iSecurity PGP Encryption

User Guide
Version 1.69

www.razlee.com

Contents

About this Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the- box" security. To learn more about the iSecurity Suite, visit our website at http://www.razlee.com/.

Intended Audience

The PGP EncryptionUser Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on page 5.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter**, **Shift-Tab**.

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRACT **> 81 > 32**

meaning: Syslog definitions activated by typing ***STRACT***and selecting option: **81** then option: **32**.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- **F1**: **Help** Display context-sensitive help
- **F3**: **Exit** End the current task and return to the screen or menu from which the task was initiated
- **F4**: **Prompt** Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- **F6**: **Add New** Create a new record or data item
- **F8**: **Print** Print the current report or data item
- **F9**: **Retrieve** Retrieve the previously-entered command
- **F12**: **Cancel** Return to the previous screen or menu without updating

Legal Notice

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

Contacts

Raz-Lee Security Inc. www.razlee.com

Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)

Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

-

Getting Started

This section describes the first steps you need to take when you start working with **PGP Encryption**, as well as listing the standard field names, option s and command keys used in the product.

Installation of PGP Encryption is documented in the global **iSecurity Installation and Base Support** manual.

Standard Fields, Options, and Command Keys

All standard fields, options and command keys are described in the table below. However, some standard command keys are not documented here as they need to have links in their description in each specific UI (for example, F6).

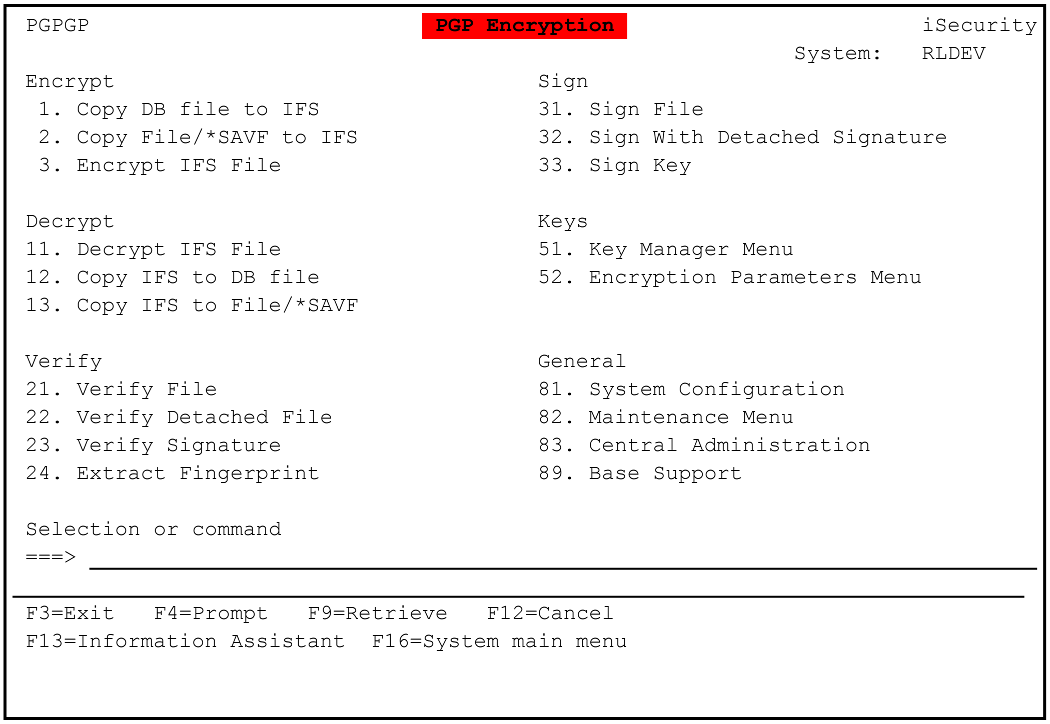
Field/Option/Command Key	Description
Library	Library name. Depending on the context, you may need to enter a specific Library Name, a generic Library Name (for example, ABC*), or you may also be allowed to enter *ALL.
Opt	The option you want to use on the selected item from the list. Put the cursor on the **Opt** field in the appropriate row and then either type the required option in the field or click on the required option in the list of options at the top of the screen.
Subset	Limits the list being displayed to only those members of the list whose value contains the value in the subset field. Use the **Subset** field to make it easier to access the specific value you are searching for.
F3=Exit	Exits from the current display or option, and returns to the calling display. In most cases, any information you have added or changed on the current display is discarded.
F4=Prompt	Displays a prompt window containing additional information about the current input prompt, usually in the form of a list. You may be able to choose any value from this list by typing 1 in the Opt prompt next to the value you want to use. Prompt is context-sensitive. You need to position the cursor on the input prompt to which the information applies before you press **F4**.
F12=Cancel	Exits from the current display or option, and returns to the previous display. Any information you have added or changed on the current display is discarded.
1=Select	Displays the selected item in a list in a screen that allows you to modify the selected item.
3=Copy	Displays a screen that allows you to copy the selected item. You will be able to change the

