MAINFRAME CRYPTO

IBM Key Management

Greg Boyd

gregboyd@mainframecrypto.com

www.mainframecrypto.com

Copyrights . . .

- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 12 years

. . . And Trademarks

- Copyright © 2016 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY**. Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

Agenda – ICSF Key Management

- Key Management Doc/Pubs
- ICSF Support
- IBM Key Management Tools
  - ICSF
  - SKLM/ISKLM/TKLM/EKM
  - TKE
  - EKMF

Key Management – A necessary evil

- Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with the keys, and the protection afforded to the keys.

  - from NIST Special Publication 800-57 Part 1 Revision 4 Recommendation for Key Management Part 1: General (dx.doi.org/10.6028/NIST.SP.800-57pt1r4)

CKMS Design

- Cryptographic Key Management System (CKMS)
  - Where/How key is generated
  - Where/How the key is stored and used
  - Metadata elements
  - Entities where key is distributed
  - How the key is protected in distribution
  - How the key is protected at endpoint
  - Archives
  - Accountability/Auditability
- Serve particular application or entire enterprise

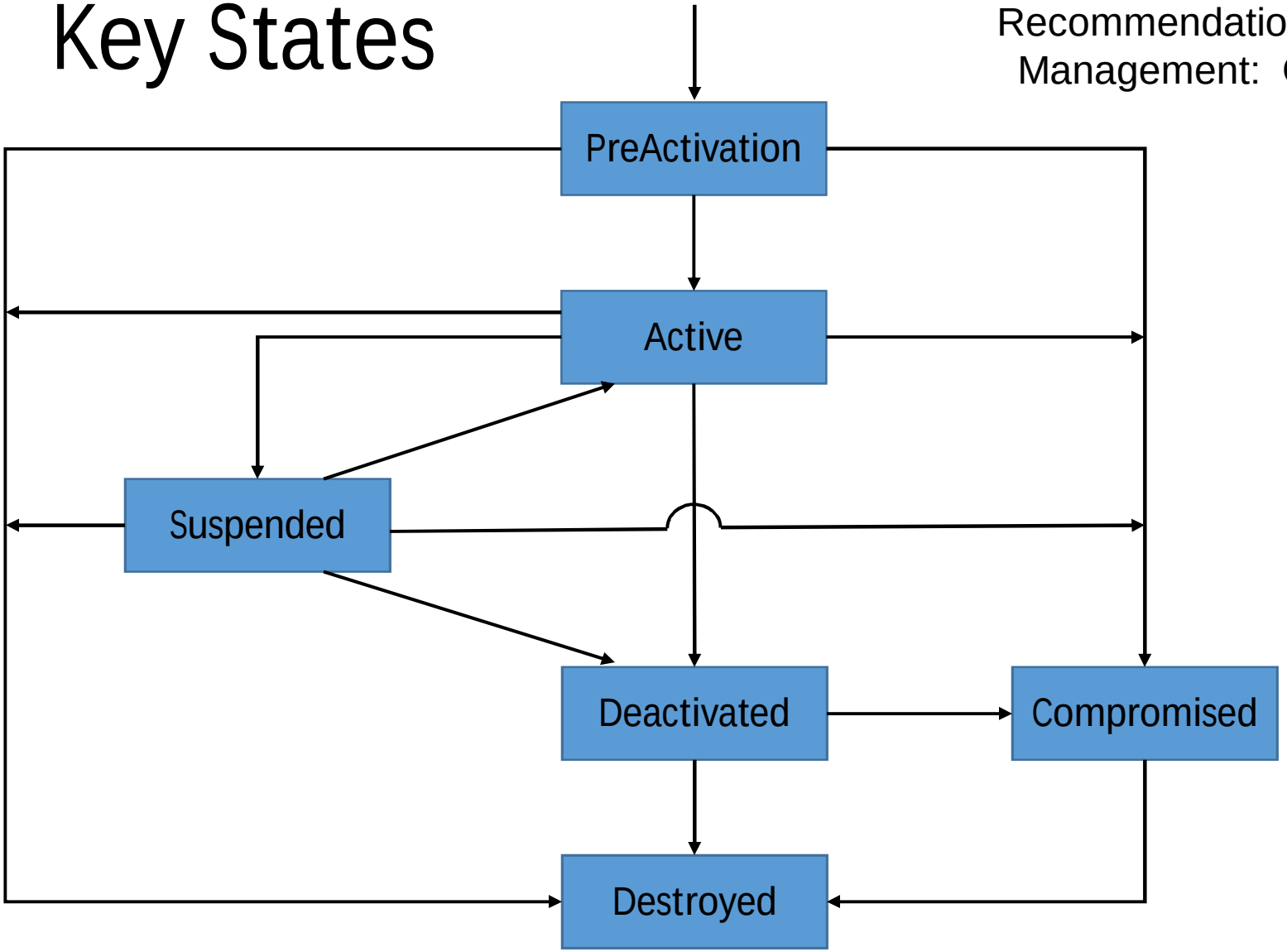
- From NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems

