Centralized Key Management using the IBM Enterprise Key Management Foundation

IBM Redbooks Solution Guide

Looking at the pervasiveness of encryption today, you can understand the challenge an organization faces with managing the cryptography infrastructure and the encryption keys and certificates for their IT infrastructures. Financial institutions use encryption to secure payments as they face compliance requirements from the Payment Card Industry (PCI): the PCI-PIN and PCI-DSS requirements. Other organizations have to deal with the protection of personal data, for example, the public sector, insurance companies, and healthcare providers. They must comply with complex regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Data Protection Directive 95/46/EC. This IBM® Redbooks® Solution Guide describes the IBM Enterprise Key Management Foundation. By using it, organizations can centralize the key management effort and, in this way, simplify their key management processes. Simplified and unified processes are an important step toward compliance. Figure 1 shows the IBM Enterprise Key Management Foundation overview.

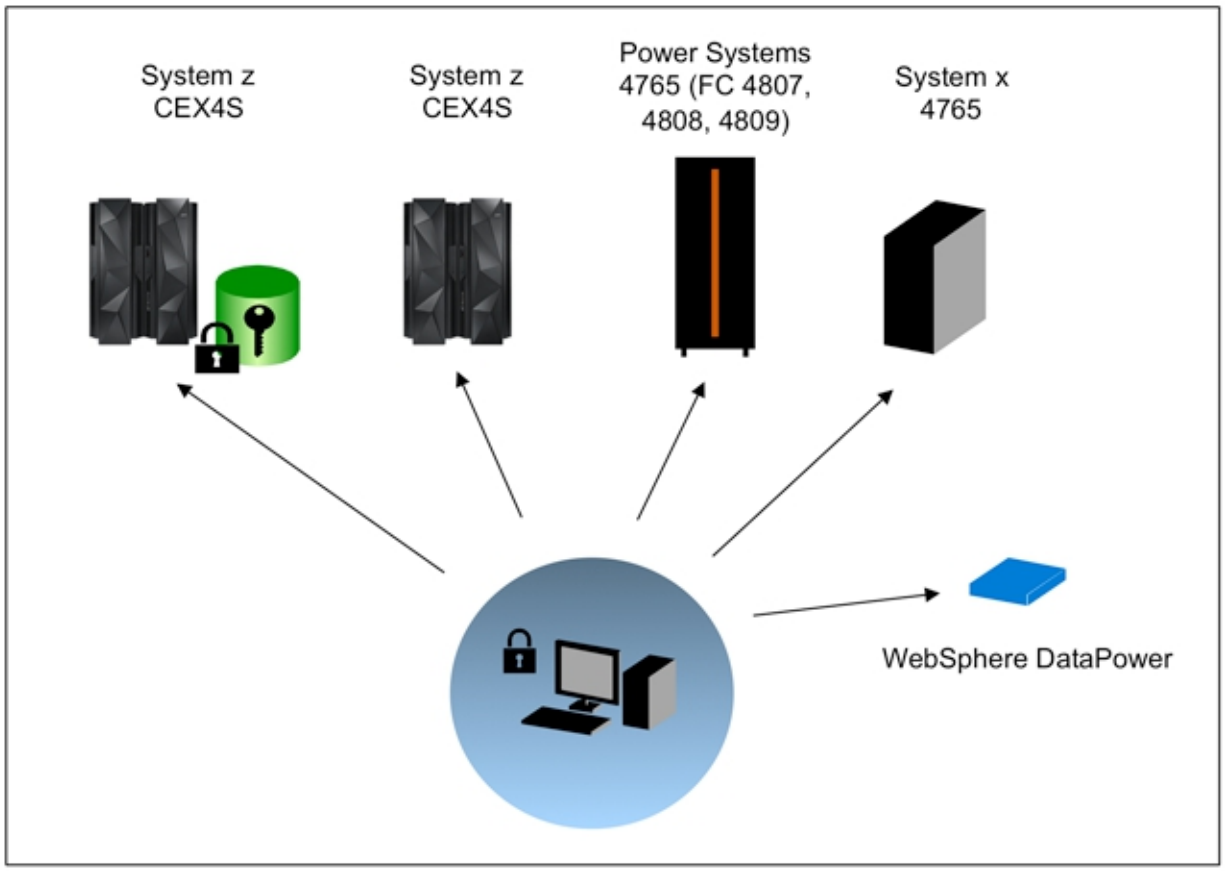

Figure 1. IBM Enterprise Key Management Foundation overview

The IBM Enterprise Key Management Foundation is built around a workstation that utilizes a key management application and an IBM 4765 cryptographic co-processor for secure key generation. The other main component in the IBM Enterprise Key Management Foundation is the key repository, an IBM DB2® database that is often deployed on an IBM z/OS® system. From the workstation, keys are pushed to the supported platforms shown in Figure 1.

Did you know?

The IBM Enterprise Key Management Foundation is policy driven and, as such, provides separation of duties. It can be configured to require two or more people to log on, and all key management activities are logged in a central log in DB2, and optionally in SMF on z/OS, as well. These capabilities make it easier to demonstrate compliance during audits.

