Program Directory for
IBM Encryption Facility
for z/OS

V1.2.0

Program Number 5655-P97

FMIDs HCF7740, HCF773D

for Use with
z/OS V1.6 or z/OS.e V1.6 and higher

Service Updated 11 January 2019

Document Date: January 2019

GI10-0771-03

Note

Before using this information and the product it supports, be sure to read the general information under 7.0, “Notices” on page 27.

A form for reader's comments appears at the back of this publication. When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 2005, 2019.**
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

1.0 Introduction . . . 1
1.1 IBM Encryption Facility Description . . . 1
1.2 IBM Encryption Facility FMIDs . . . 2

2.0 Program Materials . . . 3
2.1 Basic Machine-Readable Material . . . 3
2.2 Program Publications . . . 4
2.3 Program Source Materials . . . 4
2.4 Publications Useful During Installation . . . 4

3.0 Program Support . . . 5
3.1 Program Services . . . 5
3.2 Preventive Service Planning . . . 5
3.3 Statement of Support Procedures . . . 6

4.0 Program and Service Level Information . . . 7
4.1 Program Level Information . . . 7
4.2 Service Level Information . . . 7

5.0 Installation Requirements and Considerations . . . 9
5.1 Driving System Requirements . . . 9
5.1.1 Machine Requirements . . . 9
5.1.2 Programming Requirements . . . 9
5.2 Target System Requirements . . . 10
5.2.1 Machine Requirements . . . 11
5.2.2 Programming Requirements . . . 12
5.2.2.1 Installation Requisites . . . 12
5.2.2.2 Operational Requisites . . . 13
5.2.2.3 Toleration/Coexistence Requisites . . . 15
5.2.2.4 Incompatibility (Negative) Requisites . . . 15
5.2.3 DASD Storage Requirements . . . 15
5.3 FMIDs Deleted . . . 17
5.4 Special Considerations . . . 18

6.0 Installation Instructions . . . 19
6.1 Installing IBM Encryption Facility . . . 19
6.1.1 SMP/E Considerations for Installing IBM Encryption Facility . . . 19
6.1.2 SMP/E Options Subentry Values . . . 19
6.1.3 SMP/E CALLLIBS Processing . . . 20
6.1.4 Sample Jobs . . . 20
6.1.5 Perform SMP/E RECEIVE . . . 21
6.1.6 Allocate SMP/E Target and Distribution Libraries . . . 21

© Copyright IBM Corp. 2005, 2019

6.1.7 Allocate File System Paths . . . 21
6.1.8 Create DDDEF Entries . . . 22
6.1.9 Perform SMP/E APPLY . . . 22
6.1.10 Perform SMP/E ACCEPT . . . 23
6.1.11 Run REPORT CROSSZONE . . . 24
6.1.12 Cleaning Up Obsolete Data Sets, Paths, and DDDEFs . . . 24
6.2 Installing IBM Encryption Facility - DFSMSdss Encryption Feature . . . 24
6.3 Activating IBM Encryption Facility . . . 24
6.4 Product Customization . . . 25

7.0 Notices . . . 27
7.1 Trademarks . . . 27

Reader's Comments . . . 31

Figures

1. Program File Content . . . 3
2. Basic Material: Unlicensed Publications . . . 4
3. Publications Useful During Installation . . . 4
4. PSP Upgrade and Subset ID . . . 5
5. Component IDs . . . 6
6. Driving System Software Requirements . . . 10
7. Target System Mandatory Installation Requisites . . . 12
8. Target System Mandatory Operational Requisites . . . 13
9. Target System Conditional Operational Requisites . . . 14
10. Install Logic for Encryption Facility DFSMSdss Encription . . . 14
11. Total DASD Space Required by IBM Encryption Facility . . . 15
12. Storage Requirements for IBM Encryption Facility Target Libraries . . . 17
13. IBM Encryption Facility File System Paths . . . 17
14. Storage Requirements for IBM Encryption Facility Distribution Libraries . . . 17
15. SMP/E Options Subentry Values . . . 19
16. Sample Installation Jobs . . . 20

1.0 Introduction

This program directory is intended for system programmers who are responsible for program installation and maintenance. It contains information about the material and procedures associated with the installation of IBM Encryption Facility for z/OS. This publication refers to IBM Encryption Facility for z/OS as IBM Encryption Facility.

The Program Directory contains the following sections:

- 2.0, “Program Materials” on page 3 identifies the basic program materials and documentation for IBM Encryption Facility.
- 3.0, “Program Support” on page 5 describes the IBM support available for IBM Encryption Facility.
- 4.0, “Program and Service Level Information” on page 7 lists the APARs (program level) and PTFs (service level) that have been incorporated into IBM Encryption Facility.
- 5.0, “Installation Requirements and Considerations” on page 9 identifies the resources and considerations that are required for installing and using IBM Encryption Facility.
- 6.0, “Installation Instructions” on page 19 provides detailed installation instructions for IBM Encryption Facility. It also describes the procedures for activating the functions of IBM Encryption Facility, or refers to appropriate publications.

Before installing IBM Encryption Facility, read the *CBPDO Memo To Users* and the *CBPDO Memo To Users Extension* that are supplied with this program in softcopy format and this program directory; after which, keep the documents for your reference. Section 3.2, “Preventive Service Planning” on page 5 tells you how to find any updates to the information and procedures in this program directory.

IBM Encryption Facility is supplied in a Custom-Built Product Delivery Offering (CBPDO, 5751-CS3). The program directory that is provided in softcopy format on the CBPDO is identical to the hardcopy format if one was included with your order. All service and HOLDDATA for IBM Encryption Facility are included on the CBPDO.