Key Properties & Uses

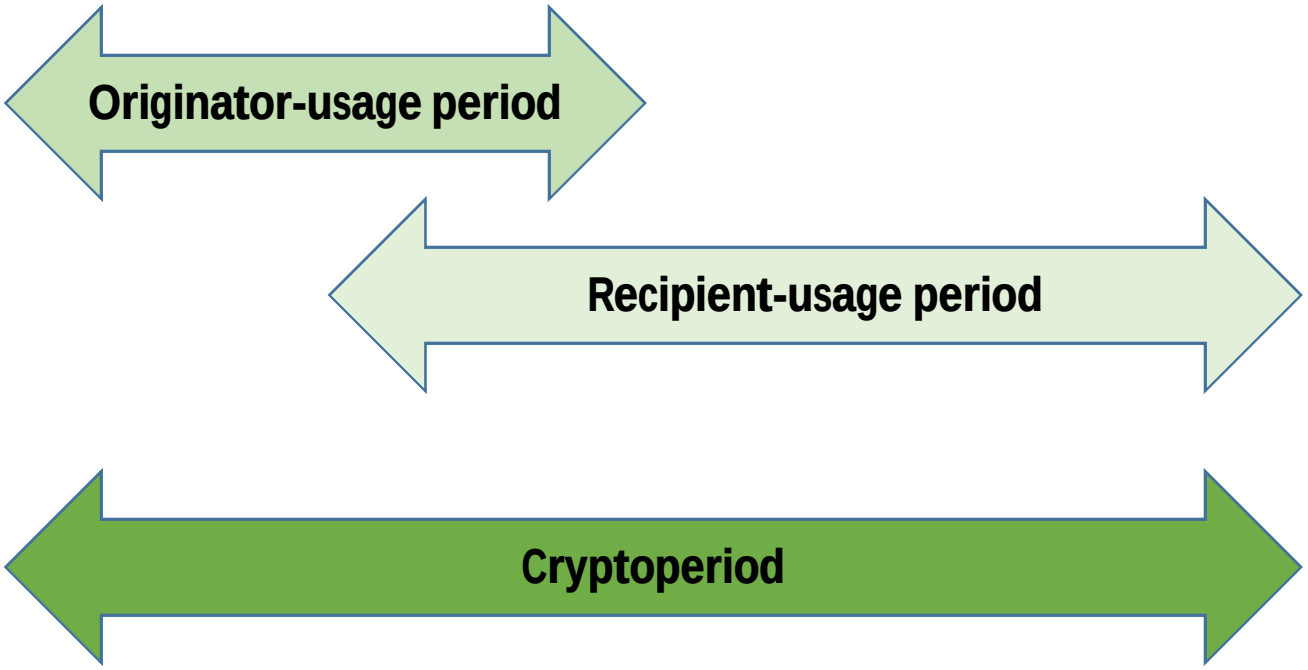
- Symmetric, public, private
- Static or ephemeral
- Key uses
  - Encryption/Decryption
  - Signature
  - Authentication
  - Key Wrapping
  - RNG
  - Master Key
  - Key Transport
  - Key Agreement
  - Authorization

Key States

From SP800-57 Part 1 Recommendation for Key Management: General



Cryptoperiod

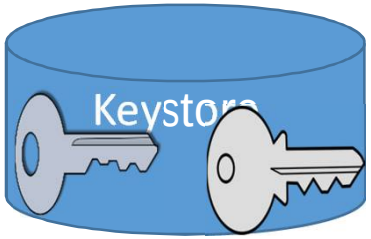


Cryptoperiod – How long a key should be used (implies change frequency)

- Limit amount (of time) data is protected by a key
- Limit amount (volume) of data protected by a key
- Security of the Crypto module – FIPS 140-2 Level 4 vs FIPS 140-2 Level 1 (Clear key)
- Who has access to the key

- Cost of key change
  - DoS Risk – how complicated is the key change process?
  - Distributing new key material

Digital Certificates



- Certificates are not keys, but they reference key material
- A Certificate store will likely contain public keys
  - So security requirements are lower
- But may contain private keys
  - Needs protection!

