IBM Enterprise Key Management Foundation

Enterprise-wide management of keys and certificates

Highlights

- Centralise key management to help meet requirements
- Manage multiple systems with standardised set of procedures and operations
- Leverage investments in IBM® System z hardware cryptography.

In an increasingly interconnected world, data breaches grab headlines. The security of sensitive information is vital; and new requirements and regulatory bodies such as the Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX) create challenges for enterprises that use encryption to protect their information. As encryption becomes more widely adopted, organisations also must contend with an ever growing set of encryption keys. Effective management of these keys is essential to ensure both the availability and security of the encrypted information. Centralised management of keys and certificates is necessary to perform the complex tasks related to key and certificate generation, renewal, backup and recovery.

The IBM Enterprise Key Management Foundation (EKMF) is a flexible and highly secure key management system for the enterprise. It provides centralised key management on IBM zEnterprise and distributed platforms for streamlined, efficient and secure key and certificate management operations. The EKMF is well suited for banks, payment card processors and other businesses that must meet Europay, MasterCard and Visa (EMV) and payment card industry (PCI)

requirements. It includes crypto-analytic capabilities to identify compliance issues and help key officers understand who has access to key material. The EKMF provides a foundation that can be tailored to address the needs of multiple industry segments to identify compliance issues and help key officers enforce enterprise key management policy requirements.

Centralise key management

A centralised key management solution is only useful if it can supply the key and certificate formats required by the vast array of systems that service the enterprise and adhere to the policies required by regulatory agencies. The EKMF offers enterprise-wide management capabilities for certificates and both symmetric and asymmetric keys. It supports a wide variety of data encryption standard (DES), advanced encryption standard (AES) and Rivest Shamir Adleman (RSA) keys for a number of platforms and crypto cards. It ensures adherence with an array of specialised industry regulations, such as EMV for payment card solutions. The functionality of the EKMF is continuously being extended and improved in accordance with customer needs, industry standards and regulatory initiatives.

With the EKMF, keys are managed independent from target platforms. It manages keys and certificates for cryptographic coprocessors, hardware security modules (HSM), software implementations like Java™ key store, ATMs and point of sale (POS) terminals. The EKMF also offers an incentive support for EMV chip cards, both for issuers and acquirers, as well as for card brands.

Manage multiple systems

Most computing centres have several server systems, often in different geographic locations. With the EKMF, you can perform all key and certificate management functions for all the systems from a single workstation. It can support every cryptographic entity on the network, whether terminal, institution, cryptographic coprocessor or server. Each entity type has its own key hierarchy and each can be defined and managed. For cryptographic coprocessors that implement a key store, the EKMF maintains the contents of that store.

Leverage System z investments

EKMF takes advantage of the strengths of the IBM System z to deliver a flexible and highly secure, centralised key management system for the enterprise. System z has been certified to the Common Criteria Evaluation Assurance Level 5 (EAL5), the highest security rating or classification in effect for any commercially available server.

Although a number of key management appliances exit, appliances can create single points of failure (SPOF) and make it difficult to achieve highly available configurations. Keeping sensitive keys, certificates and metadata on System z leverages the business continuity and disaster recovery (DR) plans already in effect at the enterprise to help create both a highly secure and highly available centralised key repository.

Why IBM?

Many System z-based banks and card processing companies have already taken advantage of the capabilities of the EKMF to implement EMV payment cards and remote key load for endpoint devices. Initially developed in cooperation with the European banking sector, the EKMF is a mature, robust and extensible solution that can meet the stringent security and compliance requirements that are now becoming standard across multiple industry segments. This maturity translates into a solution you can trust.

For more information

To learn more about the IBM EKMF, please contact your IBM representative or IBM Business Partner (BP), or visit: **ibm.com**/systems/services/labservices/platforms/labservices_z.html

Additionally, IBM Global Financing (IGF) can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We will partner with credit-qualified clients to customise an IT financing solution to suit your business goals, enable effective cash management and improve your total cost of ownership (TCO). IGF is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing/uk

IBM United Kingdom Limited
PO Box 41
North Harbour
Portsmouth
Hampshire
PO6 3AU
United Kingdom

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland Limited registered in Ireland under company number 16226.
The IBM home page can be found at **ibm.com**

IBM, the IBM logo, ibm.com, System z and zEnterprise are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries.

A current list of IBM trademarks is available on the web at 'Copyright and trademark information' at ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product and service names may be trademarks, or service marks of others.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates.

Any reference to an IBM product, program or service is not intended to imply that only IBM products, programs or services may be used. Any functionally equivalent product, program or service may be used instead.

IBM hardware products are manufactured from new parts, or new and used parts. In some cases, the hardware product may not be new and may have been previously installed. Regardless, IBM warranty terms apply.

This publication is for general guidance only.
Information is subject to change without notice. Please contact your local IBM sales office or reseller for latest information on IBM products and services.

IBM does not provide legal, accounting or audit advice or represent or warrant that its products or services ensure compliance with laws. Clients are responsible for compliance with applicable securities laws and regulations, including national laws and regulations.

Photographs may show design models.

© Copyright IBM Corporation 2013

Please Recycle

ZSS03081-GBEN-00