# Program Directory for
# IBM InfoSphere Guardium Data Encryption
# for DB2 and IMS Databases

V01.02.00

Program Number 5655-P03

FMID H29F120

for Use with
z/OS

Document Date: February 2011

GI10-8682-01

**Note !**

Before using this information and the product it supports, be sure to read the general information under 7.0, “Notices” on page 25.

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.

# Contents

# Figures

# 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 InfoSphere Guardium Data Encryption for DB2 and IMS Databases. This publication refers to IBM InfoSphere Guardium Data Encryption for DB2 and IMS Databases as InfoSphere Guardium Data Encryption.

The Program Directory contains the following sections:

- 2.0, “Program Materials” on page 4 identifies the basic and optional program materials and documentation for InfoSphere Guardium Data Encryption.
- 3.0, “Program Support” on page 7 describes the IBM support available for InfoSphere Guardium Data Encryption.
- 4.0, “Program and Service Level Information” on page 9 lists the APARs (program level) and PTFs (service level) that have been incorporated into InfoSphere Guardium Data Encryption.
- 5.0, “Installation Requirements and Considerations” on page 10 identifies the resources and considerations that are required for installing and using InfoSphere Guardium Data Encryption.
- 6.0, “Installation Instructions” on page 18 provides detailed installation instructions for InfoSphere Guardium Data Encryption. It also describes the procedures for activating the functions of InfoSphere Guardium Data Encryption, or refers to appropriate publications.

Before installing InfoSphere Guardium Data Encryption, 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 7 tells you how to find any updates to the information and procedures in this Program Directory.

InfoSphere Guardium Data Encryption 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 InfoSphere Guardium Data Encryption are included on the CBPDO tape.

Do not use this program directory if you install InfoSphere Guardium Data Encryption 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 InfoSphere Guardium Data Encryption Description

The IBM InfoSphere Guardium Data Encryption for DB2 and IMS Databases, V1.2 (5655-P03) tool is part of the InfoSphere Guardium portfolio, providing you with data encryption for both IBM DB2 Database for z/OS and IBM Information Management System (IMS) databases. This enables you to better protect your sensitive and private data for DB2 and IMS.

The need for data encryption has moved to the forefront of technology concerns with the increased demand for data privacy and security. The InfoSphere Guardium Data Encryption for DB2 and IMS Databases product addresses this need. The product delivers the capability to leverage the zSeries and S/390 Crypto Hardware to efficiently secure sensitive and private data at the DB2 row level and the IMS segment level.

InfoSphere Guardium Data Encryption for DB2 and IMS Databases offers:

- DB2 edit routines and IMS exit routines that invoke the z/OS Integrated Cryptographic Service Facility (ICSF), which exploits the Crypto Hardware for data encryption and decryption
- Sample implementation jobs
- An ISPF front end to build implementation jobs
- The capability to specify unique encryption keys

InfoSphere Guardium Data Encryption for DB2 and IMS Databases, V1.2:

- Is a single tool for both your DB2 and IMS databases.
- Offers data privacy by encrypting and decrypting data.
- Uses the Triple Data Encryption Algorithm (TDEA), which is also known as the Triple Data Encryption Standard (Triple DES); the ANSI Data Encryption Algorithm (DEA), which is also known as the Data Encryption Standard (DES); and the Advanced Encryption Standard (AES) algorithms.
- Enables you to leverage the power of storage area networks (SANs) more safely while complying with privacy and security regulations that are in place or that are being enacted worldwide.
- Adheres to the existing z/OS security model.
- Provides an ISPF front end that allows you to create and customize encryption, external compression, and exit drivers.
- Provides exit drivers to permit the execution of compression and encryption at the same exit point to avoid negating any existing compression capability. The compression exit routine invokes System z Crypto Hardware and features that assist high performance and low overhead.
- Allows fast implementation, after an encryption key label has been defined by the security analyst, through the use of standard DB2 and IMS exit routines invoked during database reload.
- Requires no changes to applications.
- Rolls up maintenance against the previous release of the product to the new release.

