Program Directory for

IBM Security Key Lifecycle Manager

for z/OS

V1.1.0

Program Number 5698-B35

FMID HCKL110

for Use with
z/OS

Document Date: May, 2011

GI11-4300-02

Note

Before using this information and the product it supports, be sure to read the general information under 7.0, “Notices” on page 21.

Contents

1.0 Introduction . . . 1
1.1 IBM Security Key Lifecycle Manager for z/OS Description . . . 1
1.2 IBM Security Key Lifecycle Manager for z/OS FMIDs . . . 2

2.0 Program Materials . . . 3
2.1 Basic Machine-Readable Material . . . 3
2.2 Program Publications . . . 3
2.2.1 Basic Program Publications . . . 3
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 . . . 8
5.1 Driving System Requirements . . . 8
5.1.1 Machine Requirements . . . 8
5.1.2 Programming Requirements . . . 8
5.2 Target System Requirements . . . 9
5.2.1 Machine Requirements . . . 9
5.2.2 Programming Requirements . . . 9
5.2.2.1 Installation Requisites . . . 9
5.2.2.2 Operational Requisites . . . 10
5.2.2.3 Toleration/Coexistence Requisites . . . 10
5.2.2.4 Incompatibility (Negative) Requisites . . . 10
5.2.3 DASD Storage Requirements . . . 11
5.3 FMIDs Deleted . . . 13
5.4 Special Considerations . . . 13

6.0 Installation Instructions . . . 14
6.1 Installing IBM Security Key Lifecycle Manager for z/OS . . . 14
6.1.1 SMP/E Considerations for Installing IBM Security Key Lifecycle Manager for z/OS . . . 14
6.1.2 SMP/E Options Subentry Values . . . 14
6.1.3 Sample Jobs . . . 15
6.1.4 Perform SMP/E RECEIVE . . . 16
6.1.5 Allocate SMP/E Target and Distribution Libraries . . . 16

6.1.6 Allocate File system Paths 16
6.1.7 Create DDDEF Entries 17
6.1.8 Perform SMP/E APPLY 17
6.1.9 Perform SMP/E ACCEPT 19
6.1.10 Cleaning Up Obsolete Data Sets, Paths, and DDDEFs 19
6.2 Activating IBM Security Key Lifecycle Manager for z/OS 20

7.0 Notices 21
7.1 Trademarks 22

Contacting Customer Support 23

Figures

1. Basic Material: Unlicensed Publications 3
2. Publications Useful During Installation 4
3. PSP Upgrade and Subset ID 5
4. Component IDs 6
5. Driving System Software Requirements 9
6. Target System Mandatory Operational Requisites 10
7. Target System Conditional Operational Requisites 10
8. Total DASD Space Required by IBM Security Key Lifecycle Manager for z/OS 11
9. Storage Requirements for IBM Security Key Lifecycle Manager for z/OS Target Libraries 12
10. IBM Security Key Lifecycle Manager for z/OS File System Paths 12
11. Storage Requirements for IBM Security Key Lifecycle Manager for z/OS Distribution Libraries . . 13
12. SMP/E Options Subentry Values 14
13. Sample Installation Jobs 15

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 Security Key Lifecycle Manager for z/OS. This publication refers to IBM Security Key Lifecycle Manager for z/OS as IBM Security Key Lifecycle Manager for z/OS.

The Program Directory contains the following sections:

- 2.0, “Program Materials” on page 3 identifies the basic and optional program materials and documentation for IBM Security Key Lifecycle Manager for z/OS.
- 3.0, “Program Support” on page 5 describes the IBM support available for IBM Security Key Lifecycle Manager for z/OS.
- 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 Security Key Lifecycle Manager for z/OS.
- 5.0, “Installation Requirements and Considerations” on page 8 identifies the resources and considerations that are required for installing and using IBM Security Key Lifecycle Manager for z/OS.
- 6.0, “Installation Instructions” on page 14 provides detailed installation instructions for IBM Security Key Lifecycle Manager for z/OS. It also describes the procedures for activating the functions of IBM Security Key Lifecycle Manager for z/OS, or refers to appropriate publications.