- Security Manager (RACF, CA-ACF2, CA-TopSecret) typically manages certificates
  - RACF Database can be the keystore
  - ICSF Keystore

Key Management Tools

- ICSF
- TKE
- SKLM/ISKLM/TKLM/EKM
- EKMF

Using ICSF for Key Management

- Key labels
  - PROD.DB2.APPX.D160928
- APIs
  - 48 Key Management APIs, all ICSF Key Types
  - Key Generation Utility Program
- Metadata
  - Record creation date/time
  - Record update date/time
  - Key material validity start date
  - Key material validity end date
  - Last used reference date
  - Record archive flag
  - Record archive date
  - Record recall date
  - Record prohibit archive flag
  - Variable-length metadata blocks
  - Installation user data

ISKLM

- EKM – Enterprise Key Manager
- TKLM – Tivoli Key Lifecycle Manager
- ISKLM – IBM Security Key Lifecycle Manager
  - Security Key Lifecycle Manager
  - Security Key Lifecycle Manager for z/OS

- On z/OS primarily a communication vehicle between drive & keystore
  - Use RACDCERT or hwkeytool to define keys
    - Use the PKDS (JCECCAKS or JCERACFCCAKS with Java) as your crypto provider
  - Adddrive & Moddrive – add a drive and associate it with a keygroup or associate a group with a device

KMIP – Key Management Interoperability Protocol

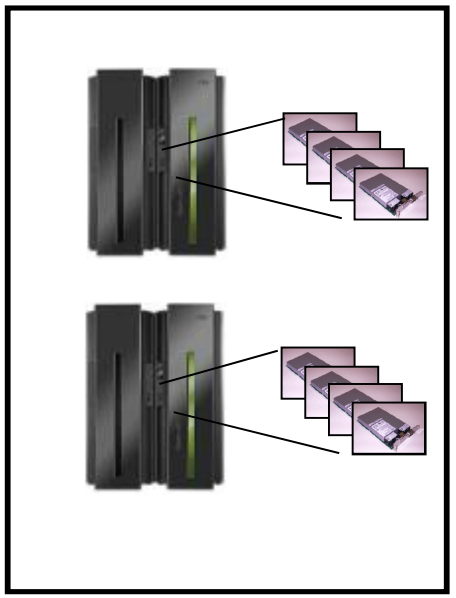
- A communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server.

Organization for the Advancement of Structured Information Standards (OASIS)

