



IBM Americas, ATS, Washington Systems Center

Enterprise Key Management Foundation - The Future of Crypto Key Management Share 13177 San Francisco, CA February, 2013

Greg Boyd (boydg@us.ibm.com)

IBM Americas ATS, Washington Systems Center

© 2013 IBM Corporation



QR Code



What are we announcing and why is it important?

IBM Enterprise Key Management Foundation is a Centralized Key Management Solution on zEnterprise which is well suited for banks, payment card processors and other businesses that must meet Payment Card Industry requirements

Key enablers are **z/OS with ICSF, IBM DB2 Version 9.1 for z/OS, IBM z9 – zEC12 & CryptoExpress 2/3/4S**

- **Leverages your investment in System z hardware**



Introducing - IBM Enterprise Key Management Foundation

Provide a centralized key management solution that leverages clients investments in System z Hardware Crypto for the ultimate protection of sensitive keys and meeting compliance standards

Solution Summary

Provide a simple centralized key management which adheres to industry standards

- **Provides a foundation that can be tailored to address the needs of multiple industry segments to help identify compliance issues and assist key officers in enforcing an enterprise key management policy requirements**
- **Features crypto analytic capabilities that help identify compliance issues to assist key officers in understand how and who has access to key material**

Solution Benefits

- **Provide higher quality of service by efficient key management and automation**
- **Leverages clients investments in System z hardware**
- **Simplifies business continuity considerations for mission critical key material**

Business outcomes

Vantiv, the #1 Largest processor of PIN debit transactions in the US*, performs over 2 billion crypto transactions per month

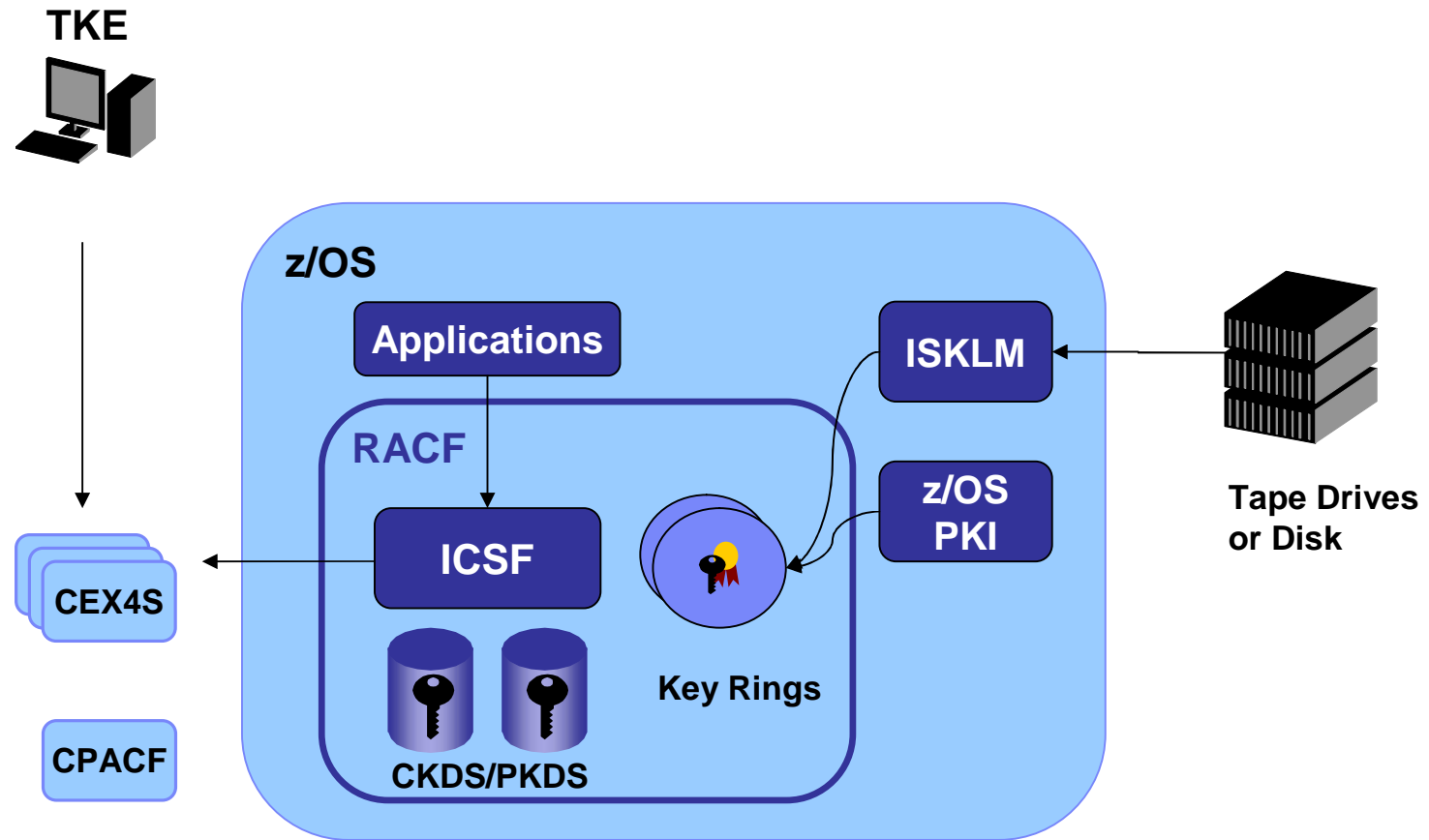
“The cryptographic coprocessors provide the ability to create tremendous encryption capacity for all operating platforms. Our use of the Crypto Express processors has expanded beyond a single purpose, mainframe-only solution, to an enterprise-wide encryption service”
- Vantiv