## 1.2 InfoSphere Guardium Data Encryption FMID

InfoSphere Guardium Data Encryption consists of the following FMID:

H29F120

# 2.0 Program Materials

An IBM program is identified by a program number and a feature number. The program number for InfoSphere Guardium Data Encryption is 5655-P03 and its feature number is 6000.

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 InfoSphere Guardium Data Encryption. 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 18 for more information about how to install the program.

You can find information about the physical tape for the basic machine-readable materials for InfoSphere Guardium Data Encryption in the *CBPDO Memo To Users Extension*.

Figure 1 describes the program file content for InfoSphere Guardium Data Encryption. You can refer to the *CBPDO Memo To Users Extension* to see where the files reside on the tape.

**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 (Page 1 of 2). Program File Content*

| Name | ORG | RECFM | LRECL | BLK SIZE |
|---|---|---|---|---|
| SMPMCS | SEQ | FB | 80 | 6400 |
| IBM.H29F120.F1 | PDS | FB | 80 | 8800 |
| IBM.H29F120.F2 | PDS | FB | 80 | 8800 |
| IBM.H29F120.F3 | PDS | FB | 80 | 8800 |
| IBM.H29F120.F4 | PDS | U | 0 | 6144 |
| IBM.H29F120.F5 | PDS | FB | 80 | 8800 |

*Figure 1 (Page 2 of 2). Program File Content*

| Name | ORG | RECFM | LRECL | BLK SIZE |
|---|---|---|---|---|
| IBM.H29F120.F6 | PDS | FB | 80 | 8800 |
| IBM.H29F120.F7 | PDS | FB | 80 | 8800 |
| IBM.H29F120.F8 | PDS | FB | 80 | 8800 |

## 2.2 Optional Machine-Readable Material

No optional machine-readable materials are provided for InfoSphere Guardium Data Encryption.

## 2.3 Program Publications

The following sections identify the basic and optional publications for InfoSphere Guardium Data Encryption.

### 2.3.1 Basic Program Publications

Figure 2 identifies the basic unlicensed program publications for InfoSphere Guardium Data Encryption. One copy of each of these publications is included when you order the basic materials for InfoSphere Guardium Data Encryption. For additional copies, contact your IBM representative.

*Figure 2. Basic Material: Unlicensed Publications*

| Publication Title | Form Number |
|---|---|
| IBM InfoSphere Guardium Data Encryption for DB2 and IMS Databases License Information | GC18-9548 |

Figure 3 identifies the basic unlicensed or licensed publications that are not available in hardcopy format, but are available through the internet or other media for InfoSphere Guardium Data Encryption.

*Figure 3. Basic Material: Other Unlicensed or Licensed Publications*

| Publication Title | Form Number | How Available |
|---|---|---|
| IBM InfoSphere Guardium Data Encryption for DB2 and IMS Databases User's Guide | SC19-3219 | http://www.ibm.com/software/data/db2imstools/library.html |

Publications are available in PDF and BookManager formats on CD-ROM and on DVD on the next release of software product libraries:

- *z/OS and Software Products DVD Collection, SK3T-4271**
  *requires a DVD drive in DVD-9 (single-sided, dual-layer) format

### 2.3.2 Optional Program Publications

No optional publications are provided for InfoSphere Guardium Data Encryption.

## 2.4 Program Source Materials

No program source materials or viewable program listings are provided for InfoSphere Guardium Data Encryption.

## 2.5 Publications Useful During Installation

You might want to use the publications listed in Figure 4 during the installation of InfoSphere Guardium Data Encryption. To order copies, contact your IBM representative or visit the IBM Publications Center at http://www.ibm.com/shop/publications/order.

*Figure 4. 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 InfoSphere Guardium Data Encryption.

## 3.1 Program Services

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

## 3.2 Preventive Service Planning

Before you install InfoSphere Guardium Data Encryption, 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 InfoSphere Guardium Data Encryption as part of a CBPDO, HOLDDATA is included.

If the CBPDO for InfoSphere Guardium Data Encryption 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-01.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 InfoSphere Guardium Data Encryption are shown as follows:

*Figure 5. PSP Upgrade and Subset ID*

| UPGRADE | SUBSET | Description |
|---|---|---|
| 5655P03 | H29F120 | InfoSphere Guardium Data Encryption |

## 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 6 on page 8 identifies the component IDs (COMPID) for InfoSphere Guardium Data Encryption.