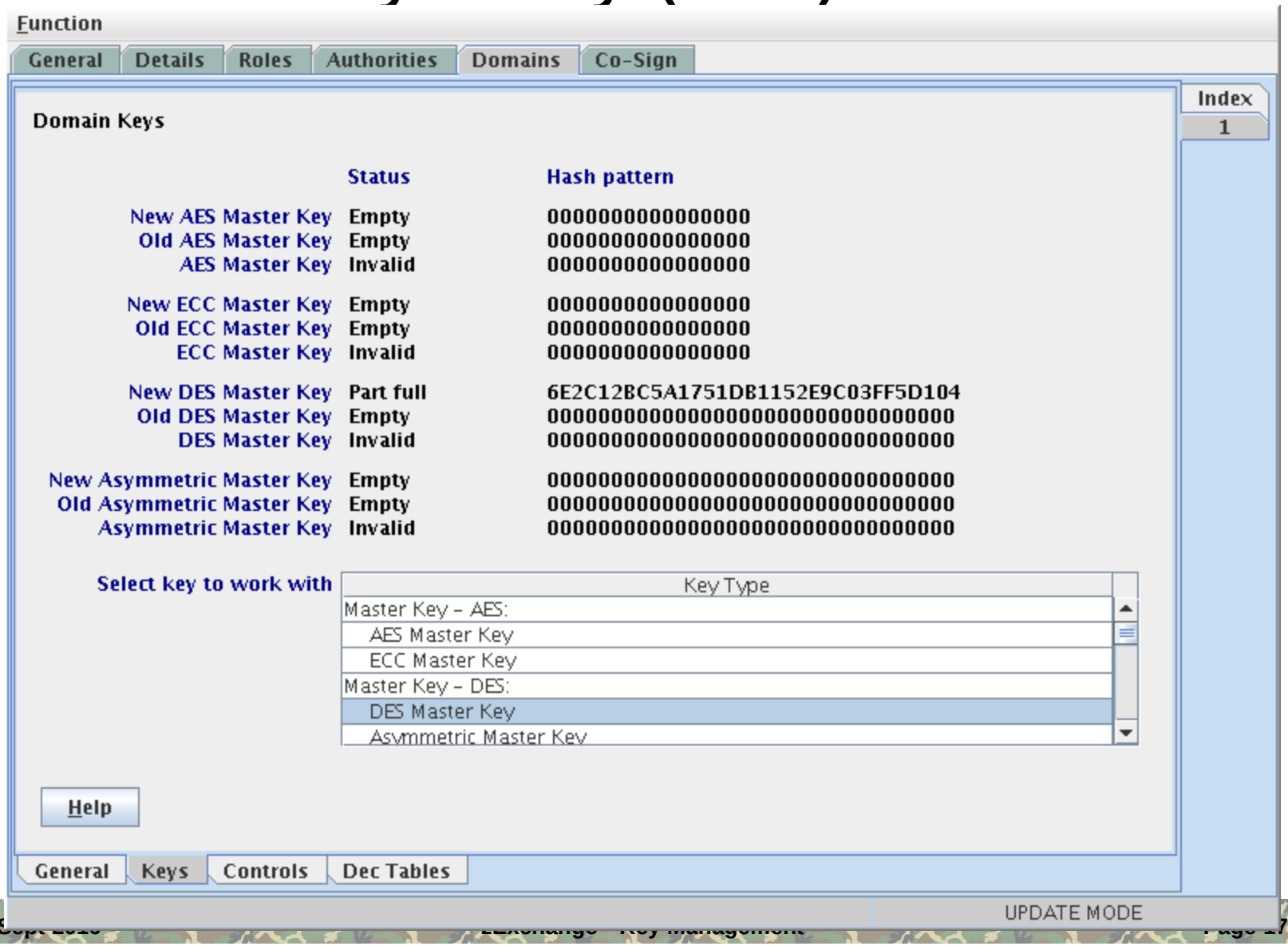
https://wiki.oasis-open.org/kmip

Trusted Key Entry (TKE) Workstation

- Secure Key Entry
  - Master keys or operational keys
  - Key material generated in hardware and never exists in the clear, outside of the tamper hardware (security)
  - Can provide dual control



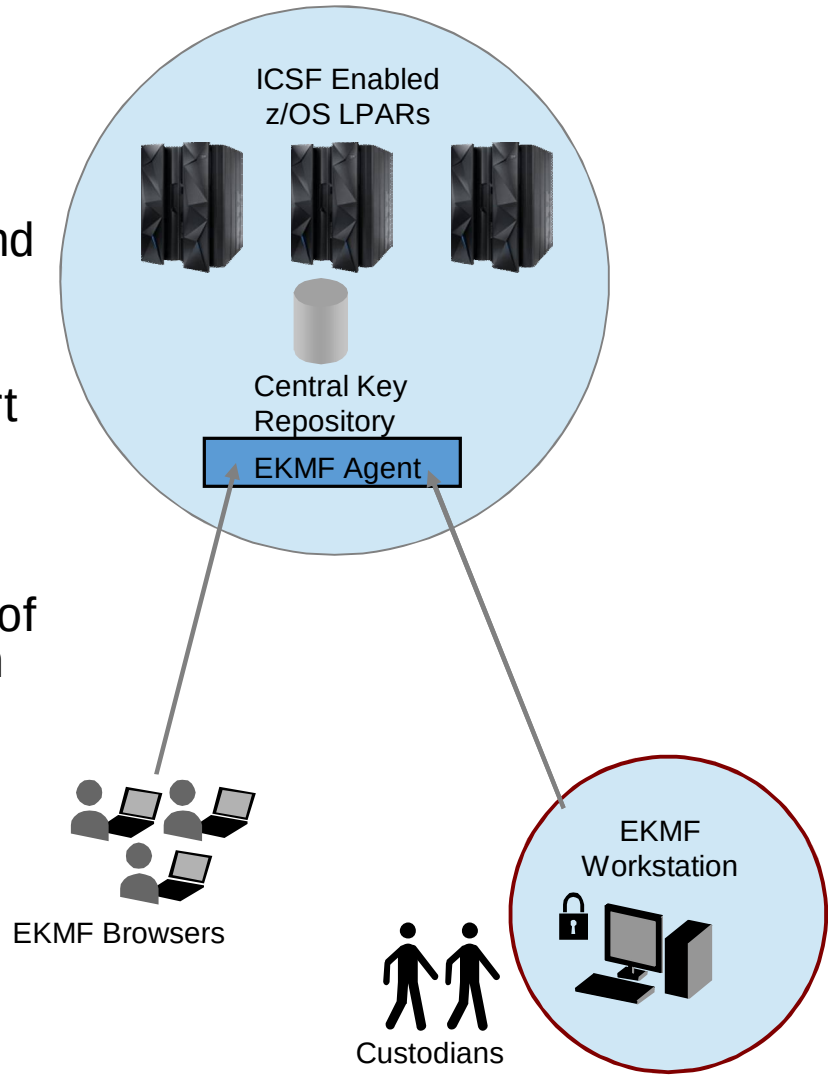
Trusted Key Entry (TKE)