Do not use this program directory if you install IBM Encryption Facility with a SystemPac or ServerPac. When you use one of those offerings, use the jobs and documentation supplied with the offering. The offering will point you to specific sections of this program directory as needed.

1.1 IBM Encryption Facility Description

IBM Encryption Facility for z/OS will address the requirements of IBM's z/OS customers to encrypt files for archive or for transfer purposes. IBM Encryption Facility for z/OS is a program product which runs on z/OS or z/OS.e and makes use of the z/OS Integrated Cryptographic Service Facility (ICSF) to perform encryption and decryption of files and to manage cryptographic keys.

© Copyright IBM Corp. 2005, 2019

IBM Encryption Facility for z/OS supports encryption of data using Triple Data Encryption Standard (TDES) triple length keys or 128-bit Advanced Encryption Standard (AES) keys. Additionally, IBM Encryption Facility for z/OS for OpenPGP also supports encryption of data using 128 bit Blowfish keys. Once an encrypted file has been created, it contains in a specialized header enough information to recover the encrypted file. Files encrypted with IBM Encryption Facility for z/OS can be encrypted such that the encrypted file and its associated secure encryption key will survive multiple master key changes in the cryptographic hardware at the originating or target systems. Given this characteristic, archive files can be created and recovered even years later if need be.

IBM Encryption Facility for z/OS supports physical sequential input files of format (RECFM) F(ixed), V(ariable), and U(ndefined) with or without the B(locked) A(sa) or M(achine) formats. It also supports an individual member of a PDS or PDSE. The Encryption Facility can optionally compress input data before encrypting it and writing it to the output medium. The output is a sequential file with a block size that the user can specify. Output that is written to a tape/cartridge can be written using the large block interface to optimize performance and media space.

Encryption Facility for OpenPGP provides data integrity services for messages and data files in accordance with the OpenPGP standards as described in Internet Draft standard RFC 2440. These services allow for data confidentiality, sender authentication, and non-repudiation.

IBM Encryption Facility for z/OS is made up of the following features:

- Encryption Facility Encryption Services Feature
- Encryption Facility DFSMSdss Encryption Feature

Each of the features can be ordered separately, or together as a single package. There are no install interdependencies between the features.

1.2 IBM Encryption Facility FMIDs

IBM Encryption Facility consists of the following FMIDs:

HCF7740
HCF773D

2.0 Program Materials

An IBM program is identified by a program number. The program number for IBM Encryption Facility is 5655-P97.

Basic Machine-Readable Materials are materials that are supplied under the base license and are required for the use of the product.

The program announcement material describes the features supported by IBM Encryption Facility. Ask your IBM representative for this information if you have not already received a copy.

2.1 Basic Machine-Readable Material

The distribution medium for this program is physical media or downloadable files. This program is in SMP/E RELFILE format and is installed by using SMP/E. See 6.0, “Installation Instructions” on page 19 for more information about how to install the program.

You can find information about the physical media for the basic machine-readable materials for IBM Encryption Facility in the *CB ServerPac Installing Your Order*.

Figure 1 describes the program file content for IBM Encryption Facility.

Notes:

1. The data set attributes in this table must be used in the JCL of jobs that read the data sets. However, because the data sets are in IEBCOPY unloaded format, their actual attributes might be different.
2. If any RELFILEs are identified as PDSEs, ensure that SMPTLIB data sets are allocated as PDSEs.

Figure 1. Program File Content

Name	ORG	RECFM	LRECL	BLK SIZE
SMPMCS	SEQ	FB	80	6400
IBM.HCF7740.F1	PDS	FB	80	8800
IBM.HCF7740.F2	PDS	FB	80	8800
IBM.HCF7740.F3	PDS	VB	255	6475
IBM.HCF7740.F4	PDS	U	0	6144

© Copyright IBM Corp. 2005, 2019

2.2 Program Publications

The following sections identify the basic publications for IBM Encryption Facility.

Figure 2 on page 4 identifies the basic unlicensed publications for IBM Encryption Facility. Those that are in softcopy format publications can be obtained from the IBM Publications Center website at http://www.ibm.com/shop/publications/order/.

Figure 2. Basic Material: Unlicensed Publications

Publication Title	Form Number
Encryption Facility for z/OS Planning and Customizing	SA23-2229
Encryption Facility for z/OS Using Encryption Facility for OpenPGP	SA23-2230

2.3 Program Source Materials

No program source materials or viewable program listings are provided for IBM Encryption Facility.

2.4 Publications Useful During Installation

You might want to use the publications listed in Figure 3 during the installation of IBM Encryption Facility.

Figure 3. Publications Useful During Installation

Publication Title	Form Number	Media Format
IBM SMP/E for z/OS User's Guide	SA23-2277	http://www.ibm.com/shop/publications/order/
IBM SMP/E for z/OS Commands	SA23-2275	http://www.ibm.com/shop/publications/order/
IBM SMP/E for z/OS Reference	SA23-2276	http://www.ibm.com/shop/publications/order/
IBM SMP/E for z/OS Messages, Codes, and Diagnosis	GA32-0883	http://www.ibm.com/shop/publications/order/

3.0 Program Support

This section describes the IBM support available for IBM Encryption Facility.

3.1 Program Services

Contact your IBM representative for specific information about available program services.

3.2 Preventive Service Planning

Before you install IBM Encryption Facility, make sure that you have reviewed the current Preventive Service Planning (PSP) information. Review the PSP Bucket for General Information, Installation Documentation, and the Cross Product Dependencies sections. For the Recommended Service section, instead of reviewing the PSP Bucket, it is recommended you use the IBM.PRODUCTINSTALL-REQUIREDSERVICE fix category in SMP/E to ensure you have all the recommended service installed. Use the **FIXCAT(IBM.PRODUCTINSTALL-REQUIREDSERVICE)** operand on the **APPLY CHECK**command. See 6.1.9, “Perform SMP/E APPLY” on page 22 for a sample APPLY command

If you obtained IBM Encryption Facility as part of a CBPDO, HOLDDATA is included.

