IBM Encryption Facility for z/OS V1.2 – Program Number 5655-P97

IBM Encryption Facility for z/OS is designed to leverage the powerful encryption capabilities of the IBM mainframe to help secure files for archive or transfer purposes. Encryption is a powerful and widely used technology to help protect data from loss and inadvertent or deliberate compromise. The Encryption Facility helps you to encrypt data to tape or disk, enabling sensitive information to be transferred across platforms with partners and vendors.

Overview

IBM Encryption Facility for z/OS Version 1.2 is a program product that runs on z/OS, and is comprised of three components: IBM Encryption Services feature, IBM DFSMSdss Encryption feature, and IBM Encryption Facility for z/OS Client Web download. With Encryption Facility for z/OS Version 1.2 the IBM Encryption Services feature is enhanced to provide support for the OpenPGP Message Format standard (RFC 2440). An OpenPGP compliant system provides data integrity services for messages and data files through encryption and digital signature authentication.

The IBM Encryption Facility for z/OS can be used on z/OS and z/OS.e: Version 1 Release 6, Version 1 Release 7, and Version 1 Release 8. The IBM Encryption Facility uses the z/OS key management capabilities of z/OS Integrated Cryptographic Service Facility (ICSF) and can leverage, when installed, the hardware cryptographic and compression capabilities of IBM System z9 and zSeries servers.

The two features of IBM Encryption Facility for z/OS are priced and optional; one or both features may be ordered:
• IBM Encryption Services (FMID HCF7740)
• IBM DFSMSdss Encryption (FMID HCF773D)

The Encryption Services feature supports encrypting and decrypting certain file formats on z/OS for transfer purposes or small-volume archival purposes. The DFSMSdss Encryption feature enables the encryption of DFSMSdss DUMP data sets. Both features are designed to use ICSF to perform encryption and decryption of files and to manage cryptographic keys.

The IBM Encryption Facility for z/OS Client (Web download program) includes a Java-based Client that can decrypt the contents of tapes encrypted by the Encryption Services feature running on z/OS, and encrypt tapes to be decrypted using the Encryption Services feature on z/OS. This allows the exchange of encrypted data between z/OS systems and other operating systems. Also included is a Decryption Client component, which is designed to decrypt data that has been created through the Encryption Services feature on z/OS. The decryption component can decrypt data that has been processed using compression.

Functions

The IBM Encryption Facility for z/OS V1.2 Encryption Services feature includes a Java-based program enhancement to support the OpenPGP standard. This includes support for the following:
• All required data integrity services for OpenPGP compliance
• Compression data service
• Minimal key management capabilities
• Radix-64 conversion services for OpenPGP certificates
Encryption Facility for z/OS Version 1.2 can operate with other OpenPGP compliant systems, and also can be integrated with z/OS Integrated Cryptographic Service Facility (ICSF) and Resource Access Control Facility (RACF).

Encryption Facility 1.2 continues to support encrypting or decrypting data using the System z format, first introduced in Encryption Facility for z/OS V1.1. The new OpenPGP format, however, will not be compatible with nor maintain data set properties for data created by the System z format.

### Specified Operating Environment

#### Machine Requirements

The IBM Encryption Facility for z/OS can use the hardware cryptographic capabilities (when installed) of IBM mainframe servers. The options that you specify for encryption and decryption, including cryptographic keys, depend on the processor type and the cryptographic hardware that you have installed on the system.

The IBM Encryption Facility for z/OS Version 1.2 runs on:

- System EC z9, BC z9, z990, z890, z900 with the CPACF cryptographic hardware
- EC z9 with and without secure key cryptographic cards
- BC z9 with and without secure key cryptographic cards
- z990s with and without secure key cryptographic cards
- z890s with and without secure key cryptographic cards
- z900s with and without secure key cryptographic cards
- z800s with and without CCFs

#### Software Requirements

**IBM Encryption Facility Version 1.2** has the following software requirements:

The *Encryption Services feature* of Encryption Facility for z/OS requires:

- z/OS (5694-A01) or z/OS.e (5655-G52) V1.6 or later release.
- PTF for z/OS DFSMS APAR OA09868 and QSAM APAR OA13571.
- PTF for z/OS V1.6 APAR OA10229.
- Integrated Cryptographic Services Facility (ICSF) Web deliverable (FMID HCR7720 or later release)
- PTF for ICSF in support of CFB mode APAR OA19177 for Encryption Facility for OpenPGP

The functions and services of Encryption Facility for OpenPGP of Encryption Services for z/OS V1.2 are not compatible with the System z functions and services of Encryption Facility for z/OS.