IBM Enterprise Key Management Foundation (EKMF)

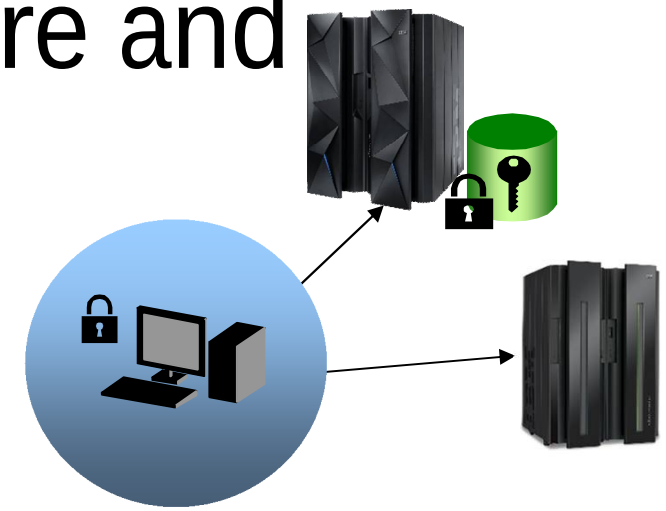
- The IBM EKMF solution comprises a highly secured workstation, a browser application and a central repository.
- All new keys are generated on the secured workstation by users authenticated with smart cards. The EKMF Workstation includes a IBM 4765.
- The EKMF Browser application features monitoring capabilities and enables planning of future key handling session to be executed on the workstation.
- The central repository contains keys and metadata for all cryptographic keys produced by the EKMF workstation. This enables easy backup and recovery of key material.

  Note that while this is a mainframe centric view, EKMF supports distributed platforms as well