If the CBPDO for IBM Encryption Facility is older than two weeks by the time you install the product materials, you can obtain the latest PSP Bucket information by going to the following website:

http://www14.software.ibm.com/webapp/set2/psearch/ search?domain=psp

You can also use S/390 SoftwareXcel or contact the IBM Support Center to obtain the latest PSP Bucket information.

For program support, access the Software Support Website at http://wwww.ibm.com/support/.

PSP Buckets are identified by UPGRADEs, which specify product levels; and SUBSETs, which specify the FMIDs for a product level. The UPGRADE and SUBSET values for IBM Encryption Facility are included in Figure 4.

Figure 4. PSP Upgrade and Subset ID

UPGRADE	SUBSET	Description
ZOSEFV1R2	HCF7740/1902	IBM Encryption Facility for z/OS
ZOSEFV1R2	EFES7740	IBM Encryption Facility for z/OS V1.2 - Encryption Services
ZOSEFV1R1	EFDSS773D	IBM Encryption Facility for z/OS V1.1 - DFSMSdss Encryption Feature

© Copyright IBM Corp. 2005, 2019

3.3 Statement of Support Procedures

Report any problems which you feel might be an error in the product materials to your IBM Support Center. You may be asked to gather and submit additional diagnostics to assist the IBM Support Center in their analysis.

Figure 5 on page 6 identifies the component IDs (COMPID) for IBM Encryption Facility.

Figure 5. Component IDs

FMID	COMPID	Component Name	RETAIN Release
HCF7740	5752XXFIL	Encryption Facility for z/OS	740
HCF773D	5752XXFIL	Encryption Facility for z/OS	73D

4.0 Program and Service Level Information

This section identifies the program and relevant service levels of IBM Encryption Facility. The program level refers to the APAR fixes that have been incorporated into the program. The service level refers to the PTFs that have been incorporated into the program.

This program is at Service Updated 11 January 2019.

4.1 Program Level Information

The following APAR fixes against previous releases of IBM Encryption Facility have been incorporated into this release. They are listed by FMID.

- FMID HCF7740

UA33757	UA76649
UA57672	UA97313

4.2 Service Level Information

PTFs containing APAR fixes against this release of IBM Encryption Facility have been incorporated into this product package. For a list of included PTFs, examine the ++VER statement in the product's SMPMCS.

Frequently check the IBM Encryption Facility PSP Bucket for HIPER and SPECIAL attention PTFs against all FMIDs that you must install. You can also receive the latest HOLDDATA, then add the **FIXCAT(IBM.PRODUCTINSTALL-REQUIREDSERVICE)** operand on your **APPLY CHECK** command. This will allow you to review the recommended and critical service that should be installed with your FMIDs.

© Copyright IBM Corp. 2005, 2019

5.0 Installation Requirements and Considerations

The following sections identify the system requirements for installing and activating IBM Encryption Facility. The following terminology is used:

- *Driving system*: the system on which SMP/E is executed to install the program.

  The program might have specific operating system or product level requirements for using processes, such as binder or assembly utilities during the installation.

- *Target system*: the system on which the program is configured and run.

  The program might have specific product level requirements, such as needing access to the library of another product for link-edits. These requirements, either mandatory or optional, might directly affect the element during the installation or in its basic or enhanced operation.

In many cases, you can use a system as both a driving system and a target system. However, you can make a separate IPL-able clone of the running system to use as a target system. The clone must include copies of all system libraries that SMP/E updates, copies of the SMP/E CSI data sets that describe the system libraries, and your PARMLIB and PROCLIB.

Use separate driving and target systems in the following situations:

- When you install a new level of a product that is already installed, the new level of the product will replace the old one. By installing the new level onto a separate target system, you can test the new level and keep the old one in production at the same time.
- When you install a product that shares libraries or load modules with other products, the installation can disrupt the other products. By installing the product onto a separate target system, you can assess these impacts without disrupting your production system.

If your order contains both features, HCF7740 and HCF773D, they may be installed concurrently.

5.1 Driving System Requirements

This section describes the environment of the driving system required to install IBM Encryption Facility.

5.1.1 Machine Requirements

The driving system can run in any hardware environment that supports the required software.

5.1.2 Programming Requirements

© Copyright IBM Corp. 2005, 2019

Figure 6. Driving System Software Requirements

Program Number	Product Name	Minimum VRM	Minimum Service Level will satisfy these APARs	Included in the shipped product?
Any **one** of the following:				
5694-A01	z/OS	V1.6 or higher	N/A	No
5655-G52	z/OS.e	V1.6 or higher	N/A	No
5694-A01	z/OS	V01.13.00 or higher	N/A	No
5650-ZOS	z/OS	V02.01.00 or higher	N/A	No
And				
5655-G44	IBM SMP/E	V3.2 or higher	N/A	No

Note: SMP/E is a requirement for Installation and is an element of z/OS but can also be ordered as a separate product, 5655-G44, minimally V03.06.00.

Note: Installation might require migration to new z/OS releases to be service supported. See https://www-01.ibm.com/software/support/lifecycle/index_z.html.

IBM Encryption Facility is installed into a file system, either HFS or zFS. Before installing IBM Encryption Facility, you must ensure that the target system file system data sets are available for processing on the driving system. OMVS must be active on the driving system and the target system file data sets must be mounted on the driving system.

If you plan to install IBM Encryption Facility in a zFS file system, this requires that zFS be active on the driving system. Information on activating and using zFS can be found in z/OS Distributed File Service zSeries File System Administration, SC24-5989.

