Redbooks

ibm.com/redbooks

Streamline Management of the IBM z Systems Host Cryptographic Module Using IBM Trusted Key Entry

Garry J. Sullivan

Security

z Systems

IBM

Point-of-View

Securing the keys to the kingdom

Highlights

Proper management of your z Systems cryptographic modules is vital to securing your data. Your cryptographic module management system needs these capabilities:

- Grouping of domains to save time and resources
- Loading master key parts efficiently and easily
- Proper collection and application of data from a source host cryptographic module to a target host cryptographic module
- Wizards to support setup and configuration activities

Every organization has the goal and responsibility to ensure data confidentiality, integrity, and authenticity. Cryptographic systems are extensively used to provide the security needed for data transport. Cryptographic systems use keys to lock and unlock the encrypted data. The security and management of these keys is critical to the cryptographic system's viability.

Cryptographic environments can be complex, with the various domains each having its own set of master keys and access control point (ACP) settings. Remember: These keys are the most important keys for protecting your data. Many standards require that the key parts of the master keys are *never* in the clear.

For IBM® z Systems™, the Host Cryptographic Module keys are the most important keys that you have. Many standards require that the key parts of master keys never be in the clear outside of a Hardware Security Module (HSM). For z Systems, IBM Trusted Key Entry (TKE) is the appliance that keeps those key parts properly encrypted while generating key material and loading master keys.

Note: Throughout this publication, the TKE acronym refers to Trusted Key Entry.

Most businesses that use TKE put the TKE workstation in a secure room with complex procedures that require layers of approval for access. Typically, dual-control management is required, and that involves multiple people. For these reasons, it is vital to keep TKE and Host Cryptographic Module management quick, efficient, and accurate.

This IBM Redbooks® Point-of-View publication reviews the IBM Trusted Key Entry product and the four features that streamline the mission-critical tasks that are performed from TKE. Proper use of these features increases the speed and accuracy of your Host Cryptographic Module management and reduces the amount of time that you need in the TKE secure room.

Trusted Key Entry is in control

Trusted Key Entry is a fully tested and supported IBM z™ Systems appliance. It is released with z Systems hardware that is used to manage the master keys and operational keys on your Host Cryptographic Modules. Crypto Express2, Crypto Express3, and Crypto Express4 modules provide 16 domains, each with its own set of master keys and access control points governing cryptographic activity. Crypto Express5S provides even more virtualization, with up to 85 domains.

TKE gives you compliance-level, hardware-based key management with the latest encryption strengths, dual controls, and security-relevant auditing. TKE also provides secure, simplified administration of both module-wide and domain-specific settings for your modules. These settings control the security policy for managing modules and the services that can be used. With multiple modules, each providing at least 16 domains, the z Systems cryptographic configurations can be complex. TKE simplifies this situation by allowing you to group modules or domains together.

In addition, TKE allows secure and efficient movement of administrative settings from one Host Cryptographic Module to another. This approach provides fast deployment of new modules on production, test, or disaster recovery systems. TKE operates from a workstation with a local cryptographic adapter that runs the TKE software. It is a closed system, so no additional code can be installed. To have full hardware-based, compliance-level master key management, smart cards and readers are required.

Domain grouping

A z Systems Host Cryptographic Module has at least 16 domains. However, a set of domains often shares the same settings. TKE domain groups allow you to treat any set of domains, across any number of systems or logical partitions (LPARS) as though they were a single domain.

Imagine this scenario as an example: You have a single LPAR with two Crypto Express 5S modules and you want the same master keys for domains 0, 1, 2, and 3 on both modules, and you want to enable the same set of cryptographic services on both modules. In addition, you want both modules to have the same roles and authority indexes.

Without domain grouping, you need to go through the time-consuming procedure of configuring each module and each domain, one at a time, making certain that the *module-wide and domain-specific settings* are exactly the same between the different modules and domains. With domain grouping, you can define a group ID, a set of domains, and a master domain, and then configure the modules and domains from within the domain group. You can also compare the members of the group to verify that there are no mismatches between their settings.