Monitoring and reporting facilities are available and the key managers can issue key management requests from their desktop computers. Later, these requests can be executed in the secure environment of the IBM Enterprise Key Management Foundation workstation, in this way providing an efficient key management workflow.

Business value and solution overview

The IBM Enterprise Key Management Foundation provides business value for all organizations that have to manage and maintain encryption keys in their IT infrastructure:

- Centralized key management

  The IBM Enterprise Key Management Foundation provides centralized key management for the organization, concentrating the key management effort to a single organizational entity, with trained personnel that use a common set of procedures.

- Compliance

  This IBM technology has been used for more than 20 years by financial institutions that needed to be compliant with the card association's rules for processing PIN-based transactions. The solution is policy driven, and an organization can configure a setup where administrators create templates for keys that can be used over and over again when renewing keys for IT applications. Furthermore, it can be configured to require dual control for all or exactly those operations that organizations require. When dealing with key parts, the system keeps track
  of which users have handled which key parts. All key management operations are logged in the systems database and optionally in the z/OS System Management Facility (SMF).

- Business-oriented solutions

  Beyond the basic key management capabilities, the IBM Enterprise Key Management Foundation offers a number of solutions for various business purposes:

  - ATM Remote Key Loading (RKL)

    For online distribution of automatic teller machine (ATM) master keys, the IBM Enterprise Key Management Foundation provides support for Rivest-Shamir-Adleman algorithm (RSA)-based key distribution built on ANSI X9.24 part II, shown in Figure 2.