5.2 Target System Requirements

This section describes the environment of the target system required to install and use IBM Encryption Facility.

IBM Encryption Facility installs in the z/OS (Z038) SREL.

5.2.1 Machine Requirements

The target system can run in any hardware environment that supports the required software.

The IBM Encryption Facility for z/OS will run on the following IBM servers:

- System z9 EC or BC, or equivalent
- zSeries z900 or z990, or equivalent
- zSeries z800 or z890, or equivalent

The IBM z9 Server requires feature 3863, CP Assist for Cryptographic Functions (CPACF), to be installed to use Cryptographic Support. The z9 server also supports optional feature 0863, the CryptoExpress2 Cryptographic Coprocessor feature.

The IBM eServer zSeries z990 Server and IBM eServer zSeries z890 Server require feature 3863, CP Assist for Cryptographic Functions CPACF), to be installed to use Cryptographic Support. The z990 and z890 servers also support optional feature 0863, the PCI X Cryptographic Coprocessor (PCIXCC) and CryptoExpress2 Coprocessor CEX2C). The IBM PCI Cryptographic Accelerator (PCICA) is another optional feature (feature code 0862), but is not used by the Encryption Facility product.

IBM Encryption Facility for z/OS can run on the IBM eServer zSeries z900 Server and IBM eServer zSeries z800 Server. The z900 and z800 servers also support optional feature 0861, the PCI Cryptographic Coprocessor (PCICC). The IBM PCI Cryptographic Accelerator (PCICA) is another optional feature (feature code 0862), but is not used by the Encryption Facility product.

The Encryption Facility options have the following requirements:

- For the PASSWORD option, use one of the following requirements:
  - CPACF only
  - CCF
- For the Clear-TDES and Clear-AES128 (no ENCTDES), use one of the following requirements:
  - CPACF only, or CPACF with PCIXCC / CEX2C
  - CCF, or CCF with PCICC
- For 2048-bit keys, use one of the following requirements:
  - CEX2C with Licensed Internal Code (LIC) at or above the January 2005 level
  - PCIXCC with Licensed Internal Code (LIC) at or above the January 2005 level
  - PCICC with PCI Crypto 2048 bit Enablement Feature 0867
- For RSA keys generated through RACF using ICSF or directly through ICSF, use one of the following requirements:
  - CEX2C
  - PCIXCC

  - PCICC
- For 1024-bit ME keys generated through RACF BSAFE and imported into ICSF, a CCF is required.

Note: Performance for secure key (ENCTDES option) is much slower than clear key (CLEAR-TDES or CLEAR-AES128). This can be mitigated by overriding the ENCTDES option to use CLEAR-* options.

5.2.2 Programming Requirements

5.2.2.1 Installation Requisites: Installation requisites identify products that are required and *must* be present on the system or products that are not required but *should* be present on the system for the successful installation of this product.

Mandatory installation requisites identify products that are required on the system for the successful installation of this product. These products are specified as PREs or REQs.

Figure 7. Target System Mandatory Installation Requisites

Program Number	Product Name	Minimum VRM	Minimum Service Level will satisfy these APARs	Included in the shipped product?
Any **one** of the following:				
5694-A01	z/OS	V1.6.0	PTF for z/OS DFSMS APAR OA09868 and PTF for z/OS BCP APAR OA10229	No
5655-G52	z/OS.e	V1.6.0	PTF for z/OS DFSMS APAR OA09868 and PTF for z/OS BCP APAR OA10229	No
5694-A01	z/OS	V1.7.0	PTF for z/OS DFSMS APAR OA09868	No
5655-G52	z/OS.e	V1.7.0	PTF for z/OS.e DFSMS APAR OA09868	No
5694-A01	z/OS	V1.13.0	N/A	No
5650-ZOS	z/OS	V2.1.0 or higher	N/A	No

Note: Installation might require migration to new z/OS releases to be service supported. See http://www-03.ibm.com/systems/z/os/zos/support/zos_eos_dates.html.

Conditional installation requisites identify products that are *not* required for successful installation of this product but can resolve such things as certain warning messages at installation time. These products are specified as IF REQs.

IBM Encryption Facility has no conditional installation requisites.

5.2.2.2 Operational Requisites: Operational requisites are products that are required and *must* be present on the system or products that are not required but *should* be present on the system for this product to operate all or part of its functions.

Mandatory operational requisites identify products that are required for this product to operate its basic functions.

Figure 8. Target System Mandatory Operational Requisites

Program Number	Product Name and Minimum VRM/Service Level
5694-A01	Integrated Cryptographic Services Facility (ICSF) Web deliverable (FMID HCR7720) or later PTF for z/OS ICSF APAR OA19177
And any **one** of the following:	
5655-R31 (31 bit) or 5655-R32 (64 bit)	IBM SDK for z/OS, Java Technology Edition, Version 6
5655-R31 (31 bit) or 5655-R32 (64 bit)	IBM SDK for z/OS, Java Technology Edition, Version 6.0.1
5655-W43 (31 bit) or 5655-W44 (64 bit)	IBM SDK for z/OS, Java Technology Edition, Version 7
5655-W43 (31 bit) or 5655-W44 (64 bit)	IBM SDK for z/OS, Java Technology Edition, Version 7 Release 1
5655-DGG (31 bit) or 5655-DGH (64 bit)	IBM SDK for z/OS, Java Technology Edition, Version 8
Note: For detailed instructions for specifying full function Java cryptography on z/OS, see https://developer.ibm.com/javasdk/support/zos/ IBM Encryption Facility applications might require full function cryptography capability.	