Colony Brands, believes that Secured platform for critical business applications enabling the best possible customer experience

“The zEnterprise provides us with a secure platform that enables us to ensure our customers’ private data is secure which improves our customer experience and overall satisfaction.” – Todd Handel Director IT Strategy & Architecture

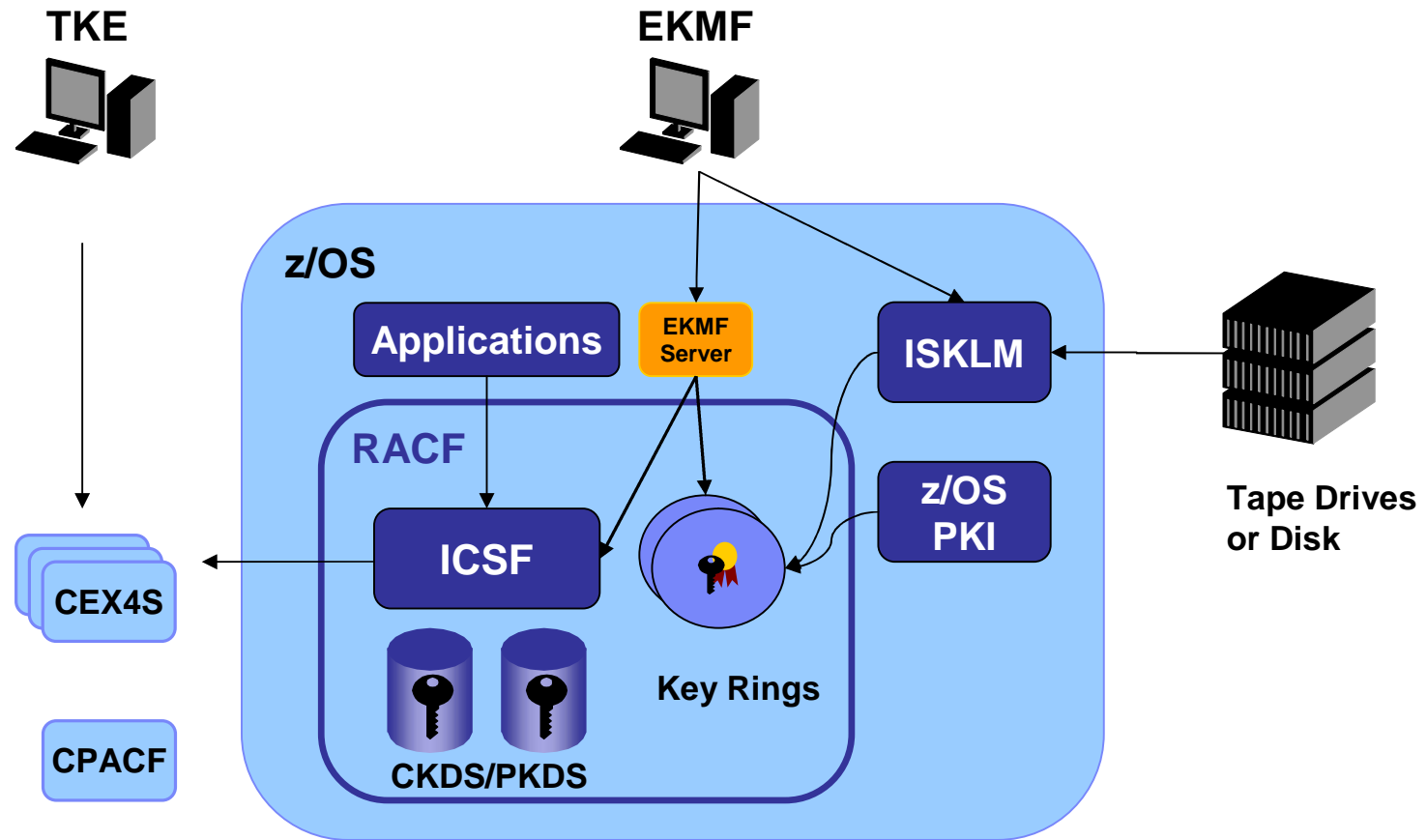
z Crypto Ecosystem

CryptoExpress, ICSF, TKE, RACF, z/OS PKI, ISKLM



IBM EKMF and the z Crypto Ecosystem

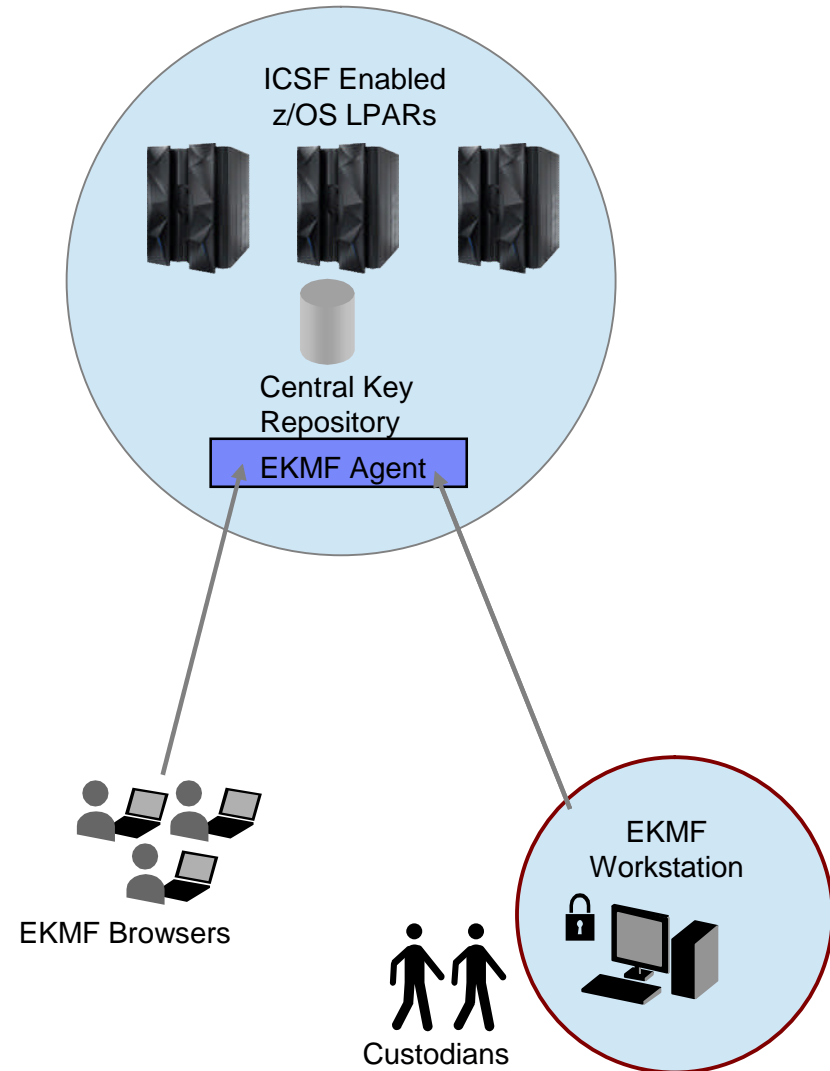
EKMF leverages the Crypto Express, ICSF, TKE, RACF, and ISKLM offering additional integration and service offerings



