Encryption Facility for z/OS
Version 1 Release 2

Encryption Facility for OpenPGP Data set support using the IBM JZOS Batch Toolkit - APAR OA46232

Contents

Chapter 1. Overview

This document describes changes to the IBM Encryption Facility for z/OS (FMID HCF7740) product due to an internal migration from using the IBM JRIO component for data set I/O to the JZOS component for data set I/O. IBM 31-bit SDK for z/OS, Java Technology Edition, Version 8, has removed the JRIO component, which in effect requires all previous exploiters to migrate over to the IBM JZOS Batch Toolkit. Encryption Facility's support for the IBM JZOS Batch Toolkit is effective when running with all in-service releases of IBM Java SDKs, not just Java Technology Edition, Version 8. This support enables IBM Encryption Facility for z/OS to continue reading and writing OpenPGP messages and OpenPGP certificates to data sets with all in-service levels of IBM Java SDKs, including Java Technology Edition, Version 8, and later.

Specifying a provider through the JCE_PROVIDER_LIST/-jce-providers command options may not be honored if the provider had already been defined within the java.security file in a particular order. The IBM Encryption Facility for z/OS product provides the ability to override the security provider configuration defined in the java.security file. A fix has been added to the logic that configures the security provider to ensure it is being honored.

These changes are available through the application of the PTF for APAR OA46232. This document contains alterations to information previously presented in *IBM Encryption Facility for z/OS: Using Encryption Facility for OpenPGP*, SA23-2230-06.

The technical changes made to the IBM Encryption Facility for z/OS product by the application of the PTF for APAR OA46232 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, SA23-2230-06, information

This topic contains updates to the document *IBM Encryption Facility for z/OS: Using Encryption Facility for OpenPGP*, SA23-2230-06, for data set support using the IBM JZOS Batch Toolkit provided by the PTF for APAR OA46232. Refer to this source document if background information is needed.

Using z/OS data sets

Encryption Facility for OpenPGP allows you to use z/OS® data as input or output for OpenPGP encryption and decryption services. Encryption Facility for OpenPGP uses the IBM® JZOS component to read and write to z/OS data sets and accepts the following kinds of z/OS data sets:

- Sequential data sets.
- Partitioned data sets (PDS) and partitioned data sets extended (PDSE).
- Large data sets (DSNTYPE=LARGE) for z/OS V1R8 with Encryption Facility APAR OA22067 applied or later releases.

Encryption Facility for OpenPGP does NOT accept VSAM data sets as input. All z/OS output data sets must be preallocated. See "Reading and writing to z/OS data sets."

Reading and writing to z/OS data sets

Encryption Facility for OpenPGP allows you to use data from z/OS data sets that you can then process on any OpenPGP-compliant system. Encryption Facility for OpenPGP uses the JZOS component to access z/OS data sets.

Other data set considerations

If you plan to use z/OS data sets for OpenPGP encryption, consider the following:

- Ensure that ICSF is active on the z/OS system.
- Ensure that users have access to the UNIX System Services files.
- Use the necessary JCL to run batch programs that use Encryption Facility services. Encryption Facility V1R2 ships sample JCL and an environment file. This JCL leverages the Java™ batch component of the IBM Java SDK. For more information, see http://www-03.ibm.com/systems/z/os/zos/tools/java/.

Encryption Facility considerations when changing Java release levels

IBM Java Technology Edition, Version 7 Release 1 and earlier allowed for the creation of and the use of X.509 certificates with a null distinguished name (DN). X.509 certificates with a null DN are invalid because they are essentially certificates with no identity and may not be accepted by other products. While it is unlikely that you would be using an X.509 certificate with a null DN, it is possible. Because IBM Java Technology Edition, Version 8 and later no longer supports X.509 certificates with a null DN, Java keystores will not load and are unusable if they contain a null DN. Therefore, X.509 certificates with a null DN must be removed prior to migrating to IBM Java Technology Edition, Version 8 or later.

Before migrating to IBM Java Technology Edition, Version 8 or later, use Encryption Facility's list commands (-pA or -pK) to determine if you have any X.509 certificates with a null DN and then use Encryption Facility's delete commands (-xA or -xK) to remove them.

If you migrate to IBM Java Technology Edition, Version 8 or later before removing all X.509 certificates with a null DN, you will need to remove these with other tooling (for example, Java keytool) or migrate back to your previous IBM Java level and use Encryption Facility's delete commands (-xA or -xK) to remove them.

