AES DATA & CIPHER KEYS	NO
	Operational Key Restore	YES	NO	NON-KDS,SECURE+	AES DATA & CIPHER KEYS	NO
	Operational Key Expiration	YES	NO	NON-KDS,SECURE+	AES DATA & CIPHER KEYS	NO
Recovery Tasks	Disaster Recovery (master keys, operational keys)	YES	YES	OPERATIONAL KEYS	AES DATA & CIPHER KEYS	SEDs

Roles and Responsibilities

Integrating encryption tasks into existing workflows in addition to defining roles and responsibilities is critical for success

- New tasks may be introduced into existing workflows
- Different parts of the organization may be working together for the first time
- Develop and test a repeatable process that can be made available to different applications and/or Lines Of Business

Who will be the master key officers?

- Security Team?
- ICSF Team?
- Management Team?

Who will be responsible for operational key generation?

- Centralized?
- Decentralized?

Who will be responsible for assigning keys to resources?

- Security admin?
- Storage admin?

Disaster Recovery Overview

Disaster Recovery systems must support the same cryptographic operations and key data sets as the primary system

Crypto Hardware

- CPACF
- Crypto Express
- TKE and/or EKMF Workstation

Crypto Middleware

- Key Data Set Availability
- ICSF Release Level

Performance

If your primary environment has newer hardware than the DR environment (e.g. z14 versus z13), performing the same crypto operations may be slower and more costly with respect to MIPS/MSUs.

Master Key Backup for Disaster Recovery

Existing master keys may need to be reloaded during hardware upgrades, for disaster recovery or when adding additional Crypto Express adapters

Backup TKE Smart Cards

Create backup TKE smart cards in multiple data centers for disaster recovery.

Backup to Removable Storage Media

Copy / paste master key material to a secure storage device (e.g. USB stick) or password locker. Easy to copy / paste the key material to the ICSF panels for re-entry.

Backup to Printed Document

Print screen to a document which can be stored in envelopes in a locked safe in a locked room. Cannot copy / paste to re-enter key material to ICSF panels.

Operational Key Backup for Disaster Recovery

Backing up z/OS key data sets ensures that the accidental or deliberate deletion or overwriting of an operational key is recoverable

Automatically with EKMF

EKMF can repopulate keys in z/OS key stores from its key repository in Db2.

Along with regular volume backups

If the DASD volume is corrupted, the entire volume can be restored from the backup