The *DFSMSdss Encryption feature* of Encryption Facility for z/OS requires:

- z/OS (5694-A01) or z/OS.e (5655-G52) V1.6 or later release
- Integrated Cryptographic Services Facility (ICSF) Web deliverable (FMID HCR7720 or later release)
- The DFSMSdss priced feature of z/OS V1.6 or z/OS.e V1.6 or later release
- PTF for z/OS DFSMS APARs OA13300, OA13453, and OA13687

The *Encryption Facility for z/OS Client*: The software requirements for the decryption client are the same as the Encryption Services feature System z format (provided in Encryption Facility for z/OS Version 1.1). The decryption component of Encryption Facility for z/OS Client only runs on z/OS and provides only decryption services.
The Java client has additional requirements. To run on z/OS, one of the following is required:

- IBM SDK for z/OS, Java 2 Technology Edition, 5655-I56, at PTF UQ90449 or later (SDK1.4.2)
- IBM Developer Kit for OS/390®, Java 2 Technology Edition, 5655-D35, at PTF UQ88094 or later (SDK1.3.1)

To run on other platforms, one of the following is required:

- Sun SDK 5.0
- An IBM JVM at SDK1.4.2
- A JVM with a JCE cryptographic provider installed that supports all the required algorithms. See Encryption Facility Client documentation for details on the algorithms, modes, and padding schemes needed.

For complete information on Encryption Facility for z/OS Client, see the following Web site: http://www.ibm.com/servers/eserver/zseries/zos/downloads/#asis. For the Java-based program, including PTF requirements for iSeries™ or other platforms, see the README file in the Java reference code for Encryption Facility for z/OS Client on the same Website.

**z/OS Cryptographic Services** requires:

- ICSF in z/OS 1.7 base (HCR7720) or z/OS 1.8 base (HCR7731)
- ICSF 64-bit Virtual Support for z/OS V1.6 and z/OS.e V1.6 (HCR7720)
- Cryptographic Support for z/OS V1R6/R7 and z/OS.e V1R6/R7 (HCR7730)
- Cryptographic Support for z/OS V1R8 and z/OS.e V1R8 (HCR7731)

**Security Server (RACF)** requires:

The optional PTF for Security Server (RACF) APAR OA13030 to perform the following:

- Use the RACF RACDCERT command to allow the storage of RSA public keys in the ICSF PKDS
- Specify the PKDS labels to be used when storing public or private keys in the PKDS
- List the PKDS labels of existing certificates

For additional information, see IBM Encryption Facility for z/OS: Planning and Customizing, SA23-2229, and Encryption Facility for z/OS: Using Encryption Facility for OpenPGP, SA23-2230.

---

**Licensed Program Materials Availability**

Restricted materials - Yes.

This licensed program is available with source licensed program materials for some modules designated as "RESTRICTED MATERIALS OF IBM." The remaining licensed programming materials are available and are not designated as "RESTRICTED MATERIALS OF IBM."

---

**Supplemental Terms**

**Designated Machine Identification**

Designated Machine Identification Required - Yes.

**Program Features Not Used on the Designated Machine**

Not applicable.
Installation/Location License
You can install IBM Encryption Facility for z/OS V1.2 and use either of the optional features:
- Encryption Services
- DFSMSdss Encryption

And you can download the Encryption Facility for z/OS Client from the IBM World-wide Web site at the following URL: http://www-03.ibm.com/servers/eserver/zseries/zos/downloads/#asis

For detailed installation information, read the IBM Encryption Facility for z/OS Program Directory.

Charges/Usage Restriction
Ordering information and charges will be available through the Offering Information Web site. Registered external customers and IBM Business Partners can access IBMLink for ordering information and charges.

In a Parallel Sysplex the charge for all copies is associated to one license by specifying the applicable PSLC license options and quantity represented by the sum of the Service Units in Millions (MSUs) in your Parallel Sysplex. For all other program copies, specify the System Usage Registration No-Charge Identifier on the licenses.

Type/Duration of Program Services
The Encryption Facility for z/OS is a separately licensed product. Program service, including the IBM® Support Center, will be available until discontinued by IBM upon twelve month’s written notice.

For assistance with Java, contact your Java provider, or IBM Java user assistance at http://www.ibm.com/deveoperworks/java.

Softcopy Publications
z/OS and z/OS.e include publications that are delivered in displayable form. Except as provided in this section, the terms and conditions of the license agreement with IBM apply to these publications and to any copies that are made from them.

Related publications include:
- IBM Encryption Facility for z/OS Planning and Customizing, SA23-2229
- IBM Encryption Facility for z/OS: Using Encryption Facility for OpenPGP, SA23-2230
- IBM Encryption Facility for z/OS Licensed Programming Specification, GA76-0419
- IBM Encryption Facility for z/OS Program Directory, GI10-0771

One copy of the program directory and the LPS are supplied automatically with the basic machine-readable material.

Refer to the IBM Publications Center website for more information about publication ordering: http://www.ibm.com/shop/publications/order

Additional Supplemental Terms
Excluded Components
Not applicable.

Separately Licensed Code
Not applicable
Warranty

These Licensed Program Specifications may be updated from time to time and such updates may constitute a change in warranty specifications. Warranty service, if any, will be provided only through the Basic License location.

Following the discontinuance of program services, this program will be provided "AS IS", as specified in the IBM license.

The IBM Encryption Facility for z/OS Client, which is a no-charge Web download, is provided "AS IS".

Trademarks

The following are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both: IBM, z/Architecture™, z/OS™, z/OS.e™, iSeries™ and zSeries.

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

PGP is a trademark of the PGP Corporation in the United States, other countries, or both.

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 state or imply that only IBM’s product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM’s intellectual property rights may be used instead of the IBM product, program, or service. Any other documentation with respect to this licensed program, including any documentation referenced herein, is provided for reference purposes only and does not extend or modify these specifications.

March 2007

GA76-0419-00