With the latest level of service, Encryption Facility checks for and does not allow the creation of a X.509 certificate with a null DN.

Note: IBM Java keystores created with IBM Java Technology Edition, Version 7 or later cannot be accessed by IBM Java Technology Edition, Version 6.0.1 or earlier due to stronger encryption. Once you have migrated to IBM Java Technology Edition, Version 7 or later, it is not recommended that you migrate to a prior IBM Java version.

For more information, see http://www-01.ibm.com/support/docview.wss?uid=isg3T1022007.

Note: Before deleting an X.509 certificate, ensure that you do not have data encrypted using the public key within it. Data encrypted using the public key must be decrypted and then encrypted using another public key before you delete the X.509 certificate and its public key.

Sample JCL and code

```
# Uncomment the following if you want to run with trace from hardware crypto
# provider
#export IBM_JAVA_OPTIONS="$IBM_JAVA_OPTIONS -Djava.security.auth.debug=all"

# Uncomment the following if you want to run with trace from the JZOS
# component
#export IBM_JAVA_OPTIONS="$IBM_JAVA_OPTIONS -Djzos.logging=T"
#export IBM_JAVA_OPTIONS="$IBM_JAVA_OPTIONS -Djzos.merge.sysout=true"

export JAVA_DUMP_HEAP=false
export IBM_JAVA_ZOS_TDUMP=NO

# Required to correctly read ASCII armor data sets since ASCII armor data sets
# contain some 0 byte records
export _EDC_ZERO_RECLEN=Y
```

Figure 1. Sample code for the Java environment (continued)

Encryption Facility for OpenPGP messages

New Encryption Facility for OpenPGP messages:

CSD1409I Referencing a PDS or PDSE data set without a member name is not supported.

Explanation: You cannot specify a PDS or PDSE data set without a member name.

System action: Encryption Facility ends with a non-zero return code.

User response: Specify a member name within the PDS or PDSE data set.

CSD1410I The supplied input and output sources must be different.

Explanation: You cannot specify the same source for input and output.

System action: Encryption Facility ends with a non-zero return code.

User response: Ensure that the command input and output specified by either the -o command option or the OUTPUT_FILE configuration option are different.

CSD1411I The supplied input sources must be different.

Explanation: You cannot specify the same source of input for a command that takes multiple arguments.

System action: Encryption Facility ends with a non-zero return code.

User response: Ensure that the source for each input that is supplied to the command are different.

CSD1412I The distinguished name information supplied for the certificate was not valid. You must supply at least one field.

Explanation: During certificate generation, you are required to supply at least one valid field for the distinguished name (DN).

System action: Encryption Facility waits for you to enter a valid DN. If batch processing is enabled, Encryption Facility ends with a non-zero return code.

User response: Ensure that you supply at least one valid field for the DN through either the command prompt or the -dn-* command options or DN_* configuration options.

CSD1413I A certificate with the following alias *alias_name* has an empty subject distinguished name. Replace the certificate with one containing a valid subject distinguished name.

Explanation: A certificate with an empty subject distinguished name was encountered during command processing.

In the message text:

alias_name
Alias name.

System action: Processing continues.

User response: Remove the certificate and replace the certificate with one containing a valid subject distinguished name. Any certificate with an empty subject distinguished name will not be usable with Java Technology Edition, Version 8 or later, and will prevent the entire keystore from being loaded.

CSD1414I A certificate with the following alias *alias_name* has an empty issuer distinguished name. Replace the certificate with one containing a valid issuer distinguished name.

Explanation: A certificate with an empty issuer distinguished name was encountered during command processing.

In the message text:

alias_name
Alias name.

System action: Processing continues.

User response: Remove the certificate and replace the certificate with one containing a valid issuer distinguished name. Any certificate with an empty issuer distinguished name will not be usable with Java Technology Edition, Version 8 or later, and will prevent the entire keystore from being loaded.

CSD1415I A certificate within the keystore has a non-valid or missing subject or issuer distinguished name and was unable to load. Replace the certificate with one containing a valid subject or issuer distinguished name.

Explanation: A certificate with an empty or non-valid distinguished name was encountered during command

processing which prevented the entire keystore from being loaded when running with Java Technology Edition, Version 8 or later.

System action: Encryption Facility ends with a non-zero return code.

User response: Remove the certificates and replace the certificates with ones containing a valid distinguished name. Encryption Facility will only be able to process a keystore containing certificates with valid distinguished names while running Java Technology Edition, Version 8 or later.

Printed in USA