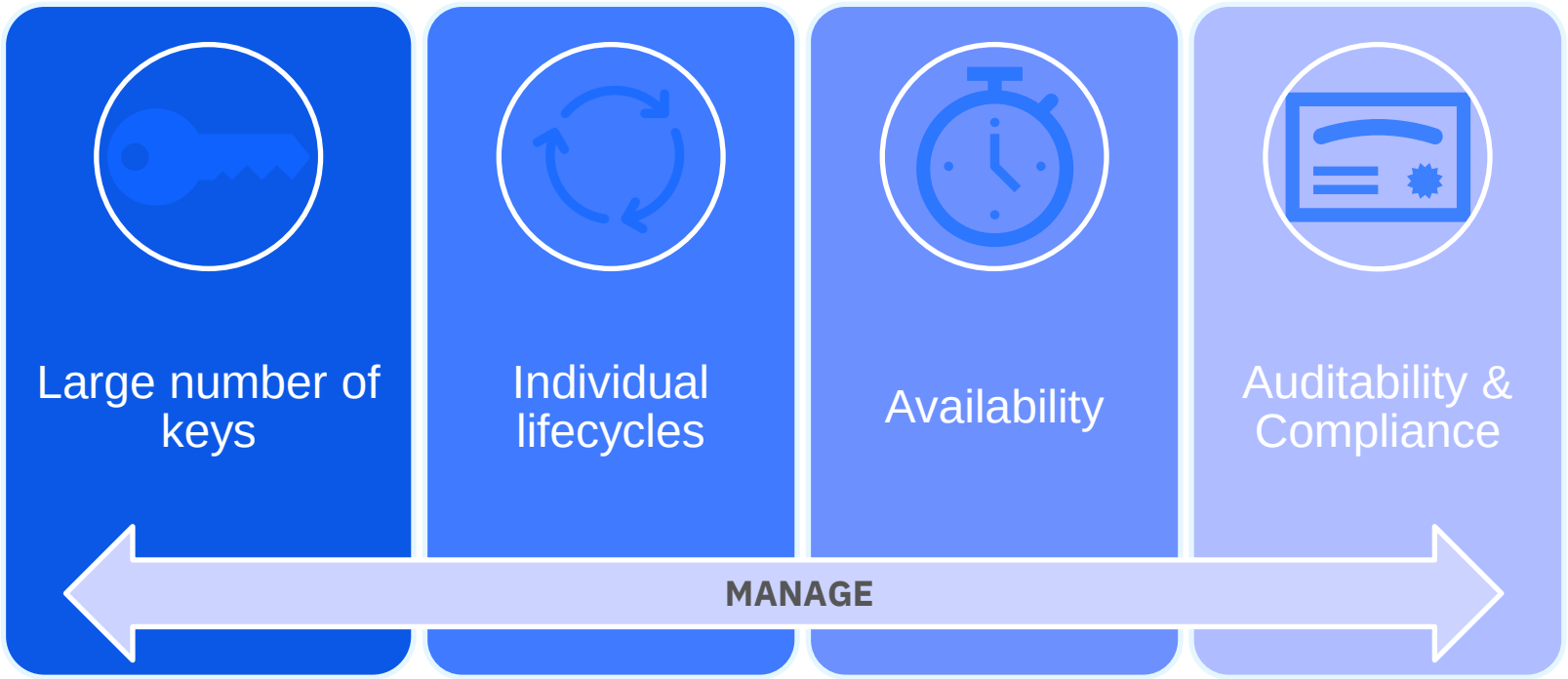
Before major key management operations

For example, backup key stores before performing unfamiliar or major key management operations (e.g. generating 1000s of keys)

After major key management operations

For example, backing up key stores after generating 1000s of keys ensures that the keys you have generated are recoverable if the key store is corrupted prior to the next regular volume backup.

The Key Management Challenge



Do I need an operational key management system for z/OS Data Set Encryption?

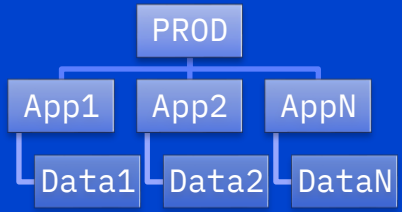
Do you want any of these:

- ✓ Easily manage a large number of keys
- ✓ Periodic, staggered key rotation
- ✓ Avoid manual distribution
- ✓ Easy overview of keys
- ✓ Keystore backup and recovery of individual keys
- ✓ Strong security and compliance for key management operations (e.g. dual control)
- ✓ Enforced key naming conventions

Downsides of < 10 keys

- ✗ Large amount of encrypted data affected if a single key is compromised
- ✗ Less granular control of how to separate people from data
- ✗ Difficult to stagger rotation periods for keys

You need good data set naming conventions




```
PROD.APP2.LOG.VER10
PROD.APP1.PAYROLL.VER7
```

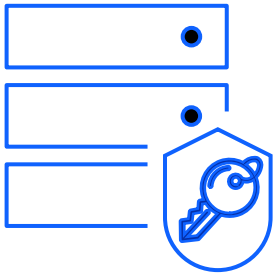
EKMF Web for Pervasive Encryption on IBM Z

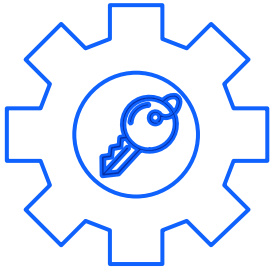
When implementing pervasive encryption, it is very important that a **robust key management system** is in place.

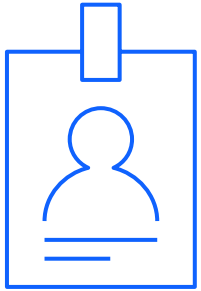
IBM Enterprise Key Management Foundation (EKMF) has a proven record of meeting the key management requirements you find in large financial companies like banks and card processors.

IBM offers EKMF Web for Pervasive Encryption that helps you **manage the keys involved in z/OS data set encryption**.