Before installing IBM Security Key Lifecycle Manager for z/OS, 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 ; then keep them for future 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 Security Key Lifecycle Manager for z/OS is supplied in a Custom-Built Product Delivery Offering (CBPDO, 5751-CS3). The Program Directory that is provided in softcopy format on the CBPDO tape is identical to the hardcopy format that is provided with your order. All service and HOLDDATA for IBM Security Key Lifecycle Manager for z/OS are included on the CBPDO tape.

Do not use this program directory if you install IBM Security Key Lifecycle Manager for z/OS with a SystemPac or ServerPac. When you use these offerings, use the jobs and documentation supplied with the offering. This program directory can point you to specific sections of it as required.

1.1 IBM Security Key Lifecycle Manager for z/OS Description

IBM Security Key Lifecycle Manager for z/OS works with IBM encryption-enabled tape drives and system storage devices. The product helps in generating, protecting, storing, and maintaining encryption keys that are used to encrypt information being written to and decrypt information being read from devices. IBM Security Key Lifecycle Manager for z/OS provides a command line interface for you to manage serving of keys to these devices.

1.2 IBM Security Key Lifecycle Manager for z/OS FMIDs

IBM Security Key Lifecycle Manager for z/OS consists of the following FMIDs:

HCKL110

2.0 Program Materials

An IBM program is identified by a program number. The program number for IBM Security Key Lifecycle Manager for z/OS is 5698-B35.

Basic Machine-Readable Materials are materials that are supplied under the base license and feature numbers, and are required for the use of the product. Optional Machine-Readable Materials are orderable under separate feature numbers, and are not required for the product to function.

The program announcement material describes the features supported by IBM Security Key Lifecycle Manager for z/OS. 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 magnetic tape 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 14 for more information about how to install the program.

You can find information about the physical tape for the basic machine-readable materials for IBM Security Key Lifecycle Manager for z/OS in the *CBPDO Memo To Users Extension*.

2.2 Program Publications

The following sections identify the basic and optional publications for IBM Security Key Lifecycle Manager for z/OS.

2.2.1 Basic Program Publications

Figure 1 identifies the basic unlicensed program publications for IBM Security Key Lifecycle Manager for z/OS. One copy of each of these publications is included when you order the basic materials for IBM Security Key Lifecycle Manager for z/OS. You can print additional copies when electronic publications are available using the softcopy url provided in the Product Announcement letter or from: http://www.ibm.com/shop/publications/order

Figure 1. Basic Material: Unlicensed Publications

Publication Title	Form Number
IBM Security Key Lifecycle Manager for z/OS Version 1.1, Planning and User's Guide	SC14-7628

The IBM Security Key Lifecycle Manager for z/OS product manuals and all other Tivoli product manuals can be found at the Tivoli Information Center url listed below:
http://publib.boulder.ibm.com/tividd/td/tdprodlist.html

2.3 Program Source Materials

No program source materials or viewable program listings are provided for IBM Security Key Lifecycle Manager for z/OS.

2.4 Publications Useful During Installation

You might want to use the publications listed in Figure 2 during the installation of IBM Security Key Lifecycle Manager for z/OS. To order copies, contact your IBM representative or visit the IBM Publications Center at
http://www.ibm.com/shop/publications/order.

Figure 2. Publications Useful During Installation

Publication Title	**Form Number**
IBM SMP/E for z/OS User's Guide	SA22-7773
IBM SMP/E for z/OS Commands	SA22-7771
IBM SMP/E for z/OS Reference	SA22-7772
IBM SMP/E for z/OS Messages, Codes, and Diagnosis	GA22-7770

3.0 Program Support

This section describes the IBM support available for IBM Security Key Lifecycle Manager for z/OS.

3.1 Program Services

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

3.2 Preventive Service Planning

Before you install IBM Security Key Lifecycle Manager for z/OS, make sure that you have reviewed the current Preventive Service Planning (PSP) information. The PSP Buckets maintain current lists (which have been identified since the package was created) of any recommended or required service for the installation of this package. This service includes software PSP information that contains HIPER and required PTFs against the base release.