IBM Enterprise Key Management Foundation

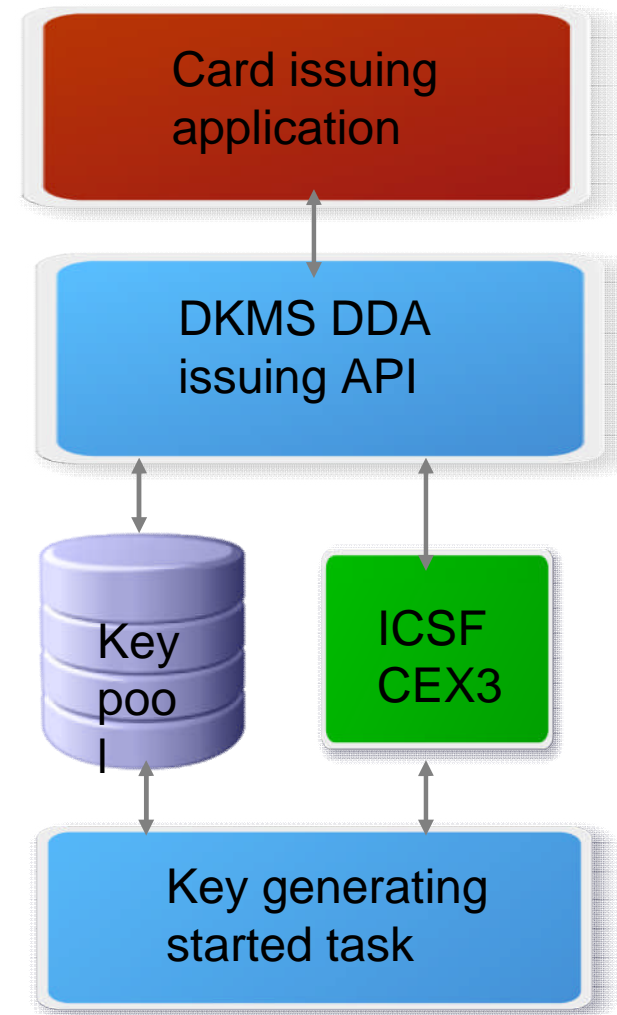
- The IBM EKMF solution comprises a highly secured workstation, a browser application and a central repository.
- All new keys are generated on the secured workstation by users authenticated with smart cards. The EKMF Workstation includes a IBM 4765.
- The EKMF Browser application features monitoring 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



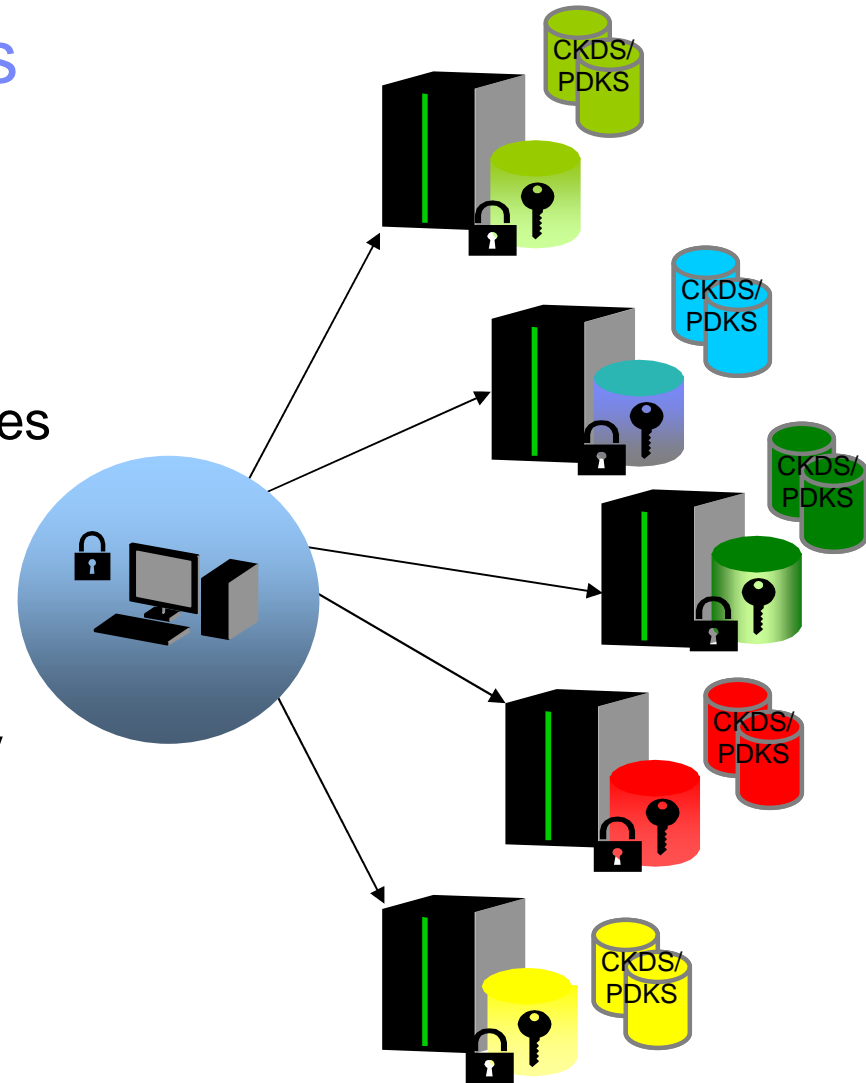
EMV Chip Card Data Generation

- **Support for SDA, DDA, and CDA chip cards**
- **Generates card unique DES keys, RSA keys, and certificates**
 - RSA key generation is time consuming
 - RSA keys generated in advance to a pool
 - utilizing spare capacity during off-peak hours
- **Signs data with Issuer RSA key**
- **Prepare data to card manufacturer (Global Platform support)**