Conditional operational requisites identify products that are *not* required for this product to operate its basic functions but are required at run time for this product to operate specific functions. These products are specified as IF REQs.

Figure 9. Target System Conditional Operational Requisites

Program Number	Product Name and Minimum VRM/Service Level	Function
5694-A01	z/OS V1.6.0 or higher, with Security Server - RACF APAR OA13030 and DFSMS - QSAM APAR OA13571	RACF and DFSMS
5655-G52	z/OS.e V1.6.0 or higher, with Security Server - RACF APAR OA13030 and DFSMS - QSAM APAR OA13571	RACF and DFSMS
5694-A01	z/OS V1.6.0 or higher, with DFSMSdss APAR OA13300	DFSMS
5655-G52	z/OS.e V1.6.0 or higher, with DFSMSdss APAR OA13300	DFSMS
5694-A01	z/OS V1.6.0 or higher, with DFSMShsm APARs OA13453 and OA13687	DFSMS
5655-G52	z/OS.e V1.6.0 or higher, with DFSMShsm APARs OA13453 and OA13687	DFSMS

Note:

1. RACF with PTF for APAR OA13030 has the following functions:
   - 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
2. z990 and z890 Enhancements to Cryptographic Support Web Deliverable (FMID HCR7720) is required for certain functions.
3. A Java-based Web-downloaded program, the IBM Encryption Facility for z/OS Client and the separately-licensed program can be used to decrypt the data encrypted by the Encryption Services feature running on z/OS.These programs can also be used to encrypt data to be decrypted by the Encryption Services feature running on z/OS. This can allow you to exchange encrypted data between z/OS systems and other operating systems.

DFSMSdss APAR OA13300 equates to the following PTFs that are required install time of HCF773D.

Figure 10. Install Logic for Encryption Facility DFSMSdss Encription

DFSMS Releases	Requisites
HDZ11G0	UA90212
HDZ11H0	UA90213
HDZ11J0	UA90214
HDZ11K0	UA90215

5.2.2.3 Toleration/Coexistence Requisites:

Toleration/coexistence requisites identify products that must be present on sharing systems. These systems can be other systems in a multisystem environment (not necessarily sysplex), a shared DASD environment (such as test and production), or systems that reuse the same DASD environment at different time intervals.

IBM Encryption Facility has no toleration/coexistence requisites.

5.2.2.4 Incompatibility (Negative) Requisites:

Negative requisites identify products that must *not* be installed on the same system as this product.

IBM Encryption Facility has no negative requisites.

5.2.3 DASD Storage Requirements

IBM Encryption Facility libraries can reside on all supported DASD types.

Figure 11 lists the total space that is required for each type of library.

Figure 11. Total DASD Space Required by IBM Encryption Facility

Library Type	Total Space Required in 3390 Trks
Target	10 tracks on 3390
Distribution	26 tracks on 3390
File System(s)	13 tracks on 3390

Notes:

1. For non-RECFM U data sets, IBM recommends using system-determined block sizes for efficient DASD utilization. For RECFM U data sets, IBM recommends using a block size of 32760, which is most efficient from the performance and DASD utilization perspective.
2. Abbreviations used for data set types are shown as follows.

   U Unique data set, allocated by this product and used by only this product. This table provides all the required information to determine the correct storage for this data set. You do not need to refer to other tables or program directories for the data set size.

   S Shared data set, allocated by this product and used by this product and other products. To determine the correct storage needed for this data set, add the storage size given in this table to those given in other tables (perhaps in other program directories). If the data set already exists, it must have enough free space to accommodate the storage size given in this table.

   E Existing shared data set, used by this product and other products. This data set is *not* allocated by this product. To determine the correct storage for this data set, add the storage size given in this table to those given in other tables (perhaps in other program directories). If

the data set already exists, it must have enough free space to accommodate the storage size given in this table.

If you currently have a previous release of this product installed in these libraries, the installation of this release will delete the old release and reclaim the space that was used by the old release and any service that had been installed. You can determine whether these libraries have enough space by deleting the old release with a dummy function, compressing the libraries, and comparing the space requirements with the free space in the libraries.

For more information about the names and sizes of the required data sets, see 6.1.6, “Allocate SMP/E Target and Distribution Libraries” on page 21.

3. Abbreviations used for the file system path type are as follows.

   N New path, created by this product.
   X Path created by this product, but might already exist from a previous release.
   P Previously existing path, created by another product.

4. All target and distribution libraries listed have the following attributes:

   - The default name of the data set can be changed.
   - The default block size of the data set can be changed.
   - The data set can be merged with another data set that has equivalent characteristics.
   - The data set can be either a PDS or a PDSE, with some exceptions. If the value in the "ORG" column specifies "PDS", the data set must be a PDS. If the value in "DIR Blks" column specifies "N/A", the data set must be a PDSE.

5. All target libraries listed have the following attributes:

   - These data sets can be SMS-managed, but they are not required to be SMS-managed.
   - These data sets are not required to reside on the IPL volume.
   - The values in the "Member Type" column are not necessarily the actual SMP/E element types that are identified in the SMPMCS.

6. All target libraries that are listed and contain load modules have the following attributes:

   - These data sets can not be in the LPA, with some exceptions. If the value in the "Member Type" column specifies "LPA", it is advised to place the data set in the LPA.
   - These data sets can be in the LNKLST.
   - These data sets are not required to be APF-authorized, with some exceptions. If the value in the "Member Type" column specifies "APF", the data set must be APF-authorized.

The following figures describe the target and distribution libraries and file system paths required to install IBM Encryption Facility. The storage requirements of IBM Encryption Facility must be added to the storage required by other programs that have data in the same library or path.

Note: Use the data in these tables to determine which libraries can be merged into common data sets. In addition, since some ALIAS names may not be unique, ensure that no naming conflicts will be introduced before merging libraries.

