



Program Directory for IBM zSecure Secret Manager

3.2.0

Program Number 5900-C54

FMIDs HBR320

for Use with
z/OS

Document Date: June 2026

GI13-0000-00

Note

Before using this information and the product it supports, be sure to read the general information under 7.0, "Notices" on page 22.

Contents

Release information	v
1.0 Introduction	1
1.1 zSecure Secret Manager Description	1
1.2 zSecure Secret Manager FMIDs	2
2.0 Program Materials	3
2.1 Basic Machine-Readable Material	3
2.2 Program Publications	3
2.3 Program Source Materials	3
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	5
4.0 Program and Service Level Information	6
4.1 Program Level Information	6
4.2 Service Level Information	6
5.0 Installation Requirements and Considerations	7
5.1 Driving System Requirements	7
5.1.1 Machine Requirements	7
5.1.2 Programming Requirements	7
5.2 Target System Requirements	8
5.2.1 Machine Requirements	8
5.2.2 Programming Requirements	8
5.2.2.1 Installation Requisites	8
5.2.2.2 Operational Requisites	9
5.2.2.3 Toleration/Coexistence Requisites	10
5.2.2.4 Incompatibility (Negative) Requisites	10
5.2.3 DASD Storage Requirements	10
5.3 FMIDs Deleted	13
5.4 Special Considerations	13
6.0 Installation Instructions	14
6.1 Installing zSecure Secret Manager	14
6.1.1 SMP/E Considerations for Installing zSecure Secret Manager	14
6.1.2 SMP/E Options Subentry Values	14
6.1.3 SMP/E CALLLIBS Processing	15
6.1.4 Sample Jobs	15

6.1.4.1 Allocate SMP/E GLOBAL CSI (Optional)	16
6.1.4.2 Allocate SMP/E Target/DLIB CSI (Optional)	16
6.1.4.3 Define OPTIONS entry to GLOBAL/TARGET/DLIB zones (Optional)	17
6.1.5 Perform SMP/E RECEIVE	17
6.1.6 Allocate SMP/E Target and Distribution Libraries	17
6.1.7 Allocate SMP/E Target ZFS	17
6.1.8 Create DDDEF Entries	17
6.1.9 Perform SMP/E APPLY	18
6.1.10 Perform SMP/E ACCEPT	20
6.1.11 Run REPORT CROSSZONE	20
6.1.12 Cleaning Up Obsolete Data Sets, Paths, and DDDEFs	21
6.2 Activating zSecure Secret Manager	21
7.0 Notices	22
7.1 Trademarks	22
Reader's Comments	23

Figures

1. Basic Material: Unlicensed Publications	3
2. Publications Useful During Installation	4
3. Component IDs	5
4. Driving System Software Requirements	8
5. Target System Mandatory Installation Requisites	9
6. Target System Mandatory Operational Requisites	9
7. Total DASD Space Required by zSecure Secret Manager	10
8. Storage Requirements for zSecure Secret Manager Target Libraries	12
9. zSecure Secret Manager File System Paths	12
10. Storage Requirements for zSecure Secret Manager Distribution Libraries	12
11. SMP/E Options Subentry Values	14
12. Sample Installation Jobs	15

Release information

The zSecure Release Information topics include details on new features and enhancements, incompatibility warnings, and documentation update information for your zSecure product. You can review the most current version of the release information from the following links:

- What's new: New feature and enhancements in zSecure Secret Manager 3.2.0
<https://www.ibm.com/docs/en/zsecure-secret-manager/3.2.0?topic=release-whats-new-zsecure-secret-manager-320>
- Release notes: Information you need before installing zSecure Secret Manager 3.2.0, such as system requirements, incompatibility warnings, and known problems.
<https://www.ibm.com/docs/en/zsecure-secret-manager/3.2.0?topic=release-notes-zsecure-secret-manager-320>

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 zSecure Secret Manager. This publication refers to IBM zSecure Secret Manager as zSecure Secret Manager.

