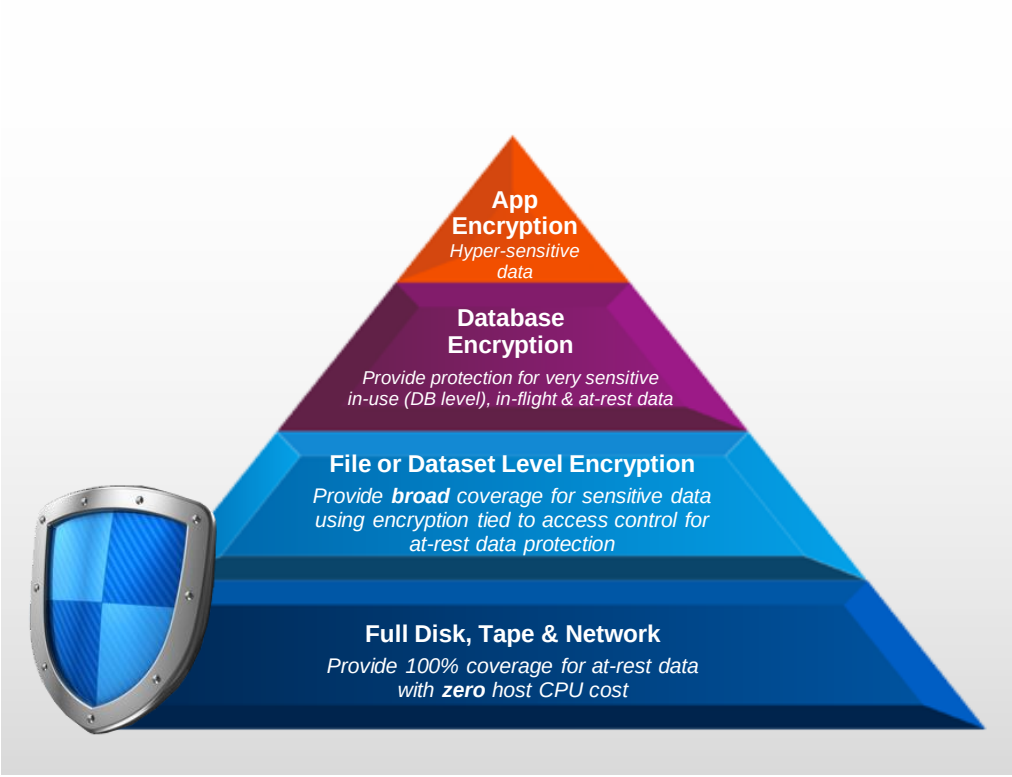
IBM Key Management im z/OS

Günter Weber, weberg@de.ibm.com

© 2022 IBM Corporation

Warum überhaupt Key-Management Lösungen ?

ENCRYPTION-Keys werden z.b. für Dataset Encryption benötigt…



Für Verschlüsselung auf jeder dieser Ebenen muss gewährleistet werden, dass:

- die “Keys” sicher gehandhabt werden bei der Erstellung und Verwendung,
- dass diese wieder hergestellt warden können, z.b. wenn ein sog. Keystore zerstört wurde
- die Key-Operationen wie erstellen, verteilen und ggf. löschen nachvollzogen werden können

Zu diesem Zweck gibt es Key-Management Lösungen wie die auf den folgenden Seiten besprochenen.

© 2022 IBM Corporation

Begriffe

Operational Keys : sind Keys mit denen Daten (z.b. Datsets auf z/OS) verschlüsselt werden

Master Keys* und Key Encryption Keys (KEKs): Schlüssel die verwendet werden (können), um Operational Keys zu verschlüssseln, damit diese zusätzlich gesichert sind, wenn:

- sie von ICSF** (auf z/OS) in sog. Key-Datasets (CKDS,PKDS,TKDS) gespeichert warden => Master Keys
- sie beim systeminternen Transport gesichert warden können (KEKs)

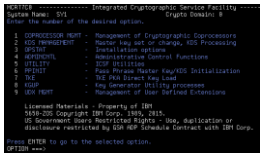
*Master Keys werden in Crypto Express Karten gespeichert (und verlassen diese nicht !)
*ICSF ist eine Software (Started Task) die:
- es ermöglicht innerhalb einer LPAR/Sysplex Keys zu managen
- aufgerufen werden kann, und Crypto-Funktionen (verschlüsseln/entschlüsseln von Daten) für andere (aufrufende) Softwarekomponenten zur Verfügung stellt.