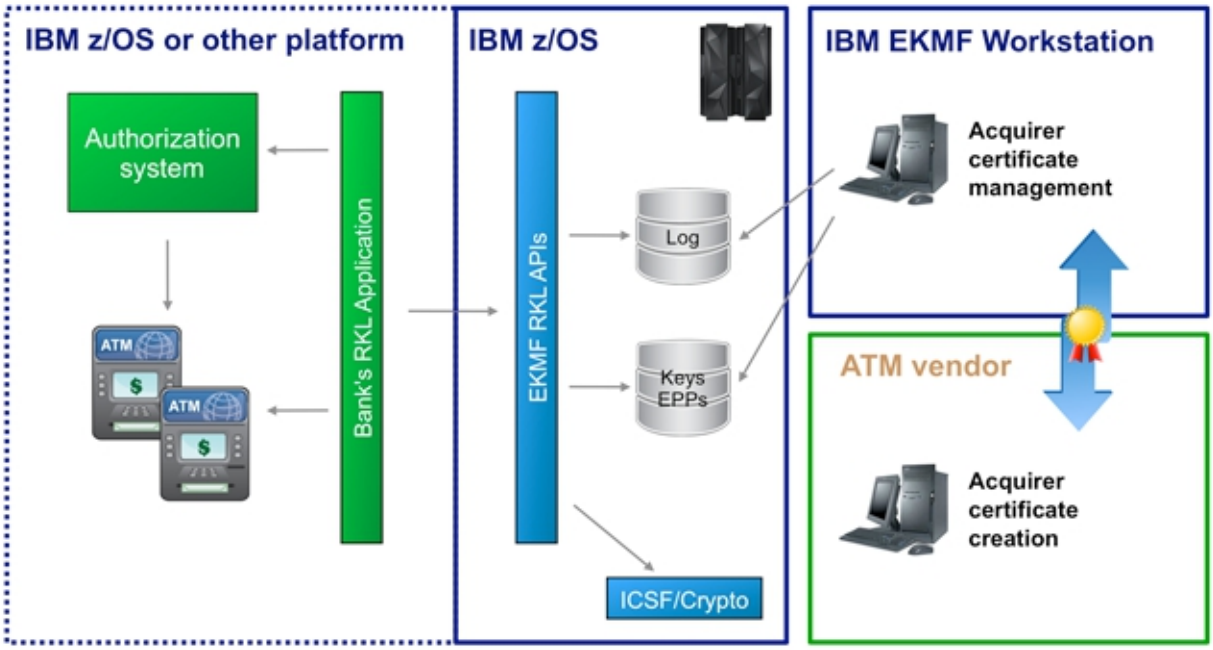

Figure 2. IBM Enterprise Key Management support for ATM RKL

- Europay, MasterCard, and Visa (EMV®)

  The EMV organization has created a set of standards for chip-based payment cards. The standards use both symmetric and asymmetric encryption techniques. See Figure 3.

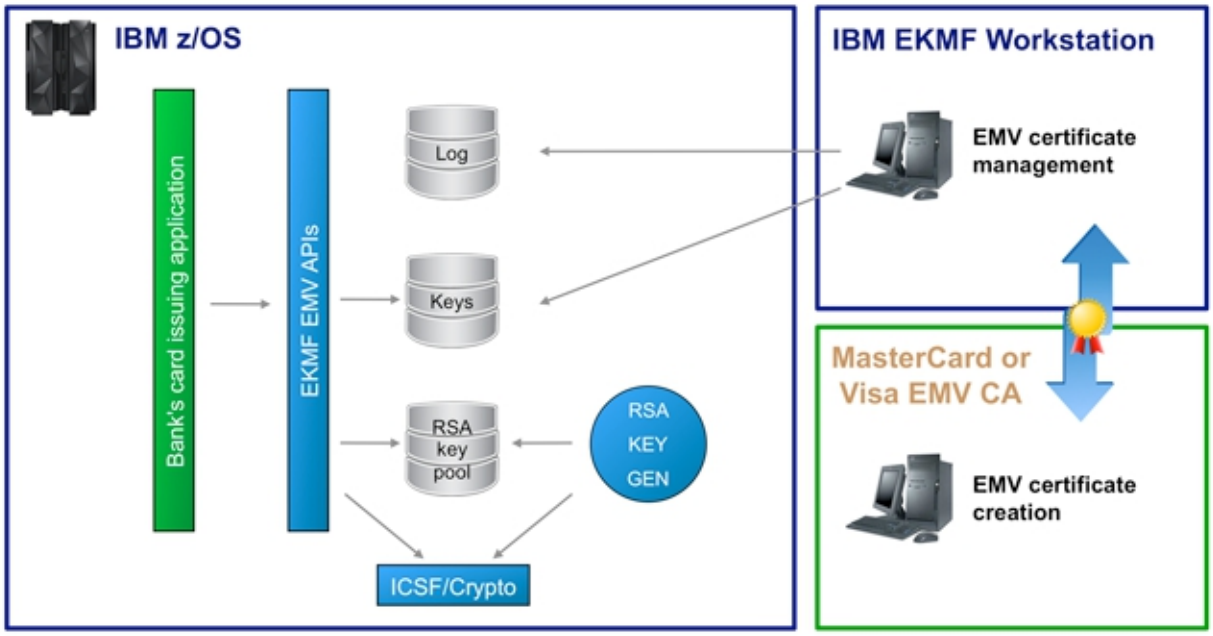

Figure 3. IBM Enterprise Key Management support for EMV

The IBM Enterprise Key Management Foundation enables an organization to manage the involved certificates, to generate the asymmetric keys to stock for all your cards in batch processes, and to encapsulate the issuing and authorization functions in application programming interfaces (APIs). The diagram in Figure 3 illustrates this functionality.