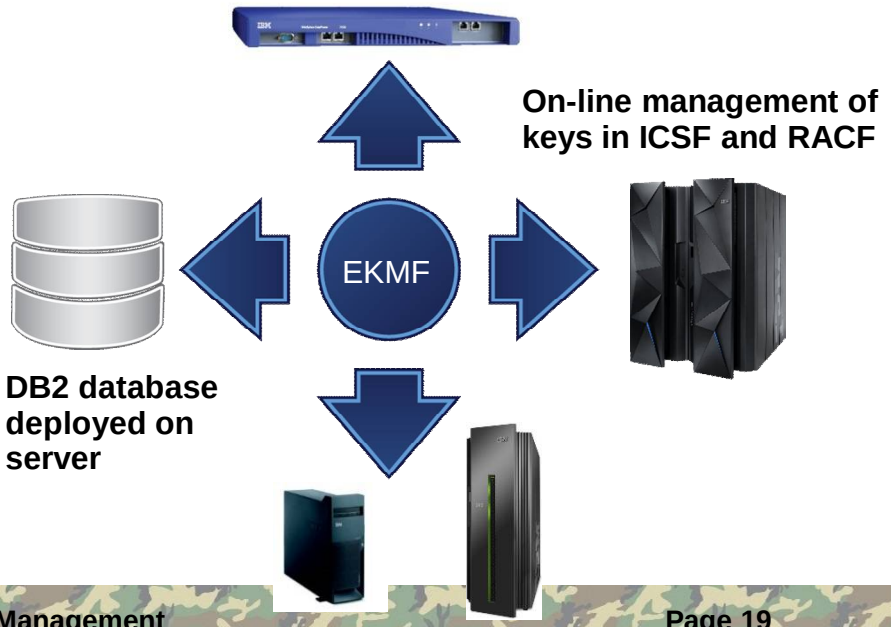


IBM EKMF Architecture and Components

- EKMF workstation is online with all mainframes in the system
  - Manages the keys in ICSF key stores
  - Support for other platforms as well
  - Support for several workstations
- One LPAR is hosting the EKMF key repository
  - Containing keys and metadata
  - Easy backup and recovery
- Database (Repository)
  - Configuration
  - Keys and metadata
  - Audit log
  - Available on z/OS, Windows, Linux, AIX
- Key stores
  - Distribution – Push mechanism
  - ICSF, RACF, Websphere SSL, CCA/PKCS #11 DataPower, Thales



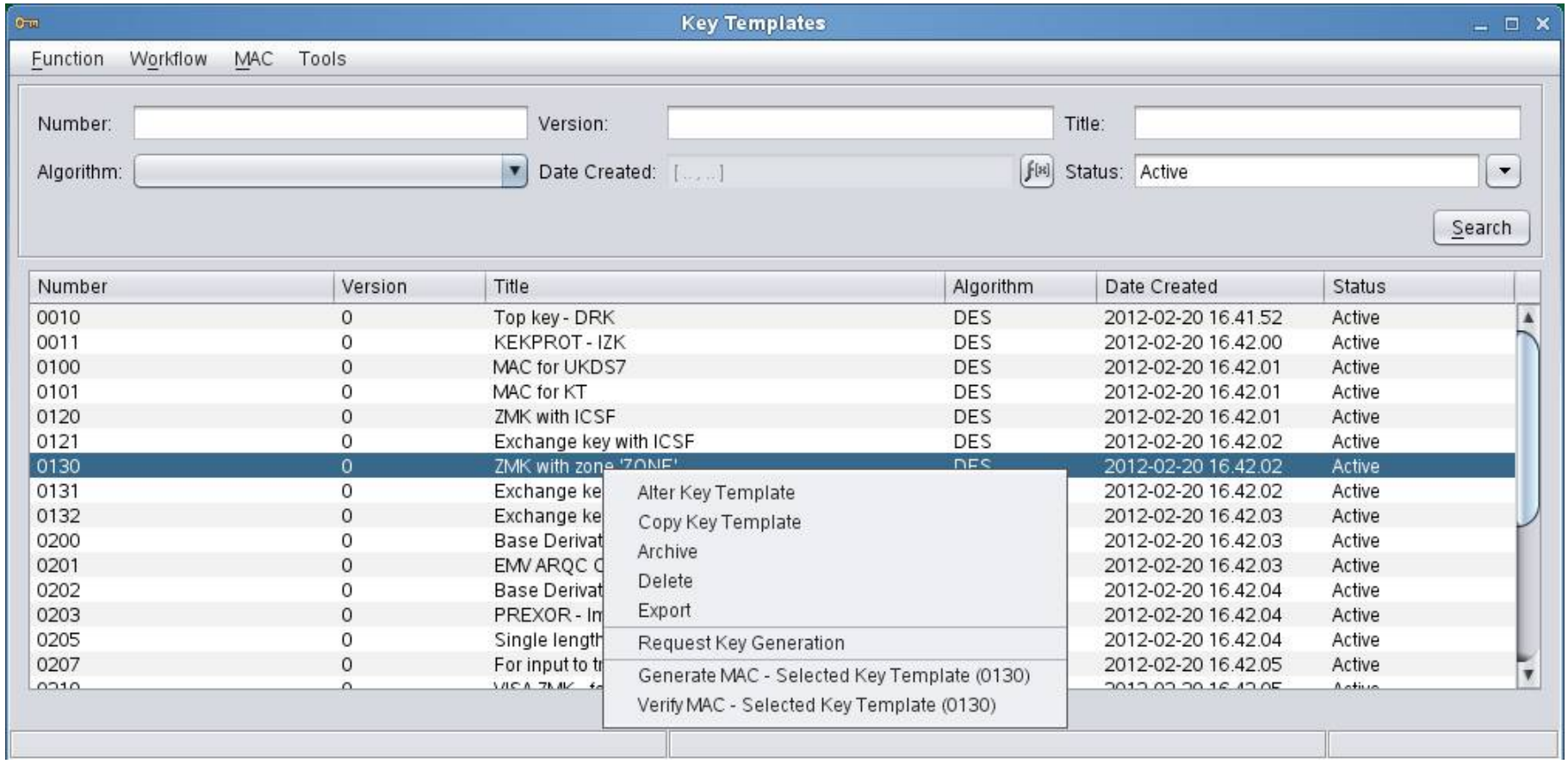
On-line management of keys and certificates for WebSphere DataPower