EKMF Web Capabilities







Single central key repository

- Stores metadata (activation dates, usage, etc.)
- Single-point backup and recovery

Key Management

- Generation based on policies
- According to NIST recommendations
- Using Hardware Security Modules (HSM)

Pervasive Encryption Support

- z/OS Data Set Encryption (DSE) dashboard
- Import and management of existing z/OS DSE keys
- Central support for multiple z/OS systems

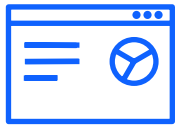
Security & Compliance

- Role-based access
- Dual control implemented using separation of privileges
- Audit logging

EKMF Components

Browser-based key generation & management for

- ✓ z/OS Data Set Encryption
- ✓ Cloud



Web Browser with EKMF Web

Secure room

EKMF Workstation

- ✓ Can be placed in secure room
- ✓ Utilizes IBM 4767 HSM
- ✓ Generate new keys by users authenticated with smart cards or automatically based on requests

Central EKMF repository

- ✓ Contains keys and metadata for all cryptographic keys produced by EKMF
- ✓ Easy backup and recovery of key material

Cloud key stores

Hardware Security Modules

IBM Crypto Express

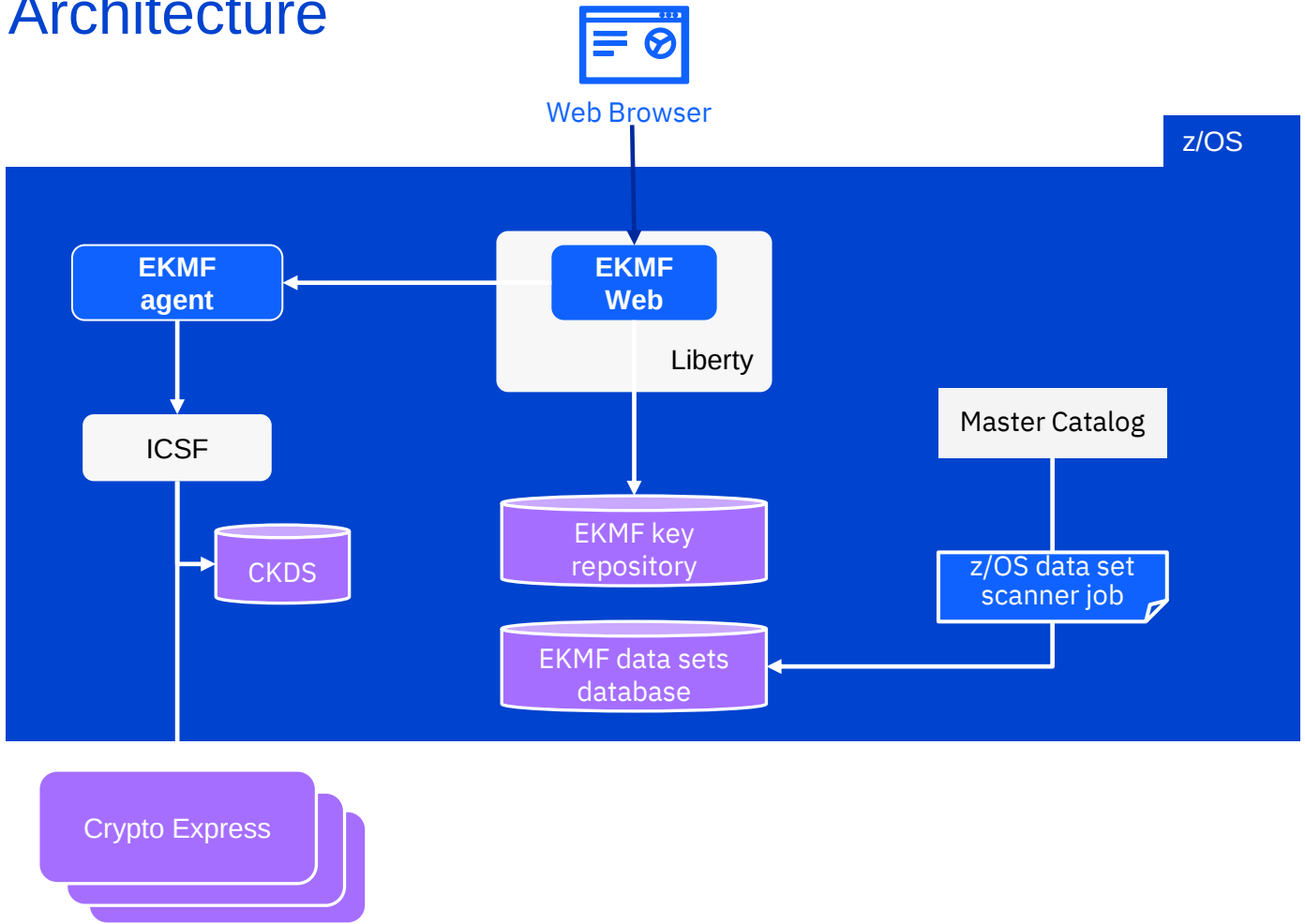
IBM 476x

Custom

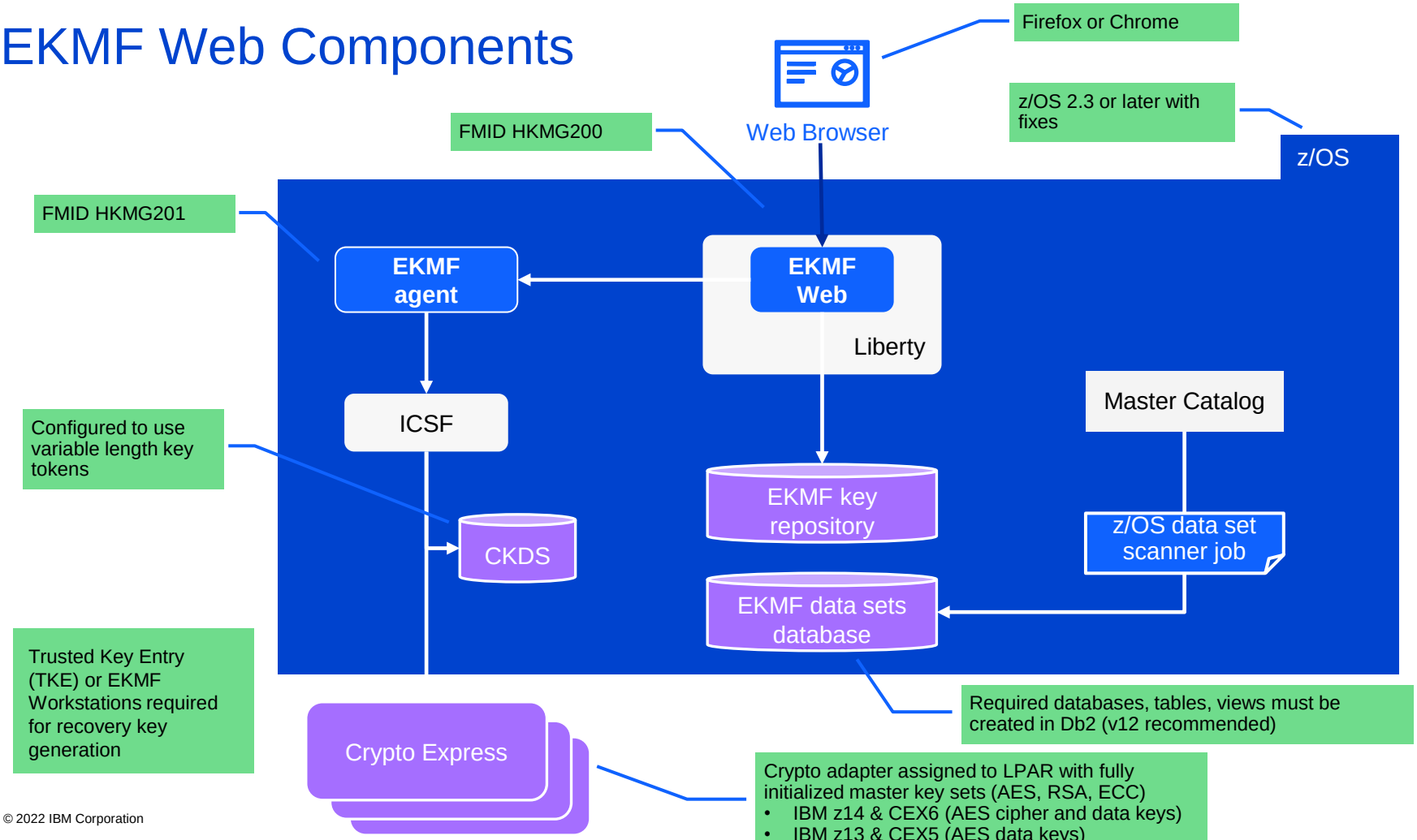
PCI

FIPS140-2 Level 4

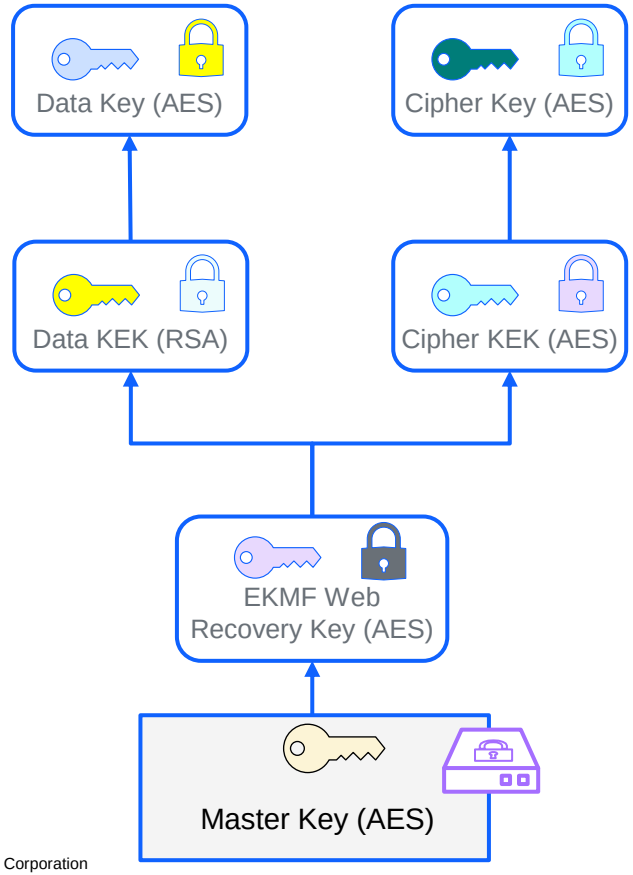
EKMF Web Architecture

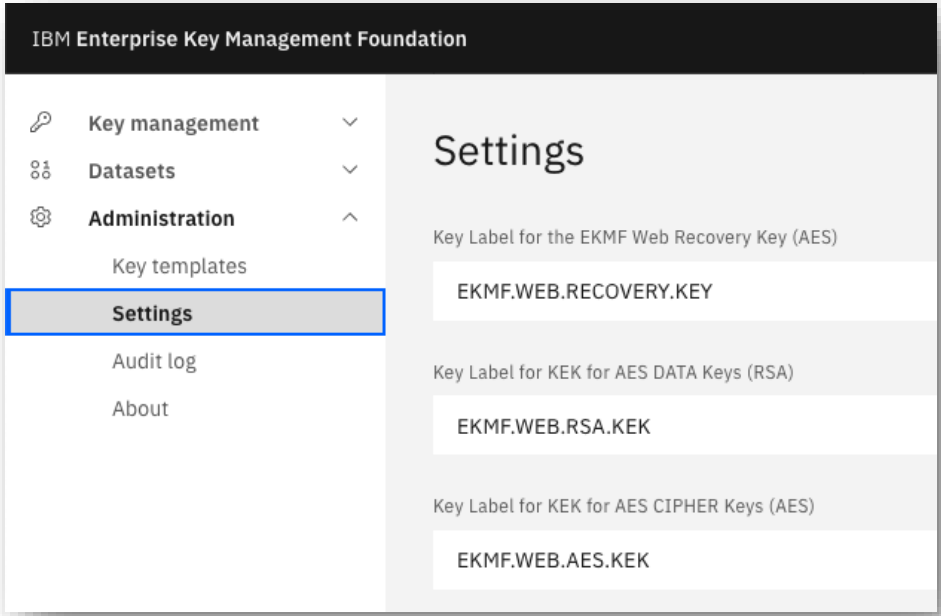


EKMF Web Components



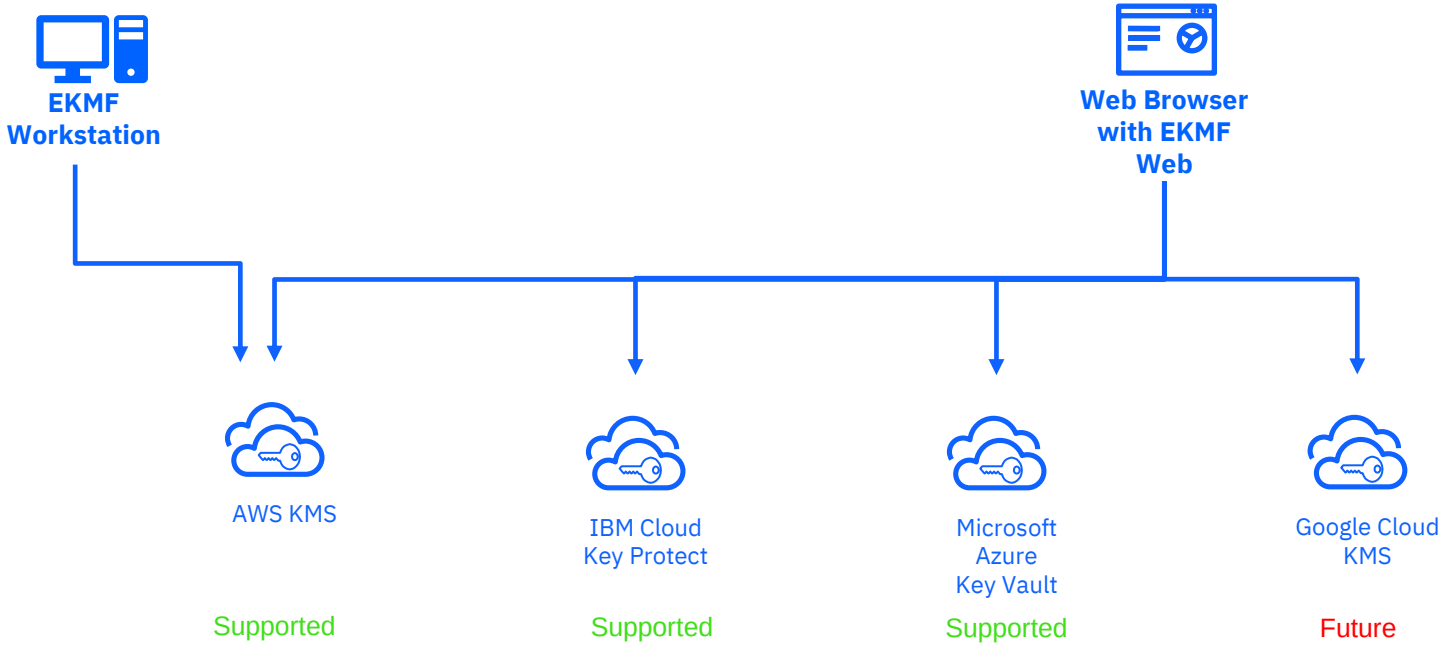
EKMF Web Key Hierarchy





EKMF Web Key Hierarchy