Field/Option/Command Key	Description
	major identifier of the item. You will then the need to select the new item to make all other necessary changes.
4=Delete	Deletes the selected item in a list. You may be asked to confirm your choice before the delete operation is performed.

Accessing PGP Encryption

You access all PGP Encryption functionality through the Encryption main menu.

To access the system: type **`strpgp`** in the command line and press **Enter**. The **PGP Encryption** Main Menu appears.



```
PGPGP                          PGP Encryption                        iSecurity
                                                            System:    RLDEV
Encrypt                                        Sign
 1. Copy DB file to IFS                        31. Sign File
 2. Copy File/*SAVF to IFS                     32. Sign With Detached Signature
 3. Encrypt IFS File                           33. Sign Key

Decrypt                                        Keys
11. Decrypt IFS File                           51. Key Manager Menu
12. Copy IFS to DB file                        52. Encryption Parameters Menu
13. Copy IFS to File/*SAVF

Verify                                         General
21. Verify File                                81. System Configuration
22. Verify Detached File                       82. Maintenance Menu
23. Verify Signature                           83. Central Administration
24. Extract Fingerprint                        89. Base Support

Selection or command
===> _________________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

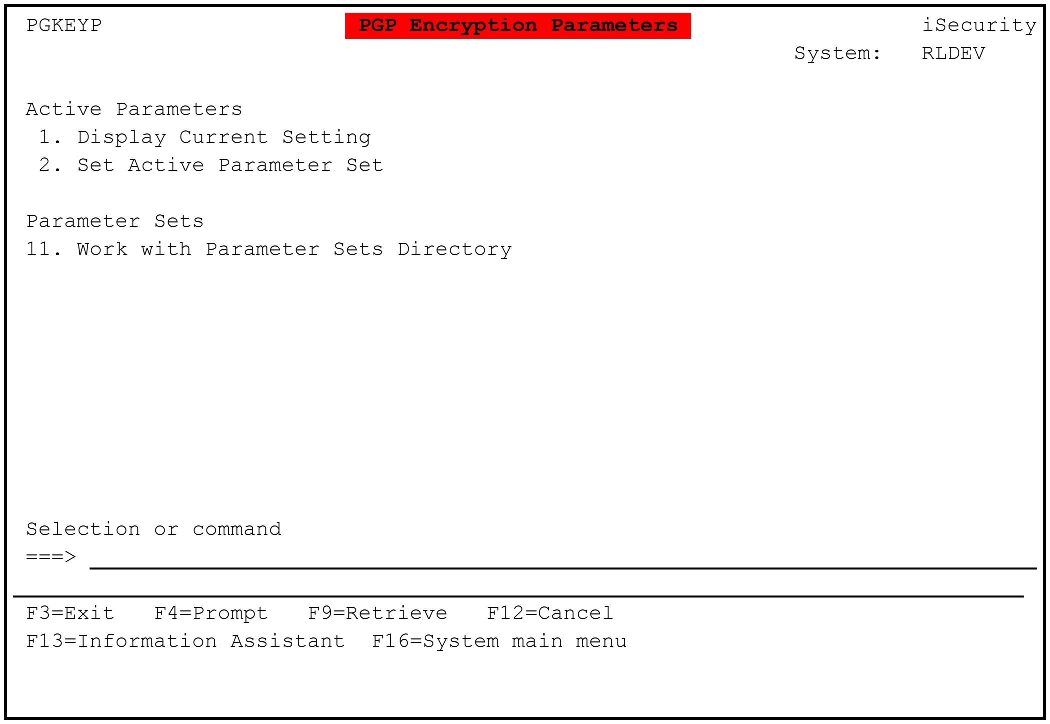
Field/Option/Command Key	Description
1. Copy DB file to IFS	Opens the **Copy To Import File (CPYTOIMPF)** screen. Use this option to copy externally described files to import files.
2. Copy File/*SAVF to IFS	Opens the **Copy to Stream File (CPYTOSTMF)** screen. Use this option to copy database files and save files to stream files.
3. Encrypt IFS File	Opens the **PGP Encrypt File (PGENCFL)** screen. Use this this option to define the file to be encrypted and the encryption key to use.
11. Decrypt IFS	Opens the **PGP Decrypt File (PGDECFL)** screen. Use this this option to define the file to be decrypted and the password to access the file.
12. Copy IFS to DB file	Opens the **Copy from Import File (CPYFRMIMPF)** screen. Use this option to copy import files to database files.