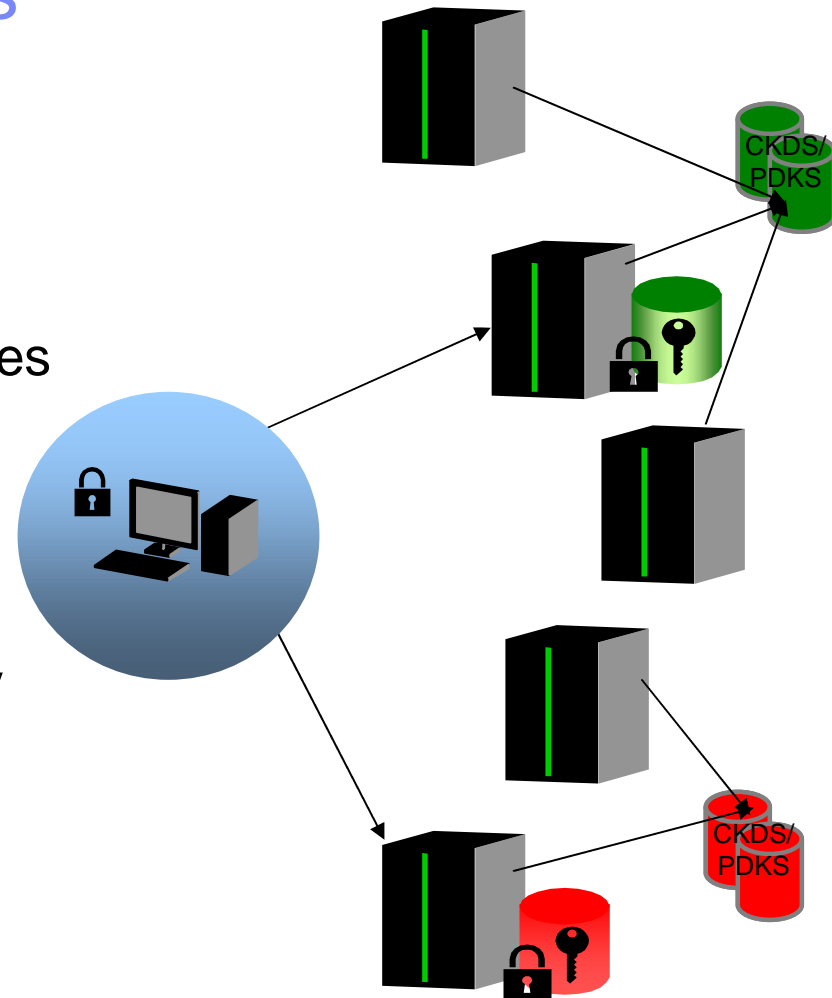
Architecture and Components

- **EKMF workstation is online with all mainframes in the system**
 - Manages the keys in ICSF key stores
 - Support for several workstations
 - Support for other platforms as well
- **One LPAR is hosting the EKMF key repository**
 - containing keys and metadata
 - for easy backup and recovery



Architecture and Components

- **EKMF workstation is online with all mainframes in the system**
 - Manages the keys in ICSF key stores
 - Support for several workstations
 - Support for other platforms as well
- **One LPAR is hosting the EKMF key repository**
 - containing keys and metadata
 - for easy backup and recovery



The Enterprise Key Management Foundation Model

- **Different user roles for segregation of duties**
 - Administrators for system configuration and planning of key ceremonies
 - Key Managers to generate key material
 - Custodians for key generations and handling of cryptographic variables
- **Key Templates for efficient key design and handling**
 - All keys in EKMF are based on a key template.
 - Enables designing and testing before generating keys in production
 - Comprises the properties of a key – such as:
 - key labels, (de)activation dates, key state etc.
 - origin of the key (generation, import or translation)
 - where it must be placed after entering the system
- **Secure audit log for reliable review by auditors**
- **Push model - keys are pushed to the keys stores**

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

The screenshot shows the 'Key Template Editor' window. It contains several sections:

- Title:** Exchange key with zone 'ZONE' for z
- Number:** 0132
- Status:** Active
- Description:** Exchange key with zone of CCA keys - IMPORTER
- Key Creation Values:** (highlighted with a red box)
 - Key Label:** <hierarchy>IAKZONE.KEYMNGNT.IAK.KEK<seqno>
 - Key State:** Active
 - Key Size:** DOUBLE
 - Algorithm:** DES
 - Key Check Method:** ENC-ZERO
 - Active Date:** Today + 0d
 - Expiry Date:** Today + 2y
 - Origins:** Generate
 - Comment:** KGN0,KGN7
- Key Instances:** (highlighted with a red box)

| Application | Key Store Label | Key Zone | Key Store Type | Key Type | Install |
|-------------|-------------------|----------------|----------------|----------|---------|
| KEYMNGNT | <hierarchy>IAK... | 2 - DKMS Ws | CCA | IMPORTER | No |
| KEYMNGNT | <hierarchy>IAK... | A - Key Zone A | CCA | IMPORTER | Yes |
- Export Key Instances:** (highlighted with a red box)

| Export key | Export Key Label | Key Destination | Preferred Key Letter |
|------------|------------------|-----------------|----------------------|
| | | | |

Key Template List

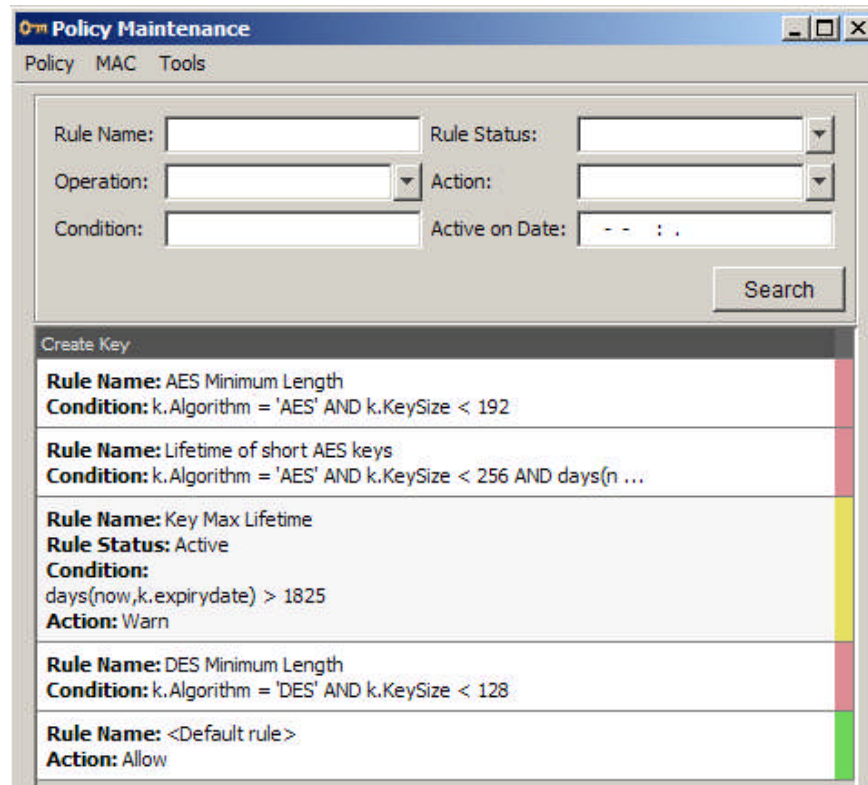
The screenshot shows the 'Key Templates' application window. At the top, there are tabs for 'Function', 'Workflow', 'MAC', and 'Tools'. Below the tabs are search filters: 'Number', 'Version', 'Title', 'Algorithm', 'Date Created', and 'Status'. A 'Search' button is located on the right. The main area contains a table with the following data:

| Number | Version | Title | Algorithm | Date Created | Status |
|--------|---------|------------------------|-----------|---------------------|--------|
| 0010 | 0 | Top key - DRK | DES | 2012-02-20 16.41.52 | Active |
| 0011 | 0 | KEKPROT - IZK | DES | 2012-02-20 16.42.00 | Active |
| 0100 | 0 | MAC for UKDS7 | DES | 2012-02-20 16.42.01 | Active |
| 0101 | 0 | MAC for KT | DES | 2012-02-20 16.42.01 | Active |
| 0120 | 0 | ZMK with ICSF | DES | 2012-02-20 16.42.01 | Active |
| 0121 | 0 | Exchange key with ICSF | DES | 2012-02-20 16.42.02 | Active |
| 0130 | 0 | ZMK with zone 'ZONE' | DES | 2012-02-20 16.42.02 | Active |
| 0131 | 0 | Exchange ke | | 2012-02-20 16.42.02 | Active |
| 0132 | 0 | Exchange ke | | 2012-02-20 16.42.03 | Active |
| 0200 | 0 | Base Derivat | | 2012-02-20 16.42.03 | Active |
| 0201 | 0 | EMV ARQC C | | 2012-02-20 16.42.03 | Active |
| 0202 | 0 | Base Derivat | | 2012-02-20 16.42.04 | Active |
| 0203 | 0 | PREXOR - In | | 2012-02-20 16.42.04 | Active |
| 0205 | 0 | Single length | | 2012-02-20 16.42.04 | Active |
| 0207 | 0 | For input to tr | | 2012-02-20 16.42.05 | Active |
| 0210 | 0 | VISA ZMK - s | | 2012-02-20 16.42.05 | Active |