EKMF Web supports key distribution to IBM Key Protect, Amazon KMS and Azure



Remember: Key Management Activities

SEDs = Self-encrypting devices

	Activity	ICSF	TKE	EKMF Workstation	EKMF Web	GKLM
Authorization Tasks	SAF Authorization (CSFKEYS and CSFSERV)	YES	YES	YES	YES	GKLM for z/OS
	Key Auditing (master keys, operational keys)	YES	YES	OPERATIONAL KEYS	AES DATA & CIPHER KEYS	YES
Master Key Tasks	Master Key Entry	YES, PANELS	YES, SECURE	NO	NO	NO
	Master Key Change	YES, PANELS	YES, SECURE	NO	NO	NO
	Master Key Zeroize	NO, HMC / SE	YES	NO	NO	NO
Basic KDS Tasks	Operational Key Record Creation (and naming)	YES	NO	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
	Operational Key Record Update	YES	NO	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
	Operational Key Record Deletion	YES	NO	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
Basic Key Tasks	Operational Key Generation, Rekey	YES	LOAD ONLY	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
	Operational Key Import	YES	LOAD ONLY	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
	Operational Key Export	YES	NO	YES, SECURE+	AES DATA & CIPHER KEYS	SEDs
KDS Metadata Tasks	Operational Key Archival	YES	NO	NON-KDS,SECURE+	AES DATA & CIPHER KEYS	NO
	Operational Key Restore	YES	NO	NON-KDS,SECURE+	AES DATA & CIPHER KEYS	NO
	Operational Key Expiration	YES	NO	NON-KDS,SECURE+	AES DATA & CIPHER KEYS	NO
Recovery Tasks	Disaster Recovery (master keys, operational keys)	YES	YES	OPERATIONAL KEYS	AES DATA & CIPHER KEYS	SEDs