- Certificate management

  The ever-growing use of cryptography for securing transactions has resulted in an intensive use of certificates. Certificates need to be managed, particularly because they have a limited lifetime. Certificate expiration can often be linked as the direct cause of IT application or server downtime. To address this issue, a certificate management model has been developed for the IBM Enterprise Key Management Foundation. The model is depicted in Figure 4; it consists of four phases:

  - In the **discovery** phase, the network and servers are scanned for certificates.
  - Discovered certificates are checked against the system's database and new certificates can be enrolled in the system in the **enrollment** phase.
  - The **monitoring** phase is an ongoing phase, where the database is scanned for certificates that will expire in the near future. Notifications are issued for expiring certificates.
  - In the **management** phase, the certificates are renewed and installed on the servers, the old certificate is decommissioned, and the new certificate enters the monitoring phase. The IBM solution provides the capability to issue X.509V3 certificates for internal use.

  To assist applications in public key infrastructure (PKI)-related functions requiring certificates, a number of APIs can be provided to help with verifying certificate chains and building structures according to Public Key Cryptography standards PKCS#1 and PKCS#7. See Figure 4.

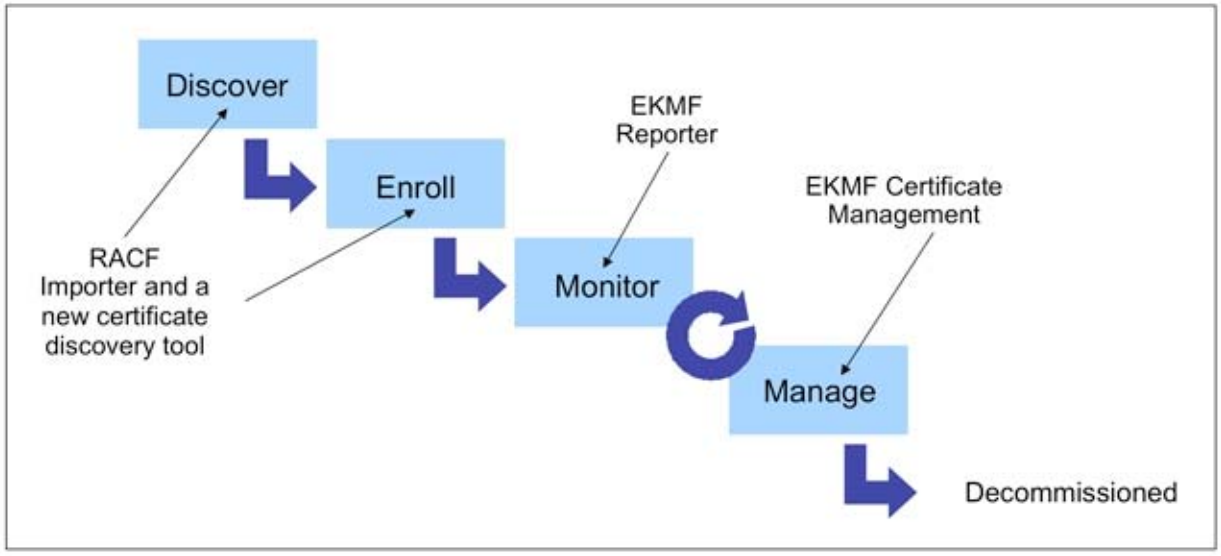

Figure 4. IBM Enterprise Key Management certificate management

Solution architecture

There are three basic components that make up an IBM Enterprise Key Management Foundation-based solution. Figure 5 depicts the components and shows how they interact.