13. Copy IFS to File/*SAVF	Opens the **Copy from Stream File (CPYFRMSTMF)** screen. Use this option to copy stream files to database files.
21. Verify File	Opens the **PGP Verify File (PGVERFL)** screen. Use this option to define the file to be verified.
22. Verify Detached File	Opens the **PGP Verify Detached File (PGVERDFL)** screen. Use this option to define the file to be verified and the Signature to use in the verification.
23. Verify Signature	Opens the **PGP Verify Signature (PGVERSIG)** screen. Use this option to define the signature key to be verified.
24. Extract Fingerprint	Opens the **PGP Fingerprint (PGEXTFP)** screen. Use this option to define the PGP User to be verified.
31. Sign File	Opens the **PGP Sign File (PGSIGFL)** screen. Use this option to add a signature to a file.
32. Sign With Detached Signature	Opens the **PGP Sign w. Detached Signature (PGSIGDFL)** screen. Use this option to add a signature to a detached file.

Field/Option/Command Key	Description
33. Sign Key	Opens the **PGP Sign Key (PGSIGKEY)** screen. Use this option to add a signature to a key.
51. Key Manager Menu	Opens the **PGP Key Manager** menu, which enables you to work with key definitions.
52. Encryption Parameters Menu	Opens the **PGP Encryption Parameters** menu, which enables you to work with current and active encryption parameters.
81. System Configuration	Opens the **System Configuration** menu. The items in this menu are used for the iSecurity Field Encryption porduct and documented in its manual. They are not used for PGP Encryption.
82. Maintenance Menu	Opens the **Maintenance** menu. The items in this menu are used for the iSecurity Field Encryption porduct and documented in its manual. They are not used for PGP Encryption.
83. Central Administration	Opens the **Central Administration** menu, which enables you to work with various definitions that are common for all modules of iSecurity.
89. Base Support	Opens the **BASE Support** menu, which enables you to work with various settings that are common for all modules of iSecurity.

Encryption Parameters Menu

The **Encryption Parameters** Menu allows you to edit various parameter sets for working with PGP in different scenarios.It follows the standard PGP workflow.

To access the **Encryption Parameters** Menu, select **52. Encryption Parameters Menu** in the **PGP Encryption** main menu. The **PGP Encryption Parameters** menu appears.

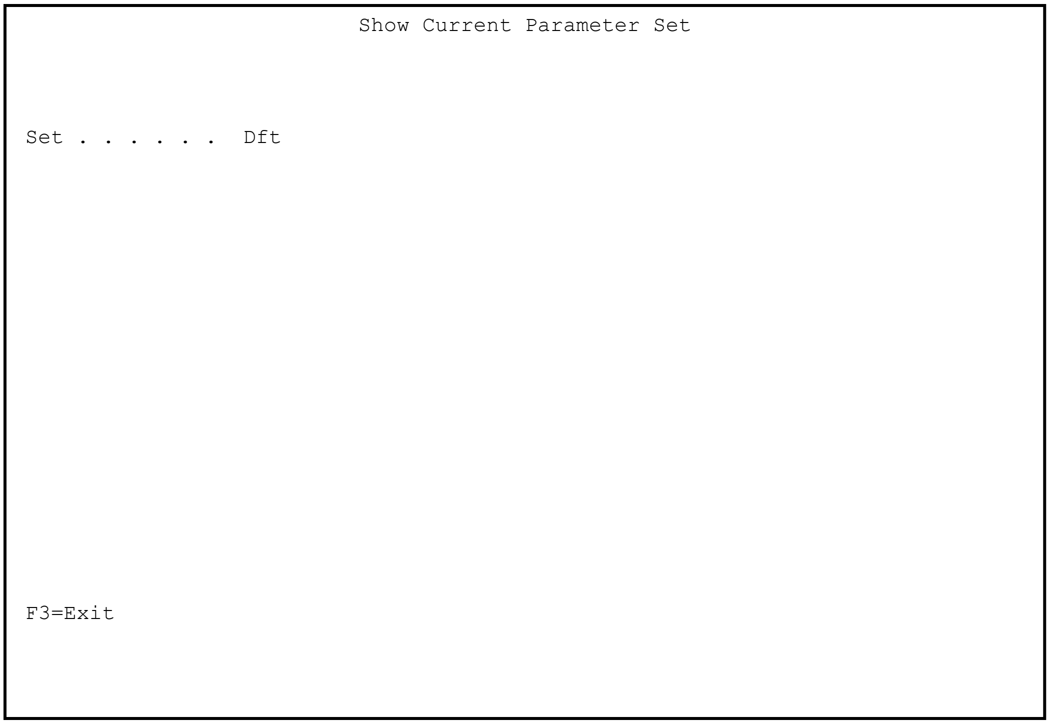


