Encryption Facility for z/OS
Version 1 Release 2

Encryption Facility for OpenPGP zEnterprise Data Compression (zEDC) Support - APAR OA43869

Contents

Chapter 1. Overview

This document describes changes to the IBM Encryption Facility for z/OS product so that zEnterprise Data Compression (zEDC) can be used for compression of OpenPGP messages when the zEDC Express feature is available on the system and when using IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 or later.

A new command, **-compress**, is added that compresses data in the OpenPGP message format without having to also encrypt or sign the data. Previously, Encryption Facility for OpenPGP performed compression only before it produced an encrypted or signed OpenPGP message. The **-d** (decrypt or decompress an OpenPGP message) command has been updated to decompress an OpenPGP message containing only compressed data in the OpenPGP message format.

This APAR also includes the following fixes:

- Encryption Facility for OpenPGP has been updated to prevent null pointer exceptions when null parameters are processed by the trace facility.
- Encryption Facility OpenPGP keyring is no longer required nor attempted to be read when only using the RECIPIENT_ALIAS (**-rA**) option for encryption.
- The iteration count calculation has been corrected when the encoded value is larger than 127 for the decryption of OpenPGP messages using the salted and iterated option in string-to-key (S2K) mode for passphrase-based encryption (PBE).

These changes are available through the application of the PTF for APAR OA43869. This document contains alterations to information previously presented in *IBM Encryption Facility for z/OS: Using Encryption Facility for OpenPGP*, SA23-2230-05.

The technical changes made to the IBM Encryption Facility for z/OS product by the application of the PTF for APAR OA43869 are indicated in this document by a vertical line to the left of the change.

Chapter 2. Update of IBM Encryption Facility for z/OS: Using Encryption Facility for OpenPGP, SA23-2230-05, information

This topic contains updates to the document *IBM Encryption Facility for z/OS: Using Encryption Facility for OpenPGP*, SA23-2230-05, for zEnterprise Data Compression (zEDC) support provided by the PTF for APAR OA43869. Refer to this source document if background information is needed.

Compressing data

Compressing data before encryption can make the encryption more efficient. In compliance with OpenPGP standards that recommends compressing data for encryption, Encryption Facility for OpenPGP supports compression and decompression of OpenPGP messages and other data.

Encryption Facility for OpenPGP also supports zEnterprise Data Compression (zEDC). In order for Encryption Facility for OpenPGP to use the zEDC feature, you must be using IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 or later. zEDC also requires the following:

- z/OS V2R1 operating system.
- IBM zEnterprise EC12 (with GA2 level microcode) or IBM zEnterprise zBC12.
- zEDC Express adapter.

Note: zEDC requires a minimum input buffer size for compression and decompression. If the input data is smaller than the minimum threshold, the data is processed using traditional software-based compression and decompression.

For additional information about zEDC, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Java algorithm support for Encryption Facility for OpenPGP

Compression algorithm support: Table 1 summarizes the type of compression algorithms that Encryption Facility for OpenPGP uses and where they are supported for OpenPGP:

Table 1. Compression algorithm support

Compression algorithm	Support for compression algorithm
ZIP	IBM® Java™ Development Kit (SDK)
ZLIB	IBM Java Development Kit (SDK)

Note: Encryption Facility for OpenPGP uses the zEDC feature for compression if available and running with the required level of Java (IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 or later).

zEDC requires a minimum input buffer size for compression and decompression. If the input data is smaller than the minimum threshold, the data is processed using traditional software-based compression and decompression.

For additional information about zEDC, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

-compress — Compress data in OpenPGP message format

Format

-compress *file*

Description

This command compresses data in OpenPGP message format. This command does not sign nor encrypt the data after it is compressed. Use the Encryption Facility **-d** command to decompress the output from this command.

Use the **-z** command option with this command to specify a compression level. If a compression level is not specified, the compression level of 9 is used in order to perform the best compression.

Use the **-compress-name** command option with this command to specify a compression algorithm. If a compression algorithm is not specified, the ZIP compression algorithm is used.

Encryption Facility for OpenPGP uses the zEDC feature for compression if available and running with the required level of Java (IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 or later).

zEDC requires a minimum input buffer size for compression and decompression. If the input data is smaller than the minimum threshold, the data is processed using traditional software-based compression and decompression.

For additional information about zEDC, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Arguments

For *file*, a valid file name for the data to be compressed.

-d — Decrypt or decompress an OpenPGP message

Format

-d *file* [*file* . . .]

Description

This command decrypts one or more encrypted OpenPGP messages.

Consider using the configuration file option USE_EMBEDDED_FILENAME or the **-use-embeeded-filename** command option, or the configuration file option CONFIDENTIAL or **-no-save** command option with this command. Otherwise, the specified file or data set specified on OUTPUT_FILE or on the **-o** command option is overwritten with the last file that you specify as input on the **-d** command.

Use this command to decompress an OpenPGP message containing only compressed data in the OpenPGP message format. The input OpenPGP message is not required to be encrypted in order for this command to perform decompression.

Encryption Facility for OpenPGP uses the zEDC feature for compression if available and running with the required level of Java (IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 or later).

zEDC requires a minimum input buffer size for compression and decompression. If the input data is smaller than the minimum threshold, the data is processed using traditional software-based compression and decompression.

For additional information about zEDC, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Arguments

For *file*, one or more valid file names for data to be decrypted, decompressed, or both.

Printed in USA