The Program Directory contains the following sections:

- 2.0, “Program Materials” on page 3 identifies the basic program materials and documentation for zSecure Secret Manager.
- 3.0, “Program Support” on page 5 describes the IBM support available for zSecure Secret Manager.
- 4.0, “Program and Service Level Information” on page 6 lists the APARs (program level) and PTFs (service level) that have been incorporated into zSecure Secret Manager.
- 5.0, “Installation Requirements and Considerations” on page 7 identifies the resources and considerations that are required for installing and using zSecure Secret Manager.
- 6.0, “Installation Instructions” on page 14 provides detailed installation instructions for zSecure Secret Manager. It also describes the procedures for activating the functions of zSecure Secret Manager, or refers to appropriate publications.

Before installing zSecure Secret Manager, 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.

zSecure Secret Manager is supplied in a Custom-Built Product Delivery Offering (CBPDO, 5751-CS3). All service and HOLDDATA for zSecure Secret Manager are included on the CBPDO.

Do not use this program directory if you install zSecure Secret Manager 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 zSecure Secret Manager Description

Secret Manager was designed to ease management of expiring certificates. It uses RACF, ICSF, IBM Vault. Secret Manager stores data in a EzNoSQL Database.

1.2 zSecure Secret Manager FMIDs

zSecure Secret Manager consists of the following FMIDs:

HBRS320

2.0 Program Materials

An IBM program is identified by a program number. The program number for zSecure Secret Manager is 5900-C54.

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 zSecure Secret Manager. 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 14 for more information about how to install the program.

You can find information about the physical media for the basic machine-readable materials for zSecure Secret Manager in the *CBPDO Memo To Users Extension*.

2.2 Program Publications

The following sections identify the basic publications for zSecure Secret Manager 3.2.0.

Figure 1 identifies the basic unlicensed publications for zSecure Secret Manager 3.2.0.

Figure 1. Basic Material: Unlicensed Publications	
Publication Title	Form Number
IBM zSecure Secret Manager Getting Started	N/A

These publications are available at the IBM Documentation at <https://www.ibm.com/docs/en/zsecure-secret-manager/3.2.0>

This information includes a list of all the unlicensed and licensed documentation; see About This Release, topic "zSecure Documentation".

2.3 Program Source Materials

No program source materials or viewable program listings are provided for zSecure Secret Manager.

2.4 Publications Useful During Installation

You might want to use the publications listed in Figure 2 on page 4 during the installation of zSecure Secret Manager which can be found at **IBM Products documentation** <https://www.ibm.com/docs/en/products> .

<i>Figure 2. Publications Useful During Installation</i>	
Publication	
<i>IBM SMP/E for z/OS User's Guide</i>	SA23-2277
<i>IBM SMP/E for z/OS Commands</i>	SA23-2275
<i>IBM SMP/E for z/OS Reference</i>	SA23-2276
<i>IBM SMP/E for z/OS Messages, Codes, and Diagnosis</i>	GA32-0883
<i>Security Server RACF Security Administrator's Guide</i>	SA23-2289
<i>Security Server RACF Command Language Reference</i>	SA23-2292

Note: These publications can be found in IBM Documentation. <https://www.ibm.com/docs/en>

3.0 Program Support

This section describes the IBM support available for zSecure Secret Manager.

3.1 Program Services

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

3.2 Preventive Service Planning

Before you install zSecure Secret Manager, make sure that you review the PSP bucket information for IBM Z products document <https://www.ibm.com/support/pages/node/7127792>. It contains the latest information concerning the installation of IBM products, including the latest service recommendations and cross-product dependencies. This information was previously available in traditional PSP buckets, which are no longer published for IBM Z products.

For support, access the Software Support Website at <https://www.ibm.com/mysupport/>

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 3 identifies the component IDs (COMPID) for zSecure Secret Manager.

<i>Figure 3. Component IDs</i>			
FMID	COMPID	Component Name	RETAIN Release
HBR320	5655ZSA00	zSecure Secret Manager	320

4.0 Program and Service Level Information

This section identifies the program and relevant service levels of zSecure Secret Manager. 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 zSecure Secret Manager.

4.2 Service Level Information

No PTFs against this release of zSecure Secret Manager have been incorporated into the product package.

Frequently check the zSecure Secret Manager 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.

5.0 Installation Requirements and Considerations

The following sections identify the system requirements for installing and activating zSecure Secret Manager. 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.