*Figure 6. Component IDs*

| FMID | COMPID | Component Name | RETAIN Release |
|---|---|---|---|
| H29F120 | 5655P0300 | InfoSphere Guardium Data Encryption | 120 |

# 4.0 Program and Service Level Information

This section identifies the program and relevant service levels of InfoSphere Guardium Data Encryption. 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

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

- FMID H29F110

| | | |
|---|---|---|
| PK17004 | PK69786 | PM04976 |
| PK18479 | PK75337 | PM08556 |
| PK37305 | PK80254 | PM10630 |
| PK43736 | PK81724 | PM11712 |
| PK45596 | PK85788 | PM15095 |
| PK48784 | PK89873 | PM16551 |
| PK48886 | PK93858 | PM18614 |
| PK55137 | PK97686 | PM19473 |
| PK55140 | PK99119 | PM22355 |
| PK56108 | PM00453 | PM27786 |

## 4.2 Service Level Information

No PTFs against this release of InfoSphere Guardium Data Encryption have been incorporated into the product tape.

It is highly recommended that you frequently check the InfoSphere Guardium Data Encryption 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 InfoSphere Guardium Data Encryption. 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 asses these impacts without disrupting your production system.

## 5.1 Driving System Requirements

This section describes the environment of the driving system that is required to install InfoSphere Guardium Data Encryption.

### 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 7. 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 | V01.10.00 | N/A | No |
| 5655-G44 | IBM SMP/E for z/OS | V03.05.00 | N/A | No |

## 5.2 Target System Requirements

This section describes the environment of the target system that is required to install and use InfoSphere Guardium Data Encryption.

InfoSphere Guardium Data Encryption installs in the DBS (P115) SREL.

### 5.2.1 Machine Requirements

InfoSphere Guardium Data Encryption for DB2 and IMS Databases, V1.2 has the following requirements:

- InfoSphere Guardium Data Encryption for DB2 and IMS Databases is supported on any processor capable of operating DB2 V8 or later and IMS V10 or later.
- To support the z10¸ processor encryption technology, Crypto Express3 with CP Assist for Cryptographic Function (CPACF protected key) hardware is required and must be installed.
- Crypto Express:
  - On the z9 EC and the z10, the Crypto Express2 feature (feature code 0863) is required.
  - On the z9 BC, the Crypto Express2 feature (feature code 0863) or the Crypto Express2-1P (feature code 0870) is required.
  - At least one of the cryptographic engines must be configured as a coprocessor to provide secure key capability.
  - Installation of either Crypto Express2 feature requires that the CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement feature (feature code 3863) is installed.
- On z890 and z990 systems, either a PCIXCC (feature code 0868) or a Crypto Express2 (feature code 0863) provides secure key support. Installation of either of these features requires that the CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement feature (feature code 3863) is installed.
- The Cryptographic Coprocessor Feature (CCF) provides secure key support on z800, z900, and earlier machines (G3, G4, G5, G6, Multiprise 2000, Multiprise 3000). The CCF hardware modules:
  - Must be enabled with configuration data, a feature that is ordered separately.

  - Require a processor power-on-reset (POR) to complete data loading into the cryptographic modules. Because this hardware does not support the clear key APIs, the use of clear keys by InfoSphere Guardium Data Encryption for DB2 and IMS Databases is not supported on the CCF-based machines.
  - The PCICC feature (feature code 0861) is an optional secure key device on the z800 and z900 systems.
- Additional hardware requirements for clear key data encryption include:
  - A z890 or z990 or later server.
  - z10 CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement (feature code 3863).
  - A secure key device for initializing and using the CKDS.
    - On a z890/z990 system, a PCIXCC or the CEX2 is required.
    - On a z9 BC system, either a CEX2 or a CEX2-1P is required with at least one engine configured as a coprocessor.
    - On a z9 EC or a z10 system, a CEX2 is required with at least one engine configured as a coprocessor.

For further configuration information, consult the following publications:

- zEnterprise System Processor Resource/Systems Manager Planning Guide
- System z10 System Processor Resource/Systems Manager Planning Guide
- System z10 Support Element Operations Guide

## 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.

InfoSphere Guardium Data Encryption 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.