- The workstation

  All key management operations that involve human interaction are carried out at the workstation. The workstation uses an IBM 4765 cryptographic co-processor installed for secure generation of the keys. The key management application is installed on the workstation, and operators can use smart cards for authentication to the application and the IBM 4765, if two-factor authentication is required. The smart cards can also be used to store the master key of the IBM 4765. If keys need to be printed, a printer can be attached to the workstation.

- The key repository

  Keys and their metadata are stored in an IBM DB2 database. This can be deployed on any server in the organization, although it is typically deployed on an IBM z/OS system when this platform is available, or on one of the servers that also provide an IBM 4765. The workstation connects to the database using Java Database Connectivity (JDBC) or an agent, described next. The network protocol is always TCP/IP.

- The agents

  The agents are installed on servers where either the key repository resides, or where there are keystores to be managed. An agent that only manages keystores is referred to as a "*crypto agent*", and an agent that manages the repository is called a "*database agent*". The crypto agent is required to push a key to the Integrated Cryptographic Service Facility (ICSF) on z/OS or an IBM 4765 on one of the other platforms, because ICSF and the IBM 4765 do not provide a network-based interface, as shown in Figure 5. The agent on z/OS image 1 in the figure serves both as database and crypto agent, and is denoted as a combined agent in the figure.

  Additionally, a crypto agent can provide private keys and certificates to IBM Resource Access and Control Facility (RACF®) key rings. The option to log in to z/OS SMF is available using either a crypto agent or a database agent. An agent is either installed as a started task on z/OS or as a service on the other available platforms. The IBM WebSphere® DataPower® solution exposes a "web service interface" that can be used for managing the keys and certificates; an agent is not needed in this case.