Figure 12. Storage Requirements for IBM Encryption Facility Target Libraries

Library DDNAME	Member Type	Target Volume	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
SAMPLIB	Sample	TVOL1	E	PDS	FB	80	5	2
LINKLIB	LMod	TVOL1	E	PDS	U	0	5	2

Figure 13. IBM Encryption Facility File System Paths

DDNAME	TYPE	Path Name
SCSDHFS	N	/usr/lpp/encryptionfacility/IBM/

Note:

1. Create the file-system directories /var/encryptionfacility and /etc/encryptionfacility.
2. You need to copy the ibmef.config file from /usr/lpp/encryptionfacility to /etc/encryptionfacility. This file should be edited in /etc/encryptionfacility.

Figure 14. Storage Requirements for IBM Encryption Facility Distribution Libraries

Library DDNAME	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
ASAMPLIB	E	PDS	FB	80	5	2
ACSDHFS	U	PDS	VB	255	13	2
ACSDMOD0	U	PDS	U	0	5	2
ALINKLIB	E	PDS	U	0	3	2

5.3 FMIDs Deleted

Installing IBM Encryption Facility might result in the deletion of other FMIDs. To see which FMIDs will be deleted, examine the ++VER statement in the SMPMCS of the product.

If you do not want to delete these FMIDs at this time, install IBM Encryption Facility into separate SMP/E target and distribution zones.

Note: These FMIDs are not automatically deleted from the Global Zone. If you want to delete these FMIDs from the Global Zone, use the SMP/E REJECT NOFMID DELETEFMID command. See the SMP/E Commands book for details.

5.4 Special Considerations

IBM Encryption Facility has no special considerations for the target system.

6.0 Installation Instructions

This chapter describes the installation method and the step-by-step procedures to install and to activate the functions of IBM Encryption Facility.

Please note the following points:

- If you want to install IBM Encryption Facility into its own SMP/E environment, consult the SMP/E manuals for instructions on creating and initializing the SMPCSI and the SMP/E control data sets.
- You can use the sample jobs that are provided to perform part or all of the installation tasks. The SMP/E jobs assume that all DDDEF entries that are required for SMP/E execution have been defined in appropriate zones.
- You can use the SMP/E dialogs instead of the sample jobs to accomplish the SMP/E installation steps.

6.1 Installing IBM Encryption Facility

6.1.1 SMP/E Considerations for Installing IBM Encryption Facility

Use the SMP/E RECEIVE, APPLY, and ACCEPT commands to install this release of IBM Encryption Facility.

6.1.2 SMP/E Options Subentry Values

The recommended values for certain SMP/E CSI subentries are shown in Figure 15. Using values lower than the recommended values can result in failures in the installation. DSSPACE is a subentry in the GLOBAL options entry. PEMAX is a subentry of the GENERAL entry in the GLOBAL options entry. See the SMP/E manuals for instructions on updating the global zone.

Figure 15. SMP/E Options Subentry Values

Subentry	Value	Comment
DSSPACE	Existing target CSI value	IBM suggests using your existing target system CSIs DSSPACE value.
PEMAX	SMP/E Default	IBM recommends using the SMP/E default for PEMAX.

© Copyright IBM Corp. 2005, 2019

6.1.3 SMP/E CALLLIBS Processing

IBM Encryption Facility uses the CALLLIBS function provided in SMP/E to resolve external references during installation. When IBM Encryption Facility is installed, ensure that DDDEFs exist for the following libraries:

- SCSFMOD0

Note: CALLLIBS uses the previous DDDEFs only to resolve the link-edit for IBM Encryption Facility. These data sets are not updated during the installation of IBM Encryption Facility.

6.1.4 Sample Jobs

The following sample installation jobs are provided as part of the product to help you install IBM Encryption Facility:

Figure 16. Sample Installation Jobs

Job Name	Job Type	Description	RELFILE
CSDALLOC	ALLOCATE	Sample job to allocate target and distribution libraries	IBM.HCF7740.F2
CSDISMKD	MKDIR	Sample job to invoke the supplied CSDMKDIR EXEC to allocate file system paths	IBM.HCF7740.F2
CSDMKDIR	SAMPLE	Create file-system directories	IBM.HCF7740.F2
CSDDDDEF	DDDEF	Sample job to define SMP/E DDDEFs	IBM.HCF7740.F2

You can access the sample installation jobs by performing an SMP/E RECEIVE (refer to 6.1.5, “Perform SMP/E RECEIVE” on page 21) then copy the jobs from the RELFILES to a work data set for editing and submission. See Figure 16 to find the appropriate relfile data set.

You can also copy the sample installation jobs from the product files by submitting the following job. Before you submit the job, add a job card and change the lowercase parameters to uppercase values to meet the requirements of your site.

```
//STEP1    EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//IN       DD DSN=IBM.fmid.Fy,UNIT=SYSALLDA,DISP=SHR,
//         VOL=SER=filevol
//OUT      DD DSNAME=jcl-library-name,
//         DISP=(NEW,CATLG,DELETE),
//         VOL=SER=dasdvol,UNIT=SYSALLDA,
//         SPACE=(TRK,(primary,secondary,dir))
//SYSUT3   DD UNIT=SYSALLDA,SPACE=(CYL,(1,1))
//SYSIN    DD *
    COPY INDD=IN,OUTDD=OUT
/*
```

See the following information to update the statements in the previous sample:

IN:

filevol is the volume serial of the DASD device where the downloaded files reside.

OUT:

jcl-library-name is the name of the output data set where the sample jobs are stored.
dasdvol is the volume serial of the DASD device where the output data set resides.