InfoSphere Guardium Data Encryption 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.

**z/OS ICSF Additional Information**

InfoSphere Guardium Data Encryption for DB2 and IMS Databases requires that the Integrated Cryptographic Service Facility (ICSF), an element of z/OS, is active and the ICSF version must support the cryptographic device on the specific platform. ICSF runs on processors that support the Integrated Cryptographic Coprocessor Feature.

- Before use of the hardware encryption can occur, the hardware modules must be loaded with at least host DES Master Keys.
- ICSF is required to be active for the I/O requests to be passed to the hardware cryptographic modules.

Note: InfoSphere Guardium Data Encryption for DB2 and IMS Databases will fail if ICSF is not active or the DES Master Keys are not loaded into the crypto modules.

*Figure 8. Target System Mandatory Operational Requisites*

| Program Number | Product Name and Minimum VRM/Service Level |
|---|---|
| Any **one** of the following: | |
| 5625-DB2 | DB2 UDB for z/OS, V08.01.00 |
| 5697-N29 | DB2 UDB for z/OS Value Unit Edition, V08.01.00 |
| 5635-DB2 | DB2 for z/OS, V09.01.00 |
| 5697-P12 | DB2 for z/OS Value Unit Edition, V09.01.00 |
| 5605-DB2 | DB2 for z/OS, V10.01.00 |
| 5697-P31 | DB2 for z/OS Value Unit Edition, V10.01.00 |
| 5635-A01 | IMS V10.01.00 |
| 5635-A02 | IMS V11.01.00 |
| 5635-A03 | IMS V12.01.00* |

***Note**

Refer to the IMS V12.01.00 Software Announcement for more information or talk to your IBM representative.

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.

InfoSphere Guardium Data Encryption 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.

InfoSphere Guardium Data Encryption 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.

InfoSphere Guardium Data Encryption has no negative requisites.

## 5.2.3 DASD Storage Requirements

InfoSphere Guardium Data Encryption libraries can reside on all supported DASD types.

Figure 9 lists the total space that is required for each type of library.

*Figure 9. Total DASD Space Required by InfoSphere Guardium Data Encryption*

| Library Type | Total Space Required in 3390 Trks |
|---|---|
| Target | 19 Tracks |
| Distribution | 19 Tracks |

**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. This 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 6.1.7, “Allocate SMP/E Target and Distribution Libraries” on page 21.

3. 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.
4. 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.
5. 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 required to install InfoSphere Guardium Data Encryption. The storage requirements of InfoSphere Guardium Data Encryption must be added to the storage required by other programs having data in the same library.

**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 10 (Page 1 of 2). Storage Requirements for InfoSphere Guardium Data Encryption Target Libraries*

| Library DDNAME | Member Type | Target Volume | TYPE | ORG | RECFM | LRECL | No. of 3390 Trks | No. of DIR Blks |
|---|---|---|---|---|---|---|---|---|
| SDECBASE | Sample | any | U | PDS | FB | 80 | 3 | 2 |

*Figure 10 (Page 2 of 2). Storage Requirements for InfoSphere Guardium Data Encryption Target Libraries*

| Library DDNAME | Member Type | Target Volume | TYPE | ORG | RECFM | LRECL | No. of 3390 Trks | No. of DIR Blks |
|---|---|---|---|---|---|---|---|---|
| SDECCEXE | EXEC | any | U | PDS | FB | 80 | 3 | 2 |
| SDECLMD0 | LMOD | any | U | PDS | U | 0 | 3 | 4 |
| SDECMLIB | Message | any | U | PDS | FB | 80 | 2 | 2 |
| SDECPLIB | Panel | any | U | PDS | FB | 80 | 3 | 2 |
| SDECSAMP | Sample | any | U | PDS | FB | 80 | 3 | 2 |
| SDECSLIB | Skel | any | U | PDS | FB | 80 | 2 | 2 |