© 2022 IBM Corporation

IBM Werkzeuge zum Keymanagement

Integrated Cryptographic Services Facility (ICSF)

ICSF provides callable services and utilities that generate, store, and manage keys, and also perform cryptographic operations.



Supports Master Keys and Operational Keys

Trusted Key Entry (TKE) Workstation

TKE securely manages multiple Cryptographic Coprocessors and keys on various generations of IBM Z from a single point of control.

Supports Master Keys and Operational Keys

Enterprise Key Management Foundation (EKMF)

EKMF securely manages keys and certificates for cryptographic coprocessors, hardware security modules (HSM), cryptographic software, ATMs, and point of sale terminals.

Supports Operational Keys

Guardium Key Lifecycle Manager (GKLM)

GKLM provides key storage, key serving and key lifecycle management for IBM and non-IBM storage solutions using the OASIS Key Management Interoperability Protocol (KMIP) and IBM Proprietary Protocol (IPP).

Supports Operational Keys
for Self Encrypting Devices (SEDs)

© 2022 IBM Corporation

Wann GKLM, wann EKMF ?

EKMF securely manages keys and certificates for cryptographic coprocessors, hardware security modules (HSM), cryptographic software, ATMs, and point of sale terminals.

Supports Operational Keys

EKMF gibt es nun in 2 Ausprägungen:

EKMF (Service-Angebot)
EKMF Web (Softwarelösung)

GKLM provides key storage, key serving and key lifecycle management for IBM and non-IBM storage solutions using the OASIS Key Management Interoperability Protocol (KMIP) and IBM Proprietary Protocol (IPP).

Supports Operational Keys
for Self Encrypting Devices (SEDs)

EKMF ist sinnvoll wenn der Kunden zentral Keys erstellen möchte, die an Keystores wie z.b. die ICSF Keydatasets verteilt werden sollen/müssen. (PUSH-Mechanismus : die Keys werden zentral erstellt und dann via EKMF Agent (ein´Started Task auf z/OS) verteilt. **EKMF bietet NICHT die Möglichkeit Keys via KMIP oder IPP abzuholen** !

GKLM bietet die Möglichkeit Keys zentral für Storage (Platten, Tape-Librarys – IBM und non-IBM) zur Verfügung zu stellen. Diese können von den Devices via KMIP oder IPP abgeholt werden. **GKLM kann nicht genutzt werden um Keystores via Push-Methode mit Keys zu versorgen**

© 2022 IBM Corporation

Kunden Status - Enterprise Key Management

Encryption of data at enterprise scale requires robust key management

- The current key management landscape can be characterized by clients who have …
  - … already deployed an enterprise key management solution
  - … developed a self-built key management solution
  - … not deployed an enterprise key management solution

Key management for pervasive encryption must provide …

- Policy based key generation
- Policy based key rotation
- Key usage tracking
- Key backup & recovery

© 2022 IBM Corporation

Enterprise Key Management Foundation

EKMF

The IBM Enterprise Key Management Foundation (EKMF) provides real-time, centralized secure management of keys and certificates in an enterprise with a variety of cryptographic devices and key stores.

EKMF gibt es in 2 Ausprägungen:

EKMF (Workstation)	- ein Service Offering
EKMF Web	- ein Software Offering

© 2022 IBM Corporation

Wann EKMF Workstation, wann EKMF-Web ?

EKMF Workststation securely manages keys and certificates **for cryptographic coprocessors, hardware security modules (HSM), cryptographic software, ATMs, and point of sale termina**

Supports Operational Keys

IBM Enterprise Key Management Foundation – Web Edition (EKMF Web) provides efficient and security-rich centralized key management for **IBM z/OS data set encryption on IBM Z** servers. Using EKMF Web, you can make encryption easy by decoupling it from