5.1 Driving System Requirements

This section describes the environment of the driving system required to install zSecure Secret Manager.

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 4. Driving System Software Requirements

Program Number	Product Name	Minimum VRM	Minimum Service Level will satisfy these APARs	Included in the shipped product?
5650-ZOS	z/OS	V03.02.00	N/A	No

Note: SMP/E is a requirement for Installation and is an element of z/OS.

Note: Installation might require migration to new z/OS releases to be service supported. See <https://www.ibm.com/support/lifecycle/>

Part of zSecure Secret Manager is installed into a file system. Before installing zSecure Secret Manager, 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 zSecure Secret Manager 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.

5.2 Target System Requirements

This section describes the environment of the target system required to install and use zSecure Secret Manager.

zSecure Secret Manager 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 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 5. Target System Mandatory Installation Requisites

Program Number	Product Name	Minimum VRM	Minimum Service Level will satisfy these APARs	Included in the shipped product?
5650-ZOS	z/OS	03.02.00	OA68812	No
5650-ZOS	z/OS Security Server	03.02.00	OA68811	No

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.

zSecure Secret Manager 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 6. Target System Mandatory Operational Requisites

Program Number	Product Name	Minimum VRM	Minimum Service Level will satisfy these APARs	Included in the shipped product?
5650-ZOS	z/OS	03.02.00 or higher	OA68812	No
5650-ZOS	z/OS Security Server	03.02.00 or higher	OA68811	No
And both of the following:				
5655-ZOS	EzNoSQL	03.02.00 or higher	N/A	No
5655-ZOS	JAVA 25	03.02.00 or higher	N/A	No

zSecure Secret Manager requires an IBM Vault solution that acts as a private certificate authority for automated certificate renewal. IBM Vault Self-Managed for Z and LinuxONE (IBM Vault) is the recommended solution. IBM Vault is not included with this product and must be provisioned and configured separately.

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.

zSecure Secret Manager has no conditional operational requisites.

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.

zSecure Secret Manager 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.

zSecure Secret Manager has no negative requisites.

5.2.3 DASD Storage Requirements

zSecure Secret Manager libraries can reside on all supported DASD types.

Figure 7 lists the total space that is required for each type of library.

<i>Figure 7. Total DASD Space Required by zSecure Secret Manager</i>		
Library Type	Total Space Required in 3390 Trks	
Target	30	Total space required by Target data sets
Distribution	400	Total space required by Distribution data sets
File System	5250	Total space required by zFS file system

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 17 and `refid=alloc1..`

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:

- SBRSLD and SBRJMOD are candidates for a LNKLIST entry
- The SBRSLD and SBRJMOD datasets are required to be APF-authorized.

The following figures describe the target and distribution libraries and file system paths required to install zSecure Secret Manager. The storage requirements of zSecure Secret Manager 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 8. Storage Requirements for zSecure Secret Manager Target Libraries

Library DDNAME	Member Type	Target Volume	T Y P E	O R G	R E C F M	L R E C L	No. of 3390 Trks	No. of DIR Blks
SBRSSAMP	Sample	ANY	U	PDS	FB	80	20	7
SBRSMAC	Sample	ANY	U	PDS	FB	80	20	7
SBRSLoad	LMOD	ANY	U	PDSE	U	0	30	N/A
SBRJSMOD	LMOD	ANY	U	PDSE	U	0	30	N/A

Figure 9. zSecure Secret Manager File System Paths

DDNAME	T Y P E	Path Name
SBRJSJAVA	N	/usr/lpp/brs/v3r2/java/IBM
SBRSLIB	N	/usr/lpp/brs/v3r2/lib/IBM
SBRSPY	N	/usr/lpp/brs/v3r2/PythonAPI/IBM/

Figure 10. Storage Requirements for zSecure Secret Manager Distribution Libraries

Library DDNAME	T Y P E	O R G	R E C F M	L R E C L	No. of 3390 Trks	No. of DIR Blks
ABRSSAMP	U	PDS	FB	80	20	7
ABRSMAC	U	PDS	FB	80	20	7
ABRSLoad	U	PDSE	U	0	30	N/A
ABRSJMOD	U	PDSE	U	0	30	N/A
ABRSZFS	U	PDSE	VB	32654	350	N/A