A context menu is open over the row for template 0130, listing the following actions:

- Alter Key Template
- Copy Key Template
- Archive
- Delete
- Export
- Request Key Generation
- Generate MAC - Selected Key Template (0130)
- Verify MAC - Selected Key Template (0130)

Key Policies



The screenshot shows the 'Policy Maintenance' application window. The title bar reads 'Policy Maintenance' and the menu bar includes 'Policy', 'MAC', and 'Tools'. The main form area contains several input fields: 'Rule Name', 'Rule Status', 'Operation', 'Action', 'Condition', and 'Active on Date'. A 'Search' button is located at the bottom right of the form. Below the form is a table titled 'Create Key' with the following entries:

| Rule Name | Condition | Rule Status | Action |
|----------------------------|--|-------------|--------|
| AES Minimum Length | k.Algorithm = 'AES' AND k.KeySize < 192 | | |
| Lifetime of short AES keys | k.Algorithm = 'AES' AND k.KeySize < 256 AND days(n ... | | |
| Key Max Lifetime | days(now,k.expirydate) > 1825 | Active | Warn |
| DES Minimum Length | k.Algorithm = 'DES' AND k.KeySize < 128 | | |
| <Default rule> | | | Allow |

Define a set of rules that must be met when a key is entering the system.

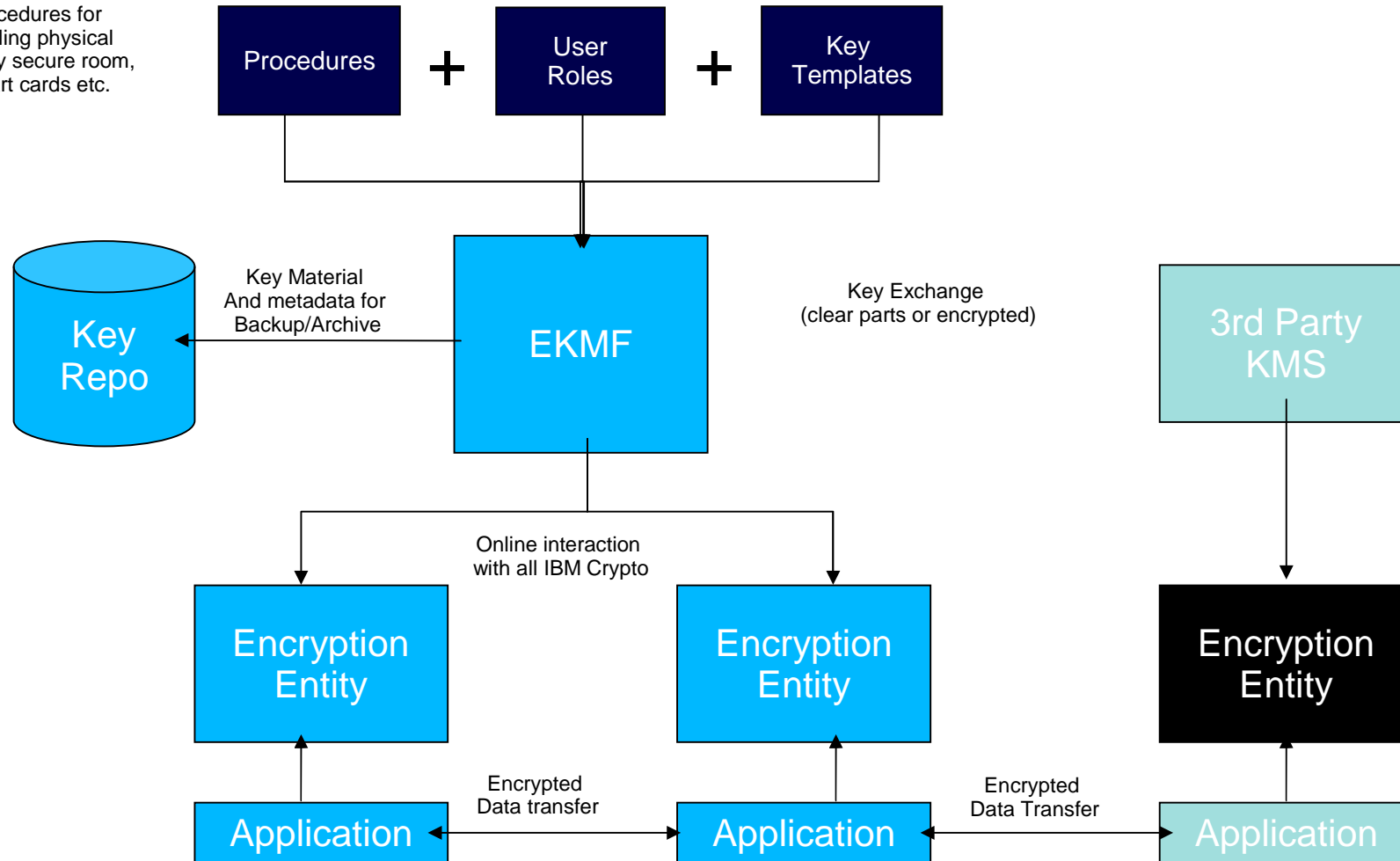
A rule refers to the attributes of a EKMF key object.