6.1.5 Perform SMP/E RECEIVE

If you have obtained IBM Encryption Facility as part of a CBPDO, use the RCVPDO job in the CBPDO RIMLIB data set to receive the IBM Encryption Facility FMIDs, service, and HOLDDATA that are included on the CBPDO package. For more information, see the documentation that is included in the CBPDO. You will receive a return code of 0 if this job runs correctly.

6.1.6 Allocate SMP/E Target and Distribution Libraries

Edit and submit sample job CSDALLOC to allocate the SMP/E target and distribution libraries for IBM Encryption Facility. Consult the instructions in the sample job for more information.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly. You will receive a return code of 0 if this job runs correctly.

6.1.7 Allocate File System Paths

The target system HFS or zFS data set must be mounted on the driving system when running the sample CSDISMKD job since the job will create paths in the HFS or zFS.

Before running the sample job to create the paths in the file system, you must ensure that OMVS is active on the driving system and that the target system's HFS or zFS file system is mounted to the driving system. zFS must be active on the driving system if you are installing IBM Encryption Facility into a file system that is zFS.

If you plan to install IBM Encryption Facility into a new HFS or zFS file system, you must create the mountpoint and mount the new file system to the driving system for IBM Encryption Facility.

The recommended mountpoint is */usr/lpp/encryptionfacility*.

Edit and submit sample job CSDISMKD to allocate the HFS or zFS paths for IBM Encryption Facility. Consult the instructions in the sample job for more information.

If you create a new file system for this product, consider updating the BPXPRMxx PARMLIB member to mount the new file system at IPL time. This action can be helpful if an IPL occurs before the installation is completed.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

6.1.8 Create DDDEF Entries

Edit and submit sample job CSDDDDEF to create DDDEF entries for the SMP/E target and distribution libraries for IBM Encryption Facility. Consult the instructions in the sample job for more information.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

6.1.9 Perform SMP/E APPLY

1. Perform an SMP/E APPLY CHECK for IBM Encryption Facility.

   The latest HOLDDATA is available through several different portals, including http://service.software.ibm.com/holdata/390holddata.html. The latest HOLDDATA may identify HIPER and FIXCAT APARs for the FMIDs you will be installing. An APPLY CHECK will help you determine if any HIPER or FIXCAT APARs are applicable to the FMIDs you are installing. If there are any applicable HIPER or FIXCAT APARs, the APPLY CHECK will also identify fixing PTFs that will resolve the APARs, if a fixing PTF is available.

   You should install the FMIDs regardless of the status of unresolved HIPER or FIXCAT APARs. However, do not deploy the software until the unresolved HIPER and FIXCAT APARs have been analyzed to determine their applicability. That is, before deploying the software either ensure fixing PTFs are applied to resolve all HIPER or FIXCAT APARs, or ensure the problems reported by all HIPER or FIXCAT APARs are not applicable to your environment.

   To receive the full benefit of the SMP/E Causer SYSMOD Summary Report, do *not* bypass the PRE, ID, REQ, and IFREQ on the APPLY CHECK. The SMP/E root cause analysis identifies the cause only of *errors* and not of *warnings* (SMP/E treats bypassed PRE, ID, REQ, and IFREQ conditions as warnings, instead of errors).

   Here are sample APPLY commands:

   a. To ensure that all recommended and critical service is installed with the FMIDs, receive the latest HOLDDATA and use the APPLY CHECK command as follows

      ```
      APPLY S(fmid,fmid,...) CHECK
      FORFMID(fmid,fmid,...)
      SOURCEID(RSU*)
      FIXCAT(IBM.ProductInstall-RequiredService)
      GROUPEXTEND .
      ```

      Some HIPER APARs might not have fixing PTFs available yet. You should analyze the symptom flags for the unresolved HIPER APARs to determine if the reported problem is applicable to your environment and if you should bypass the specific ERROR HOLDs in order to continue the installation of the FMIDs.

      This method requires more initial research, but can provide resolution for all HIPERs that have fixing PTFs available and are not in a PE chain. Unresolved PEs or HIPERs might still exist and require the use of BYPASS.

   b. To install the FMIDs without regard for unresolved HIPER APARs, you can add the BYPASS(HOLDCLASS(HIPER)) operand to the APPLY CHECK command. This will allow you to

install FMIDs even though one or more unresolved HIPER APARs exist. After the FMIDs are installed, use the SMP/E REPORT ERRSYSMODS command to identify unresolved HIPER APARs and any fixing PTFs.

```
APPLY S(fmid,fmid,...) CHECK
FORFMID(fmid,fmid,...)
SOURCEID(RSU*)
FIXCAT(IBM.ProductInstall-RequiredService)
GROUPEXTEND
BYPASS(HOLDCLASS(HIPER)) .
 ..any other parameters documented in the program directory
```

This method is quicker, but requires subsequent review of the Exception SYSMOD report produced by the REPORT ERRSYSMODS command to investigate any unresolved HIPERs. If you have received the latest HOLDDATA, you can also choose to use the REPORT MISSINGFIX command and specify Fix Category IBM.PRODUCTINSTALL-REQUIREDSERVICE to investigate missing recommended service.

If you bypass HOLDs during the installation of the FMIDs because fixing PTFs are not yet available, you can be notified when the fixing PTFs are available by using the APAR Status Tracking (AST) function of ServiceLink or the APAR Tracking function of ResourceLink.

2. After you take actions that are indicated by the APPLY CHECK, remove the CHECK operand and run the job again to perform the APPLY.

   Note: The GROUPEXTEND operand indicates that SMP/E applies all requisite SYSMODs. The requisite SYSMODS might be applicable to other functions.

   Expected Return Codes and Messages from APPLY CHECK: You will receive a return code of 0 if this job runs correctly.