Although SW, HW, and functional PSP Buckets might have overlap, review all that apply to this package to ensure that you identify all the known service that is required for your installation of this package.

If you obtained IBM Security Key Lifecycle Manager for z/OS as part of a CBPDO, HOLDDATA is included.

If the CBPDO for IBM Security Key Lifecycle Manager for z/OS is older than two weeks old by the time you install the product materials, you should contact the IBM Support Center or use S/390 SoftwareXcel to obtain the latest PSP Bucket information. You can also obtain the latest PSP Bucket information by going to the following Web site:
http://www14.software.ibm.com/webapp/set2/psearch/search?domain=psp

For program support, access the Software Support Web site at http://www.ibm.com/software/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 Security Key Lifecycle Manager for z/OS are shown as follows:

Figure 3. PSP Upgrade and Subset ID

UPGRADE	SUBSET	Description
ITKLM4ZOS	HCKL110	ISKLM BASE

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 4 on page 6 identifies the component IDs (COMPID) for IBM Security Key Lifecycle Manager for z/OS.

Figure 4. Component IDs

FMID	COMPID	Component Name	RETAIN Release
HCKL110	5698B3500	ISKLM BASE	110

4.0 Program and Service Level Information

This section identifies the program and relevant service levels of IBM Security Key Lifecycle Manager for z/OS. 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.

4.1 Program Level Information

No APARs have been incorporated into IBM Security Key Lifecycle Manager for z/OS.

4.2 Service Level Information

No PTFs against this release of IBM Security Key Lifecycle Manager for z/OS have been incorporated into the product tape.

It is highly recommended that you frequently check the IBM Security Key Lifecycle Manager for z/OS PSP Bucket for HIPER and SPECIAL Attention PTFs against all FMIDs that you must install.

5.0 Installation Requirements and Considerations

The following sections identify the system requirements for installing and activating IBM Security Key Lifecycle Manager for z/OS. The following terminology is used:

- *Driving system*: the system used to install the program; where SMP/E executes.

  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

5.1 Driving System Requirements

This section describes the environment of the driving system that is required to install IBM Security Key Lifecycle Manager for z/OS.

5.1.1 Machine Requirements

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

5.1.2 Programming Requirements

Figure 5. Driving System Software Requirements

Program Number	Product Name	Minimum VRM	Minimum Service Level will satisfy these APARs	Included in this product's shipment?
Any **one** of the following:				
5694-A01	z/OS	V1.11.0 or later	N/A	No
5655-G44	IBM SMP/E for z/OS	V03.04.00 or later	N/A	No

Note: Installation may 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.

5.2 Target System Requirements

This section describes the environment of the target system that is required to install and use IBM Security Key Lifecycle Manager for z/OS.

IBM Security Key Lifecycle Manager for z/OS 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.

5.2.2 Programming Requirements

5.2.2.1 Installation Requisites

Installation requisites identify products that are required by and *must* be present on the system or products that are not required by 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.

IBM Security Key Lifecycle Manager for z/OS has no mandatory installation requisites.

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 Security Key Lifecycle Manager for z/OS has no conditional installation requisites.

5.2.2.2 Operational Requisites

Operational requisites are products that are required by and *must* be present on the system or products that are not required by 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. These products are specified as PREs or REQs.

Figure 6. Target System Mandatory Operational Requisites

Program Number	**Product Name and Minimum VRM/Service Level**
5655-N98	IBM 31-bit SDK for z/OS, Java 2 Technology Edition, V5 or later

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 7. Target System Conditional Operational Requisites

Program Number	**Product Name and Minimum VRM/Service Level**	**Function**
5694-A01	z/OS V1R11 or later	RACF SMF data unload support for ISKLM for z/OS
Any **one** of the following:		
5694-A01	Cryptographic Support for z/OS V1R7-R9 & z/OS.e V1R7-R8	AES Key Generation for JAG Drives and DS8000 Disk only
5694-A01	Cryptographic Support for z/OS V1R8-R10 & z/OS.e V1R8	AES Key Generation for JAG Drives, DS8000 Disk, and LTO Drives

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 Security Key Lifecycle Manager for z/OS 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 Security Key Lifecycle Manager for z/OS has no negative requisites.