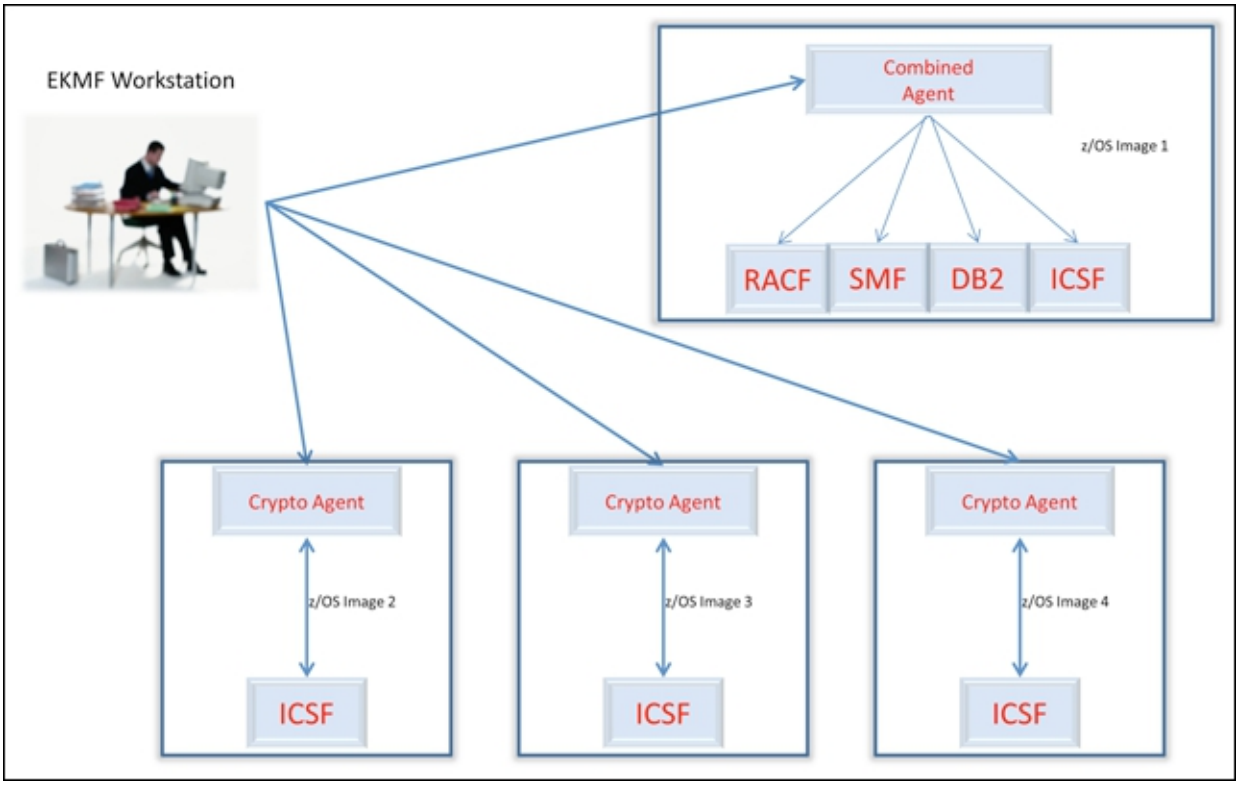

Figure 5. IBM Enterprise Key Management for IBM z/OS overview

Usage scenario

Financial institutions both issue payment cards (credit or debit cards) to their customers and also authorize the respective transactions when the cards are used in ATMs or at points-of-sale. Many banks today have separated the issuing and the authorization systems by deploying them on separate IBM z/OS logical partitions (LPARs). This requires that the cryptographic keys for the payment cards are available on those systems.

Let us look at an example where the bank needs to issue and verify the "*card verification value*" (CVV). In this case, the key that can generate the CVV needs to be installed on the issuing system, and an instance of the key that can verify the CVV has to be installed on the authorization system. Figure 6 shows a system configuration with two IBM System z® servers, each with two LPARs. Three of these LPARs are grouped into an IBM Parallel Sysplex® that runs the authorization system (Sysplex 1 in the diagram), while the issuing system is installed in Sysplex 2. To accomplish this key distribution, a database agent that can manage both DB2 and ICSF is installed in z/OS 2A, and crypto agents that can manage ICSF are installed in all three LPARs in Sysplex 1. Since these LPARs share the cryptographic key data set (CKDS), only one crypto agent needs to receive a key in order to install it in all three LPARs.