5.3 FMIDs Deleted

Installing zSecure Secret Manager 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 zSecure Secret Manager 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

zSecure Secret Manager needs EzNoSQL setup. Please refer to DFSMSxxx documentation.

zSecure Secret Manager comes packaged in TERSED format used by TRSMAIN / AMATERSE. JCL is provided in file hbrs320.restore.jcl to unterse and unpack the files into standard z/OS datasets which are used to install the product via SMP/E. Refer to that JCL job for instructions.

6.0 Installation Instructions

This chapter describes the installation method and the step-by-step procedures to install and to activate the functions of zSecure Secret Manager.

Please note the following points:

- If you want to install zSecure Secret Manager 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.
- The SMP/E dialogs may be used instead of the sample jobs to accomplish the SMP/E installation steps.

6.1 Installing zSecure Secret Manager

6.1.1 SMP/E Considerations for Installing zSecure Secret Manager

Use the SMP/E RECEIVE, APPLY, and ACCEPT commands to install this release of zSecure Secret Manager.

6.1.2 SMP/E Options Subentry Values

The recommended values for certain SMP/E CSI subentries are shown in Figure 11. 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 11. SMP/E Options Subentry Values

Subentry	Value	Comment
DSSPACE	15,5,20	This is the minimum. Any larger value is acceptable.
PEMAX	SMP/E Default	IBM recommends using the SMP/E default for PEMAX.

6.1.3 SMP/E CALLLIBS Processing

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

- JAVADD

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

6.1.4 Sample Jobs

The following sample installation jobs are provided as part of the product to help you install zSecure Secret Manager:

<i>Figure 12. Sample Installation Jobs</i>			
Job Name	Job Type	Description	RELFILE
BRSJSMPA	DEFINE	Sample job to create a Global CSI	IBM.HBRS320.F2
BRSJSMPB	DEFINE	Sample job to create a Target/Dlib CSI	IBM.HBRS320.F2
BRSJSMPC	DEFINE	Sample job to create an SMP/E OPTIONS entry	IBM.HBRS320.F2
BRSJREC	RECEIVE	Sample RECEIVE job	IBM.HBRS320.F2
BRSJALL	ALLOCATE	Sample job to allocate target and distribution libraries	IBM.HBRS320.F2
BRSJALZF	ALLOCATE	Sample job to allocate and mount the install zFS and create directory structure	IBM.HBRS320.F2
BRSJDDD	DDDEF	Sample job to define SMP/E DDDEFs	IBM.HBRS320.F2
BRSJAPP	APPLY	Sample APPLY job	IBM.HBRS320.F2
BRSJACC	ACCEPT	Sample ACCEPT job	IBM.HBRS320.F2

You can copy the sample installation jobs from the directory where your Shopz order is stored by submitting the following job.

```
//STEP1 EXEC PGM=GIMUNZIP,REGION=0M,PARM='HASH=NO'
//SYSUT3 DD UNIT=SYSALLDA,SPACE=(CYL,(10,10))
//SYSUT4 DD UNIT=SYSALLDA,SPACE=(CYL,(15,5))
//SMPJHOME DD PATH='/usr/lpp/java/J7.0/' <===NOTE 1
//SMPCPATH DD PATH='/usr/lpp/smp/classes/' <===NOTE 1
//SMPOUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SMPDIR DD PATHDISP=KEEP,
// PATH='/<ntsdire>/<orderid>/SMPRELF/' <===NOTE 2
//SYSIN DD *
<GIMUNZIP>
<ARCHDEF
name="CBCACHE.IBM.HBRS320.F2.pax.Z"
volume="<volser>" <===NOTE 3
newname="<your-prefix>.BRSINST" <===NOTE 4
</ARCHDEF>
</GIMUNZIP>
/*
```

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

Add a job card that is specific to your installation requirements.

Note 1: Change these directories to your installations java and smp classes directories.

Note 2: Change ntsdire to the directory that holds your Shopz orders. Change orderid to your order ID, for example 2008567304_000010_PROD.