5.2.3 DASD Storage Requirements

IBM Security Key Lifecycle Manager for z/OS libraries can reside on all supported DASD types.

Figure 8 on page 11 lists the total space that is required for each type of library.

Figure 8. Total DASD Space Required by IBM Security Key Lifecycle Manager for z/OS

Library Type	Total Space Required in 3390 Trks
Target	4
Distribution	17
HFS or zFS	13

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 6.1.5, “Allocate SMP/E Target and Distribution Libraries” on page 16.
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 may 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 may be changed.
   - The default block size of the data set may be changed.
   - The data set may be merged with another data set that has equivalent characteristics.
   - The data set may be either a PDS or 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 be in the LPA, but they are not required to be in the LPA.
   - These data sets can be in the LNKLST.
   - These data sets are not required to be APF-authorized.

The following figures describe the target and distribution libraries and file system paths required to install IBM Security Key Lifecycle Manager for z/OS. The storage requirements of IBM Security Key Lifecycle Manager for z/OS must be added to the storage required by other programs having data in the same library or path.

Note: The data in these tables should be used when determining 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 9. Storage Requirements for IBM Security Key Lifecycle Manager for z/OS Target Libraries

Library DDNAME	Member Type	Target Volume	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
SCKLSAMP	Sample	Any	U	PO	FB	80	4	2

Figure 10. IBM Security Key Lifecycle Manager for z/OS File System Paths

DDNAME	TYPE	Path Name
SCKLHFS	U	/usr/lpp/ISKLM/IBM/

Figure 11. Storage Requirements for IBM Security Key Lifecycle Manager for z/OS Distribution Libraries

Library DDNAME	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
ACKLHFS	U	PO	VB	8796	13	2
ACKLSAMP	U	PO	FB	80	4	2

5.3 FMIDs Deleted

Installing IBM Security Key Lifecycle Manager for z/OS 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 Security Key Lifecycle Manager for z/OS 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, see the SMP/E manuals for instructions.

5.4 Special Considerations

IBM Security Key Lifecycle Manager for z/OS 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 Security Key Lifecycle Manager for z/OS.

Please note the following:

- If you want to install IBM Security Key Lifecycle Manager for z/OS 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. Additionally, to assist you in doing this, IBM has provided samples to help you create an SMP/E environment at the following url:
http://www.ibm.com/support/docview.wss?uid=swg21066230
- 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 Security Key Lifecycle Manager for z/OS

6.1.1 SMP/E Considerations for Installing IBM Security Key Lifecycle Manager for z/OS

Use the SMP/E RECEIVE, APPLY, and ACCEPT commands to install this release of IBM Security Key Lifecycle Manager for z/OS.

6.1.2 SMP/E Options Subentry Values

The recommended values for certain SMP/E CSI subentries are shown in Figure 12. 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 12. SMP/E Options Subentry Values

Subentry	Value	Comment
DSSPACE	200,10,20	Space allocation for the SMPTLIB data sets
PEMAX	SMP/E Default	IBM recommends using the SMP/E default for PEMAX.

6.1.3 Sample Jobs

The following sample installation jobs are provided as part of the product to help you install IBM Security Key Lifecycle Manager for z/OS:

Figure 13. Sample Installation Jobs

Job Name	Job Type	Description	RELFILE
CKLISREC	RECEIVE	Sample RECEIVE job	IBM.HCKL110.F1
CKLISALC	ALLOCATE	Sample job to allocate target and distribution libraries	IBM.HCKL110.F1
CKLISMKD	MKDIR	Sample job to invoke the supplied CKLMKDIR EXEC to allocate HFS or zFS paths	IBM.HCKL110.F1
CKLMKDIR	MKDIR	EXEC to allocate HFS or zFS paths	IBM.HCKL110.F1
CKLISDDD	DDDEF	Sample job to define SMP/E DDDEFs	IBM.HCKL110.F1
CKLISAPP	APPLY	Sample APPLY job	IBM.HCKL110.F1
CKLISACC	ACCEPT	Sample ACCEPT job	IBM.HCKL110.F1

You can access the sample installation jobs by performing an SMP/E RECEIVE and then copying the jobs from the relfiles to a work data set for editing and submission. See Figure 13 to find the appropriate relfile data set.