Supports Operational Keys for z/OS data set encrpytion

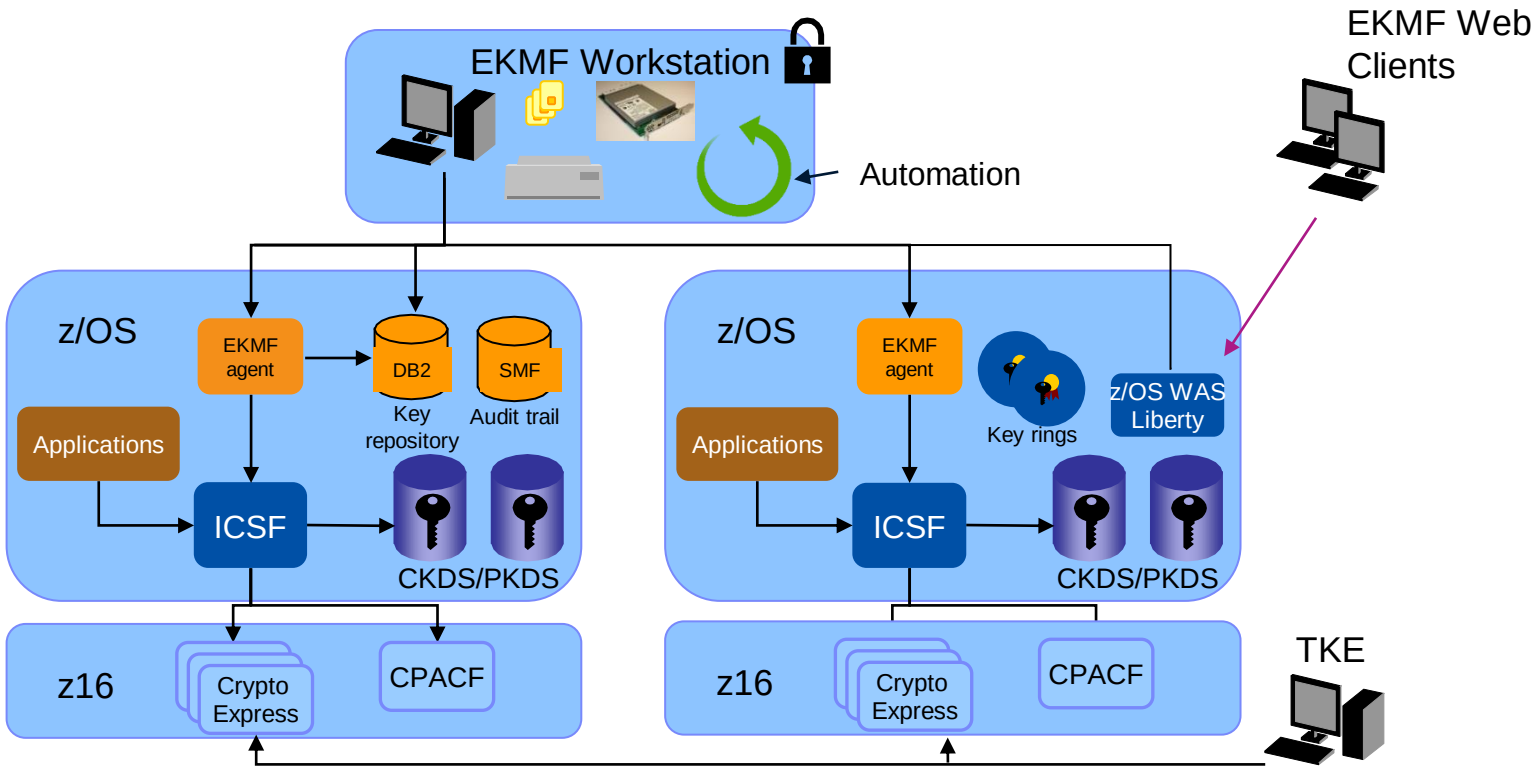
EKMF ist sinnvoll wenn der Kunden zentral Keys erstellen möchte, die an Keystores wie z.b. die ICSF Keydatasets verteilt werden sollen/müssen. (PUSH-Mechanismus : die Keys werden zentral erstellt und dann via EKMF Agent (ein Started Task auf z/OS) verteilt. **EKMF bietet NICHT die Möglichkeit Keys via KMIP oder IPP abzuholen** !

Beide EKMF Optionen nutzen den erwähnten EKMF Agent wenn Keys für ICSF erzeugt und verteilt werden müssen. Die EKMF-Web Lösung bietet die Möglichkeit die benötigten Funktionen in einem Web-Browser auszuführen. Sie benötigt daher keinen Secure-Room bzw. ermöglicht nicht einen zu nutzen für Key-Operationen.

Wenn ein Kunde bereits EKMF Workststation einsetzt, gibt es (fast) keinen Grund auch EKMF Web einzusetzten !

© 2022 IBM Corporation

IBM Enterprise Key Management (EKMF) and IBM Z crypto ecosystem



© 2022 IBM Corporation