Note 3: Change volser to a volser that you want the output dataset to reside on.

Note 4: Change your-prefix to the high-level qualifier(s) for the output dataset.

Installing through electronic shipment, refer to *CBPDO Internet Delivery User's Guide*.

6.1.4.1 Allocate SMP/E GLOBAL CSI (Optional)

If you choose to install this product into its own SMP/E environment, edit and submit sample job BRSJSMPA to allocate a new SMP/E GLOBAL CSI.

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

6.1.4.2 Allocate SMP/E Target/DLIB CSI (Optional)

If you choose to install this product into its own SMP/E environment, edit and submit sample job BRSJSMPB to allocate a new SMP/E TARGET/DLIB CSI.

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

6.1.4.3 Define OPTIONS entry to GLOBAL/TARGET/DLIB zones (Optional)

If you choose to install this product into its own SMP/E environment, edit and submit sample job BRSJSMPC to create and specify an OPTIONS entry for use during installation of zSecure Secret Manager.

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

6.1.5 Perform SMP/E RECEIVE

If you install zSecure Secret Manager as a Web download package, the SMP/E RECEIVE is performed during the execution of the README file. In this case, you can skip this section and continue with the next section of the program directory.

If you have obtained zSecure Secret Manager as part of a CBPDO, use the RCVPDO job in the CBPDO RIMLIB data set to receive the zSecure Secret Manager FMIDs, service, and HOLDDATA that are included on the CBPDO package. For more information, see the documentation that is included in the CBPDO.

You can also choose to edit and submit sample job BRSJREC to perform the SMP/E RECEIVE for zSecure Secret Manager. 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 SMP/E Target and Distribution Libraries

Edit and submit sample job BRSJALL to allocate the SMP/E target and distribution libraries for zSecure Secret Manager. 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.

6.1.7 Allocate SMP/E Target ZFS

Edit and submit sample job BRSJALZF to allocate the SMP/E target zFS and create the directoru structure for zSecure Secret Manager. 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 Create DDDEF Entries

Edit and submit sample job BRSJDDD to create DDDEF entries for the SMP/E target and distribution libraries for zSecure Secret Manager. 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. Ensure that you have the latest HOLDDATA; then edit and submit sample job BRSJAPP to perform an SMP/E APPLY CHECK for zSecure Secret Manager. Consult the instructions in the sample job for more information.

The latest HOLDDATA is available through several different portals, including <https://public.dhe.ibm.com/s390/assigns/> or <https://www.ibm.com/support/pages/enhanced-holddata-zos> for usage instructions. 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.

After installing new functions, you should perform two operations:

1. Create a backup of the updated data sets, including any SMP/E data sets affected, in case something happens to the data sets during the next phase.
2. Do some testing before putting the new function into production.

After you are satisfied that an applied SYSMOD has performed reliably in your target system, you can install it in your distribution libraries using the ACCEPT process.

Another good practice is to accept most SYSMODs, particularly FMIDs, before performing another APPLY process. This provides you the ability to use the RESTORE process of SMP/E and to support the scenario where SMP/E needs to create a new load module from the distribution libraries during the APPLY process.

6.1.10 Perform SMP/E ACCEPT

Edit and submit sample job BRSJACC to perform an SMP/E ACCEPT CHECK for zSecure Secret Manager. 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. 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 zSecure Secret Manager, 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

There is not cleanup needed when installing this release.

6.2 Activating zSecure Secret Manager

zSecure Secret Manager is not fully operational after the SMP/E installation is completed. You have to do further customization to activate this function.

The publication *IBM zSecure Secret Manager Getting Started 3.2.0, N/A* contains the necessary information to fully activate the functions of zSecure Secret Manager.

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 refer to the instructions in the **Service Recommendation Summary and Service Recommendations** and **Cross Product Dependencies** sections of the **PSP bucket information for IBM Z products** at <https://www.ibm.com/support/pages/node/7127792>, to ensure you have all required service.

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 (other IBM trademark listed on the IBM Trademarks List) are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

Reader's Comments

Program Directory for IBM zSecure Secret Manager, June 2026 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 ibmdocs@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. °



Printed in Ireland

GI13-0000-00