Policies work outside the standard EKMF access control system.

Keys not compliant with the defined policies can be found using reports.

Key Management Model

Procedures for handling physical Security secure room, smart cards etc.



IBM Enterprise Key Management Foundation

User Example - Work flow based key management

- 1 Request new keys, key renewals, or key revocation.
- 2 Requested tasks performed by security officers
- 3 Monitoring and Reporting – e-mail & EKMF Browser
- 4 Analysis leading to new key management requests



Monitoring Service

- **Monitors expiration of keys and certificates in EKMF key repository**
- **Monitoring and reports are customizable**
- **Alerts key managers / application owners by e-mail**
- **Report available on EKMF workstation as a list of tasks to perform**



IBM Enterprise Key Management Foundation

What makes this solution unique?

Auditing & Compliance

- Compliance with Payment Card Industry Requirements
- Bringing a heterogeneous HSM environment in control and in compliance by utilizing the IBM system z platform as a proven base
- Centralization of key management simplifies the Security Officer or the Key Managers need to identify compliance issues for key material

Simplification

- Facilitates a standardized set of procedures and operations to enforce an enterprise key management policy
- Simple to manage task oriented dash board with automated management tasks to help simplify key management operations
- Monitoring and reporting facilities provided to help identify compliance issues and assist key officers in enforcing policy requirements

IBM Enterprise Key Management Foundation

Things you should ask yourself

How do you currently manage your keys?

How do you know when your keys need to be updated/changed/expired?

How do you ensure you are meeting the Payment Card Industry requirements?

What are the difficulties in passing an audit?

What is your current investment in IBM Hardware for Security?

References - IBM EKMF

- **IBM System z Security:** [System z Security Page](#)
 - <http://www.ibm.com/systems/z/solutions/security.html>
- **Lab Based Services:** [EKMF Information](#)
 - <http://www.ibm.com/systems/services/labservices/index.html>
 - Or send a note to Systemz@us.ibm.com
- [Crypto Competency Center](#)
 - <http://www.ibm.com/security/cccc/>
- **Announcement Info**
 - . www.ibm.com/systems/zsolutions

Thank
YOU



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

| | | | |
|------------|---|---|------------------------|
| AlphaBlox* | GDPS* | RACF* | Tivoli* |
| APPN* | HiperSockets | Redbooks* | Tivoli Storage Manager |
| CICS* | HyperSwap | Resource Link | TotalStorage* |
| CICS/VSE* | IBM* | RETAIN* | VSE/ESA |
| Cool Blue | IBM eServer | REXX | VTAM* |
| DB2* | IBM logo* | RMF | WebSphere* |
| DFSMS | IMS | S/390* | zEnterprise |
| DFSMSHsm | Language Environment* | Scalable Architecture for Financial Reporting | xSeries* |
| DFSMSrmm | Lotus* | Sysplex Timer* | z9* |
| DirMaint | Large System Performance Reference™ (LSPR™) | Systems Director Active Energy Manager | z10 |
| DRDA* | Multiprise* | System/370 | z10 BC |
| DS6000 | MVS | System p* | z10 EC |
| DS8000 | OMEGAMON* | System Storage | z/Architecture* |
| ECKD | Parallel Sysplex* | System x* | z/OS* |
| ESCON* | Performance Toolkit for VM | System z | z/VM* |
| FICON* | PowerPC* | System z9* | z/VSE |
| FlashCopy* | PR/SM | System z10 | zSeries* |
| | Processor Resource/Systems Manager | | |

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.