On-line management of keys in ICSF and RACF

DB2 database deployed on server

Key Template List

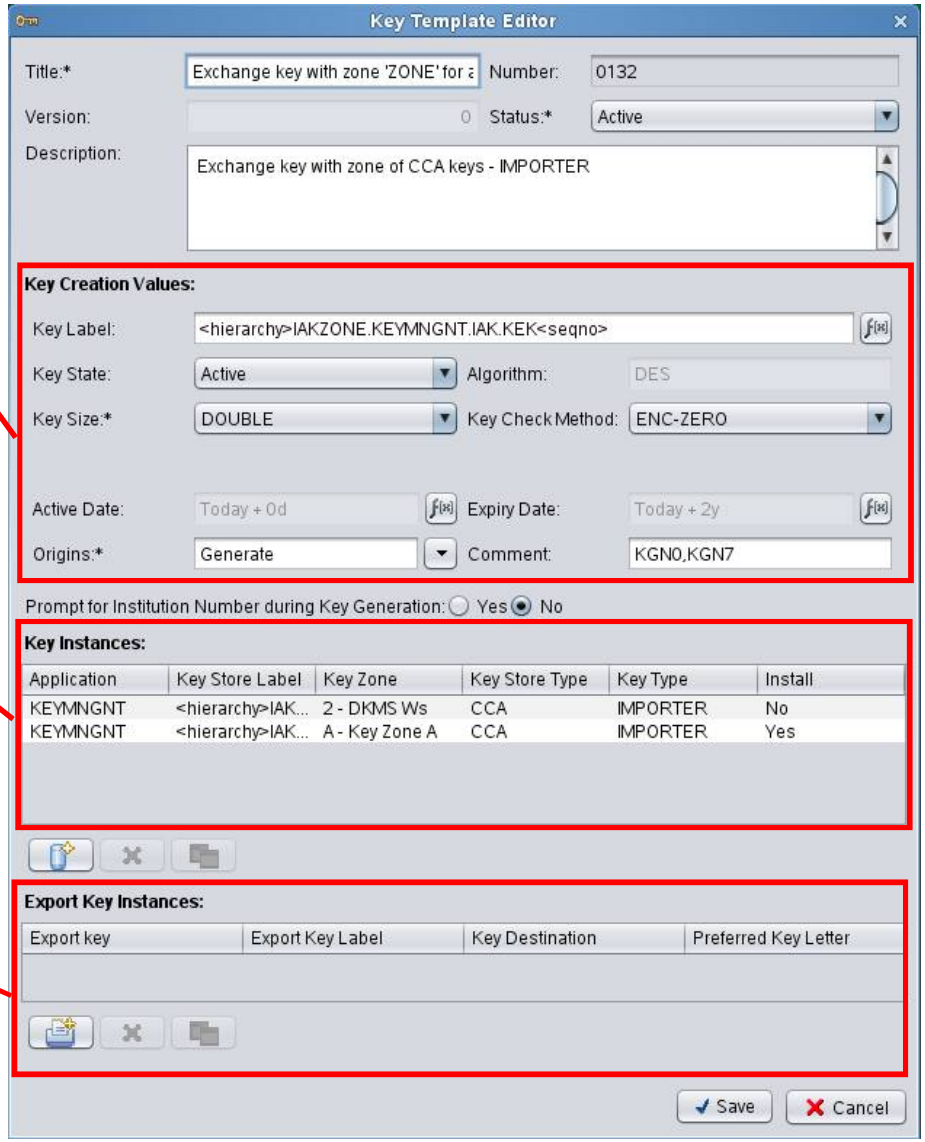


Key Template

Key Creation Values:
Main attributes such as label, activation date, origin etc.