   Expected Return Codes and Messages from APPLY: You will receive a return code of 0 if this job runs correctly.

6.1.10 Perform SMP/E ACCEPT

Perform an SMP/E ACCEPT CHECK for IBM Encryption Facility.

To receive the full benefit of the SMP/E Causer SYSMOD Summary Report, do *not* bypass the PRE, ID, REQ, and IFREQ on the ACCEPT CHECK. The SMP/E root cause analysis identifies the cause of *errors* but not *warnings* (SMP/E treats bypassed PRE, ID, REQ, and IFREQ conditions as warnings rather than errors).

Before you use SMP/E to load new distribution libraries, it is recommended that you set the ACCJCLIN indicator in the distribution zone. In this way, you can save the entries that are produced from JCLIN in the distribution zone whenever a SYSMOD that contains inline JCLIN is accepted. For more information about the ACCJCLIN indicator, see the description of inline JCLIN in the SMP/E Commands book for details.

After you take actions that are indicated by the ACCEPT CHECK, remove the CHECK operand and run the job again to perform the ACCEPT.

Note: The GROUPEXTEND operand indicates that SMP/E accepts all requisite SYSMODs. The requisite SYSMODS might be applicable to other functions.

Expected Return Codes and Messages from ACCEPT CHECK: You will receive a return code of 0 if this job runs correctly.

If PTFs that contain replacement modules are accepted, SMP/E ACCEPT processing will link-edit or bind the modules into the distribution libraries. During this processing, the Linkage Editor or Binder might issue messages that indicate unresolved external references, which will result in a return code of 4 during the ACCEPT phase. You can ignore these messages, because the distribution libraries are not executable and the unresolved external references do not affect the executable system libraries.

Expected Return Codes and Messages from ACCEPT: You will receive a return code of 0 if this job runs correctly.

6.1.11 Run REPORT CROSSZONE

The SMP/E REPORT CROSSZONE command identifies requisites for products that are installed in separate zones. This command also creates APPLY and ACCEPT commands in the SMPPUNCH data set. You can use the APPLY and ACCEPT commands to install those cross-zone requisites that the SMP/E REPORT CROSSZONE command identifies.

After you install IBM Encryption Facility, it is recommended that you run REPORT CROSSZONE against the new or updated target and distribution zones. REPORT CROSSZONE requires a global zone with ZONEINDEX entries that describe all the target and distribution libraries to be reported on.

For more information about REPORT CROSSZONE, see the SMP/E manuals.

6.1.12 Cleaning Up Obsolete Data Sets, Paths, and DDDEFs

6.2 Installing IBM Encryption Facility - DFSMSdss Encryption Feature

Ensure that the appropriate DFSMS required PTFs are installed or available for concurrent installation with HCF773D See Figure 10 on page 14 for more information.

The DFSMSdss Encryption Feature must be installed in the same zone as the BCP Base. and the following statement entry added in the IFAPRDxx PARMLIB member:

6.3 Activating IBM Encryption Facility

6.4 Product Customization

The publication *Encryption Facility for z/OS Planning and Customizing* (SA23-2229) contains the necessary information to customize and use IBM Encryption Facility.

7.0 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.

APAR numbers are provided in this document to assist in locating PTFs that may be required. Ongoing problem reporting may result in additional APARs being created. Therefore, the APAR lists in this document may not be complete. To obtain current service recommendations and to identify current product service requirements, always contact the IBM Customer Support Center or use S/390 SoftwareXcel to obtain the current "PSP Bucket".

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, New York 10504-1785
USA

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

7.1 Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

© Copyright IBM Corp. 2005, 2019

Reader's Comments

Program Directory for IBM Encryption Facility for z/OS, January 2019 We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have. Send your comments by emailing us at ibmkc@us.ibm.com, and include the following information: Your name and address Your email address Your telephone or fax number The publication title and order number The topic and page number related to your comment The text of your comment When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you submit. Thank you for your participation.

© Copyright IBM Corp. 2005, 2019

Communicating Your Comments to IBM

Program Directory for
IBM Encryption Facility for z/OS V1.2.0
z/OS V1.6 or z/OS.e V1.6 and higher

Service Updated 11 January 2019

Publication No. GI10-0771-03

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a reader's comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:
  - FAX: (International Access Code)+1+845+432-9405
- If you prefer to send comments electronically, use the following e-mail address:
  - mhvrcfs@us.ibm.com

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies

Optionally, if you include your telephone number, we will be able to respond to your comments by phone.

Reader's Comments — We'd Like to Hear from You

Program Directory for
IBM Encryption Facility for z/OS V1.2.0
z/OS V1.6 or z/OS.e V1.6 and higher

Service Updated 11 January 2019

Publication No. GI10-0771-03

You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you. Your comments will be sent to the author's department for whatever review and action, if any, are deemed appropriate.

Note: Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.

Today's date: _____

What is your occupation?

Newsletter number of latest Technical Newsletter (if any) concerning this publication:

How did you use this publication?

[ ]	As an introduction	[ ]	As a text (student)
[ ]	As a reference manual	[ ]	As a text (instructor)
[ ]	For another purpose (explain)		

Is there anything you especially like or dislike about the organization, presentation, or writing in this manual? Helpful comments include general usefulness of the book; possible additions, deletions, and clarifications; specific errors and omissions.

Page Number: Comment:

Name	Address
Company or Organization	
Phone No.	

Reader's Comments — We'd Like to Hear from You
GI10-0771-03

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
MHVRCFS, Mail Station P181
2455 South Road
Poughkeepsie, NY 12601-5400

Fold and Tape **Please do not staple** Fold and Tape

GI10-0771-03

Cut or Fold
Along Line

GI10-0771-03