*Figure 11. Storage Requirements for InfoSphere Guardium Data Encryption Distribution Libraries*

| Library DDNAME | TYPE | ORG | RECFM | LRECL | No. of 3390 Trks | No. of DIR Blks |
|---|---|---|---|---|---|---|
| ADECBASE | U | PDS | FB | 80 | 3 | 2 |
| ADECCEXE | U | PDS | FB | 80 | 3 | 2 |
| ADECMLIB | U | PDS | FB | 80 | 2 | 2 |
| ADECMOD0 | U | PDS | U | 0 | 3 | 4 |
| ADECPLIB | U | PDS | FB | 80 | 3 | 2 |
| ADECSAMP | U | PDS | FB | 80 | 3 | 2 |
| ADECSLIB | U | PDS | FB | 80 | 2 | 2 |

## 5.3 FMIDs Deleted

Installing InfoSphere Guardium Data Encryption 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 InfoSphere Guardium Data Encryption 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

InfoSphere Guardium Data Encryption 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 InfoSphere Guardium Data Encryption.

Please note the following:

- If you want to install InfoSphere Guardium Data Encryption 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 InfoSphere Guardium Data Encryption

### 6.1.1 SMP/E Considerations for Installing InfoSphere Guardium Data Encryption

Use the SMP/E RECEIVE, APPLY, and ACCEPT commands to install this release of InfoSphere Guardium Data Encryption.

### 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 | (200,200,500) | 3390 DASD tracks |
| 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 InfoSphere Guardium Data Encryption:

*Figure 13. Sample Installation Jobs*

| Job Name | Job Type | Description | RELFILE |
|---|---|---|---|
| DECALA | SMP/E | Sample job to allocate and initialize a new SMP/E CSI data set **(Optional)** | IBM.H29F120.F2 |
| DECALB | SMP/E | Sample job to allocate SMP/E data sets **(Optional)** | IBM.H29F120.F2 |
| DECRECEV | RECEIVE | Sample RECEIVE job | IBM.H29F120.F2 |
| DECALLOC | ALLOCATE | Sample job to allocate target and distribution libraries | IBM.H29F120.F2 |
| DECDDDEF | DDDEF | Sample job to define SMP/E DDDEFs | IBM.H29F120.F2 |
| DECAPPLY | APPLY | Sample APPLY job | IBM.H29F120.F2 |
| DECACCEP | ACCEPT | Sample ACCEPT job | IBM.H29F120.F2 |

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 on page 18 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=*
//************************************************************
//* Make the //TAPEIN DD statement below active if you install*
//* from a CBPDO tape by uncommenting the DD statement below. *
//************************************************************
//*TAPEIN   DD DSN=IBM.H29F120.F2,UNIT=tunit,
//*         VOL=SER=volser,LABEL=(x,SL),
//*         DISP=(OLD,KEEP)
//************************************************************
//* Make the //TAPEIN DD statement below active if you install*
//* from a product tape received outside the CBPDO process    *
//* (using the optional SMP/E RECEIVE job) by uncommenting    *
//* the DD statement below.                                   *
//************************************************************
//*TAPEIN   DD DSN=IBM.H29F120.F2,UNIT=tunit,
//*         VOL=SER=29F120,LABEL=(3,SL),
//*         DISP=(OLD,KEEP)
//************************************************************
//* Make the //FILEIN DD statement below active for           *
//* downloaded DASD files.                                    *
//************************************************************
//*FILEIN   DD DSN=IBM.H29F120.F2,UNIT=SYSALLDA,DISP=SHR,
//*         VOL=SER=filevol
```