Load All New Master Keys

Loading new master key parts has been a tedious and time-consuming process, requiring clearing of registers and separate loading of master key parts. Trusted Key Entry version 8.0 makes it possible to load all master key parts in a single process.

Loading the master key involves four basic steps:

1. Clear the new master key register, if it is not empty.
2. Load the first key part.
3. Load middle key parts, if there are any.
4. Load the last key part.

Typically, businesses have different key officers for their first, middle, and last key parts.

The Load All New Master Keys function takes you through this entire process. Officers need to supply their parts of the master key only once. The function can be started from any master key. You simply highlight a master key, right-click for options, and select **Load All New Master Keys**.

At the beginning of each step, a window opens where you can choose which keys to work with. The current step is always populated with your selections from the previous step. All commands sent to the module must be signed, including the **`clear`** command and all of the **`load`** commands. Any time that a step requires an authority signature key, you are asked for one.

The Full Function Migration Wizard

The Full Function Migration Wizard is the common name for a set of tasks that you can perform from the Configuration Migration Tasks application of TKE. This application includes two wizards that collect configuration data from a source Host Cryptographic Module and apply that data to the target Host Cryptographic Module.

The source and target modules might be on the same z Systems platform or they might be on different z Systems platforms. They can be extremely valuable if you purchase new cryptographic modules for an existing z Systems platform or if you purchase a new z Systems platform and want the new cryptographic modules as clones of existing ones. Also, if you need to replace a cryptographic module for any reason, you might want to configure the replacement with the same settings.

Without the Migration Wizard, the only way to set up a new z Systems cryptographic module is to go through all of the steps of configuring it independently, including creating roles and authority indexes, clearing and loading master key registers, and selecting which services can be used within each domain.

After the initial Full Function Migration Wizard tasks have been performed, the Collect Configuration Data Wizard takes approximately five minutes to collect all of the data from a module, no matter how many domains the module might have. An *Apply* operation also takes approximately five minutes. The time saved over a similar manual configuration of the module is enormous.

Also, the keys end up in the same state as they were during the collect operation. If your logical partitions are using key data sets (KDS) that are already encrypted under the master key, your domain is ready to use immediately.

The Trusted Key Entry Workstation Setup Wizard

TKE provides a Workstation Setup Wizard to help you set up a workstation or confirm that the workstation settings are configured correctly. The wizard gives you the opportunity to enable features that you want, including smart card readers, along with the ability to check or change existing settings, such as network settings or default passwords, and to highlight problems that you might not have noticed until you were doing a mission-critical task. The wizard takes minimal time to run and significantly reduces the time that it takes to deploy a TKE. It also helps you confirm that your workstation has been properly secured.

What's next: How IBM can help

The management of your z Systems Host Cryptographic Module environment requires efficient and secure setup and maintenance. The Trusted Key Entry Workstation Setup wizard, domain groups, Load <<All?>> New Master Keys function, and the Full Function Host Migration Wizard all simplify that management while continuing to provide the hardware-based, compliance-level features that you demand. When properly used, these features can increase the speed and accuracy of your Host Cryptographic Module management and reduce the amount of time that you need in the TKE secure room.

To help you get started, there are details about TKE in the IBM Knowledge Center. There is also an IBM TKE YouTube channel that has dozens of how-to videos, with an entire playlist dedicated to the Full Function Host Migration Wizard. The links to these resources are in the “Resources for more information” section that follows.

Resources for more information

For more information about the concepts highlighted in the paper, see the following resources:

- IBM z/OS® Cryptographic Services, IBM Knowledge Center

  http://ibm.co/1iSEuu8
- *z/OS Cryptographic Services ICSF TKE Workstation User’s Guide*, IBM Knowledge Center

  http://ibm.co/1PnKERu
- IBM TKE YouTube channel for various how-to videos

  https://www.youtube.com/user/IBMTKE

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 grant 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

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 measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US 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 http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM®	Redbooks®	z Systems™
IBM z™	Redbooks (logo)  ®	z/OS®

The following terms are trademarks of other companies:

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

REDP-5305-00

ISBN 0738454702

Printed in U.S.A.