You can also copy the sample installation jobs from the tape or product files by submitting the following job. Depending on your distribution medium, Use either the //TAPEIN or the //FILEIN DD statement and comment out or delete the other statement. 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=*
//TAPEIN   DD DSN=IBM.HCKL110.F1,UNIT=tunit,
//         VOL=SER=volser,LABEL=(x,SL),
//         DISP=(OLD,KEEP)
//FILEIN   DD DSN=IBM.HCKL110.F1,UNIT=SYSALLDA,DISP=SHR,
//         VOL=SER=filevol
//OUT      DD DSNAME=jcl-library-name,
//         DISP=(NEW,CATLG,DELETE),
//         VOL=SER=dasdvol,UNIT=SYSALLDA,
//         SPACE=(TRK,(4,1,3))
//SYSUT3   DD UNIT=SYSALLDA,SPACE=(CYL,(1,1))
//SYSIN    DD *
   COPY INDD=xxxxIN,OUTDD=OUT
/*
```

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

TAPEIN:

tunit is the unit value that matches the product tape.
volser is the volume serial that matches the product tape.
x is the tape file number that indicates the location of the data set name on the tape.
See the documentation that is provided by CBPDO for the location of IBM.fmid.Fy on the tape.

FILEIN:

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.

SYSIN

xxxxIN is either TAPEIN or FILEIN depending on your input DD statement.

6.1.4 Perform SMP/E RECEIVE

If you have obtained IBM Security Key Lifecycle Manager for z/OS as part of a CBPDO, use the RCVPDO job in the CBPDO RIMLIB data set to receive the IBM Security Key Lifecycle Manager for z/OS FMIDs, service, and HOLDDATA that are included on the CBPDO tape. For more information, see the documentation that is included in the CBPDO.

You can also choose to edit and submit sample job CKLISREC to perform the SMP/E RECEIVE for IBM Security Key Lifecycle Manager for z/OS. 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.

6.1.5 Allocate SMP/E Target and Distribution Libraries

Edit and submit sample job CKLISALC to allocate the SMP/E target and distribution libraries for IBM Security Key Lifecycle Manager for z/OS. 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.

6.1.6 Allocate File system Paths

Mount the file system data set of the target system on the driving system when you run the sample CKLISMKD job because the job will create paths in the file system.

Before you run the sample job to create the paths in the file system, ensure that OMVS is active on the driving system, and that the file system of the target system is mounted to the driving system. If you install IBM Security Key Lifecycle Manager for z/OS into a zFS file system, zFS must be active on the driving system.

If you plan to install IBM Security Key Lifecycle Manager for z/OS into a new file system, create the mountpoint and mount the new file system to the driving system. For IBM Security Key Lifecycle Manager for z/OS, the recommended mountpoint is /usr/lpp/ISKLM. 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.

6.1.7 Create DDDEF Entries

Edit and submit sample job CKLISDDD to create DDDEF entries for the SMP/E target and distribution libraries for IBM Security Key Lifecycle Manager for z/OS. 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.

6.1.8 Perform SMP/E APPLY

1. Ensure that you have the latest HOLDDATA; then edit and submit sample job CKLISAPP to perform an SMP/E APPLY CHECK for IBM Security Key Lifecycle Manager for z/OS. Consult the instructions in the sample job for more information.

   HOLDDATA introduces ERROR HOLDs against FMIDs for HIPER APARs. Before the installation, ensure that you have the latest HOLDDATA, which is available through several different portals, including http://service.software.ibm.com/holdata/390holddata.html. Install the FMIDs regardless of the status of unresolved HIPERs. However, don't deploy the software until the unresolved HIPERs are analyzed to determine applicability.

   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. This is because 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 two methods to install FMIDs when ++HOLDs for HIPERs exist for the FMIDs that you install:

   a. To ensure that all recommended and critical service is installed with the FMIDs, if you are using SMP/E 3.5 or higher and have received the latest HOLDDATA, add the FIXCAT operand to the APPLY command as shown below. If you are using a prior release of SMP/E, add the SOURCEID(HIPER,RSU*) operand to the APPLY command.