```
//OUT      DD DSNAME=jcl-library-name,
//          DISP=(NEW,CATLG,DELETE),
//          VOL=SER=dasdvol,UNIT=SYSALLDA,
//          SPACE=(TRK,(20,10,5))
//SYSUT3   DD UNIT=SYSALLDA,SPACE=(CYL,(1,1))
//SYSIN    DD *
    COPY INDD=xxxxIN,OUTDD=OUT
/*
```

In the sample above, update the statements as noted below:

If using TAPEIN:

**tunit** is the unit address where the product tape is mounted
**volser** is the volume serial matching the product tape
**x** is the tape file number where the data set name is on the tape
Refer to the documentation provided by CBPDO to see where IBM.H29F120.F2 is on the tape.

If using 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 will be stored
**dasdvol** is the volume serial of the DASD device where the output data set will reside

SYSIN

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

## 6.1.4 Allocate SMP/E CSI (Optional)

If you are using an existing CSI, do not execute this job.

If you are allocating a new SMP/E data set for this install, edit, and submit sample job DECALA to allocate the SMP/E data set for InfoSphere Guardium Data Encryption. 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 Initialize CSI zones (Optional)

Edit and submit sample job DECALB to initialize SMP/E zones for InfoSphere Guardium Data Encryption. 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 Perform SMP/E RECEIVE

If you have obtained InfoSphere Guardium Data Encryption as part of a CBPDO, use the RCVPDO job in the CBPDO RIMLIB data set to receive the InfoSphere Guardium Data Encryption FMID, 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 DECRECEV to perform the SMP/E RECEIVE for InfoSphere Guardium Data Encryption. 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 and Distribution Libraries

Edit and submit sample job DECALLOC to allocate the SMP/E target and distribution libraries for InfoSphere Guardium Data Encryption. 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 DECDDDEF to create DDDEF entries for the SMP/E target and distribution libraries for InfoSphere Guardium Data Encryption. 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 DECAPPLY to perform an SMP/E APPLY CHECK for InfoSphere Guardium Data Encryption. 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 have received the latest HOLDDATA, add the FIXCAT operand to the APPLY command as shown below.

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

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:** This job should complete with a return code 4 or less, and may issue any of the following messages which do not affect product installation: GIM23903W or GIM23913W and IEW2454W.

## 6.1.10 Perform SMP/E ACCEPT

Edit and submit sample job DECACCEP to perform an SMP/E ACCEPT CHECK for InfoSphere Guardium Data Encryption. 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-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 InfoSphere Guardium Data Encryption, 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.

## 6.2 Activating InfoSphere Guardium Data Encryption

The publication *IBM InfoSphere Guardium Data Encryption for DB2 and IMS Databases User's Guide, SC19-3219* contains the necessary information to customize and use InfoSphere Guardium Data Encryption.

# 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 Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

# Reader's Comments

**Program Directory for IBM InfoSphere Guardium Data Encryption for DB2 and IMS Databases, February 2011**

You may use this form to comment about this document, 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.

For each of the topics below please indicate your satisfaction level by circling your choice from the rating scale. If a statement does not apply, please circle N.

**RATING SCALE**

```
  very                                very          not
satisfied  <====================>  dissatisfied  applicable
    1        2        3        4        5            N
```

| | Satisfaction | | | | | |
|---|---|---|---|---|---|---|
| Ease of product installation | 1 | 2 | 3 | 4 | 5 | N |
| Contents of Program Directory | 1 | 2 | 3 | 4 | 5 | N |
| Installation Verification Programs | 1 | 2 | 3 | 4 | 5 | N |
| Time to install the product | 1 | 2 | 3 | 4 | 5 | N |
| Readability and organization of Program Directory tasks | 1 | 2 | 3 | 4 | 5 | N |
| Necessity of all installation tasks | 1 | 2 | 3 | 4 | 5 | N |
| Accuracy of the definition of the installation tasks | 1 | 2 | 3 | 4 | 5 | N |
| Technical level of the installation tasks | 1 | 2 | 3 | 4 | 5 | N |
| Ease of getting the system into production after installation | 1 | 2 | 3 | 4 | 5 | N |

How did you order this product?

___ CBPDO
___ CustomPac
___ ServerPac
___ Independent
___ Other

Is this the first time your organization has installed this product?

___ Yes
___ No

Were the people who did the installation experienced with the installation of z/OS products?

___ Yes

__ No

If yes, how many years? __

If you have any comments to make about your ratings above, or any other aspect of the product installation, please list them below:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Please provide the following contact information:

_____
Name and Job Title

_____
Organization

_____

_____
Address

_____
Telephone

Thank you for your participation.

Please send the completed form to (or give to your IBM representative who will forward it to the IBM InfoSphere Guardium Data Encryption for DB2 and IMS Databases Development group):

International Business Machines Corporation
Reader's Comments
Department DTX/E269
555 Bailey Avenue
San Jose, California
USA
95141-9989

E-Mail: comments@us.ibm.com

Printed in USA

GI10-8682-01