Key Instances:
Where you want the key to be placed after generation

Export Key Instances:
Attributes if the key is to be Exported, e.g. as clear key parts



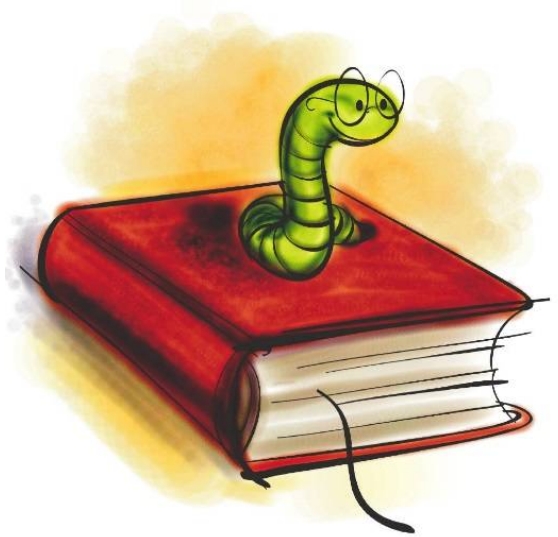
Comparison

	ICSF	SKLM	TKE	EKMF
Clear Keys/ Secure Keys	Clear or Secure Keys	Secure Keys	Secure Keys	Secure Keys
Products Required	Roll your own	IBM Software Product	IBM Hardware & Software	IBM Hardware & Software
Master or Operational Keys	Operational	Operational	Both	Operational
Symmetric/ Asymmetric / PKCS #11	All	Symmetric & Asymmetric	Symmetric	Symmetric & Asymmetric
Key Types	All	Limited	All	Most

NIST Special Publications (SP)

- http://csrc.nist.gov/publications/PubsSPs.html
  - SP 800-152 A Profile for U.S. Federal Cryptographic Key Management Systems
  - SP 800-135 Rev. 1 Recommendation for Existing Application-Specific Key Derivation Functions
  - SP 800-133 Recommendation for Cryptographic Key Generation
  - SP 800-132 Recommendation for Password-Based Key Derivation: Part 1: Storage Applications
  - SP 800-131A Rev. 1 Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
  - SP 800-130 A Framework for Designing Cryptographic Key Management Systems
  - SP 800-57 Part 1 Rev. 4 Recommendation for Key Management, Part 1: General
  - SP 800-57 Part 2 Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
  - SP 800-57 Part 3 Rev. 1 Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance

ICSF Pubs



- ICSF Overview
  - z/OS 2.1 SC14-7505
  - z/OS 1.13 SA22-7519
- ICSF Administrator's Guide
  - z/OS 2.1 SC14-7506
  - z/OS 1.13 SA22-7521
- ICSF Application Programmer's Guide
  - z/OS 2.1 SC14-7508
  - z/OS 1.13 SA22-7522

SKLM/ISKLM/TKLM

- IBM Security Key Lifecycle Manager for z/OS Information Center - http://www.ibm.com/support/knowledgecenter/SSB2KG_1.0.0/com.ibm.tivoli.isklm.doc_11/ic-homepage.html
  - Planning your Security Key Lifecycle Manager for z/OS Environment
  - Installing the Security Key Lifecycle Manager for z/OS
  - Configuring the Security Key Lifecycle Manager for z/OS
  - Administering the Security Key Lifecycle Manager for z/OS
- Redbook
  - REDP-4646 IBM Security Key Lifecycle Manager for z/OS: Deployment and Migration Considerations (2011)

Trusted Key Entry Workstation

- SC14-7511 Trusted Key Entry Workstation User's Guide
- Redbooks
  - REDP-5305 Streamline Management of the IBM z Systems Host Cryptographic Module Using IBM Trusted Key Entry (2015)
  - SG24-7848 System z Crypto and TKE Update (2011)
  - SG24-7123 z9-109 Crypto and TKE V5 Update (2005)
  - Sg24-6499 zSeries Trusted Key Entry (TKE) V4.2 Update (2004)
  - SG24-7070 IBM eServer zSeries 990 (z990) Cryptography Implementation (2004)

EKMF/DKMS Doc

- EKMF/DKMS Redbook
  - SG24-8181 Key Management Deployment Guide Using the IBM Enterprise Key Management Foundation
  - TIPS1052 Centralized Key Management using the IBM Enterprise Key Management Foundation
  - SA22-7519 z/OS Cryptographic Services ICSF Overview
    - See 'Managing keys with the Distributed Key Management System (DKMS)'
  - GG24-4406 Distributed Key Management System Installation and Customization Guide (from 1995)
- Presentation
  - Interconnect 2016 Cryptographic Keys Life Cycle Management for Your Company - https://www.ibm.com/events/tools/interconnect/2016ems/REST/presentations/PDF/InterConnect2016_6800.pdf