```
If using SMP/E V3.5 or higher:
APPLY S(fmid,fmid,...)
FORFMID(fmid,fmid,...)
SOURCEID(RSU*)
FIXCAT(IBM.ProductInstall-RequiredService)
GROUPEXTEND .
If using SMP/E V3.4 or prior:
APPLY S(fmid,fmid,...)
FORFMID(fmid,fmid,...)
SOURCEID(HIPER,RSU*)
GROUPEXTEND .
```

Some HIPER APARs might not have PTFs available yet. You have to analyze the symptom flags to determine if you want to bypass the specific ERROR HOLDs and continue the installation of the FMIDs.

This method requires more initial research, but can provide resolution for all HIPERs that have fixes 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 the HIPERs, you can add a BYPASS(HOLDCLASS(HIPER)) operand to the APPLY command. In this way, you can install FMIDs even though HIPER ERROR HOLDs against them still exist. Only the HIPER ERROR HOLDs are bypassed. After the FMIDs are installed, run the SMP/E REPORT ERRSYSMODS command to identify missing HIPER maintenance.

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

This method is the quicker of the two, but requires subsequent review of the REPORT ERRSYSMODS to investigate any HIPERs. If you are running SMP/E V3.5 or higher and have received the latest HOLDDATA, you can also choose to run REPORT MISSINGFIX for Fix Category IBM.ProductInstall-RequiredService to investigate missing recommended service.

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

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.

6.1.9 Perform SMP/E ACCEPT

Edit and submit sample job CKLISACC to perform an SMP/E ACCEPT CHECK for IBM Security Key Lifecycle Manager for z/OS. Consult the instructions in the sample job for more information.

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. This is because the SMP/E root cause analysis identifies the cause of only *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 manuals.

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-edits or binds 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.

6.1.10 Cleaning Up Obsolete Data Sets, Paths, and DDDEFs

The following file system paths, which were created and used by previous releases of this product, are no longer used in this release. You can delete these obsolete file system paths after you delete the previous release from your system.

- /usr/lpp/tklm

6.2 Activating IBM Security Key Lifecycle Manager for z/OS

The file system in which you have installed IBM Security Key Lifecycle Manager for z/OS must be mounted in read-only mode during execution. To activate IBM Security Key Lifecycle Manager for z/OS, follow the instructions in *IBM Security Key Lifecycle Manager for z/OS Version 1.1, Planning and User's Guide, SC14-7628*.

7.0 Notices

References in this document 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 on any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

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 online versions of this book, we authorize you to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine readable documentation.

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.

Contacting Customer Support

For support for this or any Tivoli product, you can contact Tivoli Customer Support in one of the following ways:

- Submit a problem management record (PMR) electronically at **IBMSERV/IBMLINK**.
- Submit a problem management record (PMR) electronically from our Web site at http://www.ibm.com/software/sysmgmt/products/support/

You can also review the *IBM Software Support Guide*, which is available on the Web site listed above. An *End of Support Matrix* is provided as well which will tell you when products you are using are nearing the end of support date for a particular version or release.

When you contact Tivoli Customer Support, be prepared to provide identification information for your company so that support personnel can readily assist you. Company identification information may also be needed to access various online services available on the Web site.

The support Web site offers extensive information, including a guide to support services (the IBM Software Support Guide); frequently asked questions (FAQs); and documentation for all Tivoli products, including Release Notes, Redbooks, and Whitepapers. The documentation for some product releases is available in both PDF and HTML formats. Translated documents are also available for some product releases.

Printed in USA

GI11-4300-02