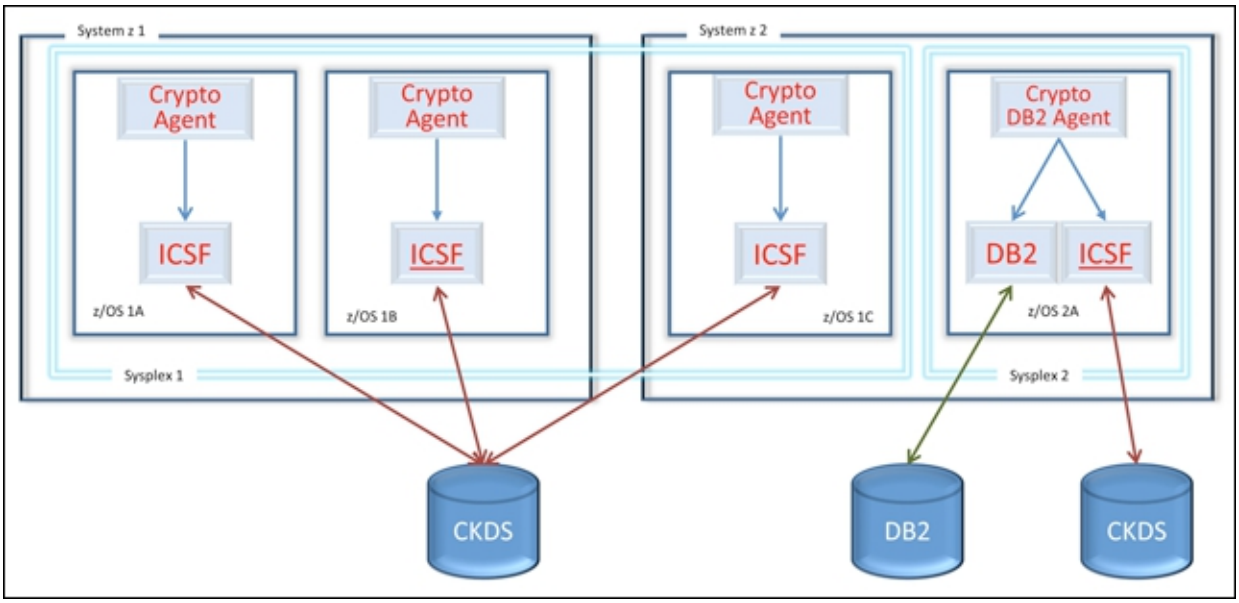

Figure 6. IBM Enterprise Key Management for IBM z/OS usage scenario with two Parallel Sysplex systems

Installation requirements

In order to deploy a complete IBM Enterprise Key Management Foundation system, both a workstation and a server with the database are required. If you do not want to make use of the workflow capabilities or if your applications do not need to use the attributes of the keys in the repository, the database can be deployed on the workstation.

Workstation requirements

The workstation requires the following components:

- An IBM 4765 cryptographic coprocessor
- An IBM System x® server that supports the IBM 4765 (models change frequently)

  Consult the IBM ServerProven® list at
  http://ibm.com/systems/info/x86servers/serverproven/compat/us/xseries/upgrades/matrix.html
- SUSE Linux Enterprise Server 11 SP 2 32 bit
- License file for IBM DB2 Connect™ v9 or later (only for certain features and connection to DB2 on z/OS)
- Omnikey 3821 smart card readers

  For additional information about Omnikey smart card readers, visit
  https://www.hidglobal.com/products/readers/omnikey
- Smart cards (contact the IBM Crypto Competence Center, Copenhagen, at ccc@dk.ibm.com)

IBM DB2

The IBM Enterprise Key Management Foundation uses IBM DB2 as the database server for the key repository. The database can be deployed on IBM z/OS, Windows® 2003 Server, Windows 2008 Server, Linux, or IBM AIX®.

DB2 v 9.5 or later is required.

IBM z/OS requirements

The IBM Enterprise Key Management Foundation installation also requires that the following IBM products have been installed on the system and are customized for use in case you are connecting to a z/OS system:

- IBM DB2 for z/OS (if you have the IBM Enterprise Key Management Foundation database on z/OS)
- IBM Resource Access and Control Facility (RACF) or similar product
- IBM Enterprise COBOL for z/OS and OS/390®
- IBM High Level Assembler for IBM MVS™
- Integrated Cryptographic Service Facility (ICSF)

All versions supported by IBM are supported. Certain IBM Enterprise Key Management Foundation features may require newer versions.

Ordering information

This solution can be ordered via IBM Systems and Technology Groups, Lab Services in the US, by contacting your local IBM representative, or by contacting the IBM Crypto Competence Center, in Copenhagen, at ccc@dk.ibm.com.

Related information

For more information, see the following documents:

- IBM Redbooks: *Key Management Deployment Guide using the IBM Enterprise Key Management Foundation*, SG24-8181

  This IBM Redbooks publication is currently in development. The access information will be posted here as soon as the book becomes available.
- IBM Enterprise Key Management Foundation
  http://ibm.com/security/cccc/products/ekmf.shtml
- IBM Enterprise security on System z
  http://ibm.com/systems/z/solutions/security.html
- IBM Offering Information page (to search on announcement letters, sales manuals, or both):
  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  On this page, enter IBM Enterprise Key Management Foundation, select the information type, and then click **Search**. On the next page, narrow your search results by geography and language.

Notices

This information was developed for products and services offered in the U.S.A.

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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: 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 states 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of 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. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document was created or updated on July 12, 2013.

Send us your comments in one of the following ways:

- Use the online **Contact us** review form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

This document is available online at http://www.ibm.com/redbooks/abstracts/tips1052.html .

Trademarks