```
PGKEYP                    PGP Encryption Parameters                  iSecurity
                                                             System:    RLDEV

Active Parameters
 1. Display Current Setting
 2. Set Active Parameter Set

Parameter Sets
11. Work with Parameter Sets Directory










Selection or command
===> ____________________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

Field/Option/Command Key	Description
1. Display Current Setting	Displays the name of the current parameter set being used by **PGP Encryption**.
2. Set Active Parameter Set	Allows you to set the name of the current parameter set being used by **PGP Encryption**.
11. Work with Parameter Sets Directory	Displays the current parameter sets that are available for **PGP Encryption**.

Display Current Setting

To display the name of the file that holds the current parameter set, select **1. Display Current Setting** in the **PGP Encryption Parameters** menu. The **Show Current Parameter Set** screen appears, showing the file name of the current parameter setting.

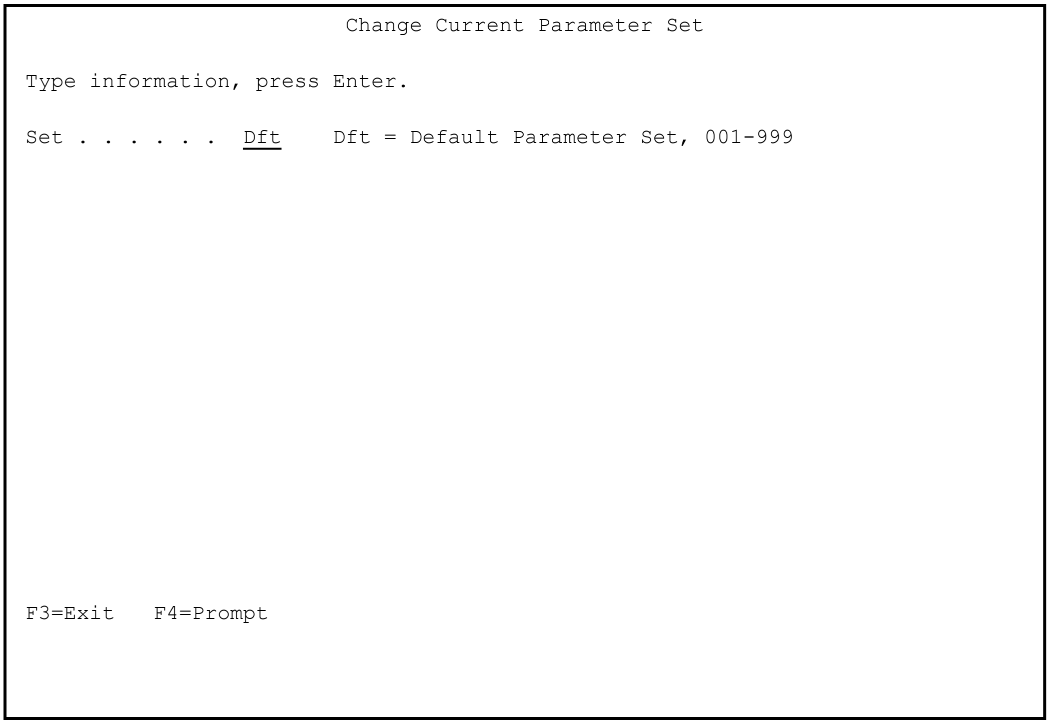


```
                            Show Current Parameter Set



 Set . . . . . . .  Dft
















 F3=Exit
```

Set Active Parameter Set

You may need to have different parameter sets for different business purposes.

To set the active parameter set, select **2. Set Active Parameter Set** in the **PGP Encryption Parameters** menu. The **Change Current Parameter Set** screen appears.



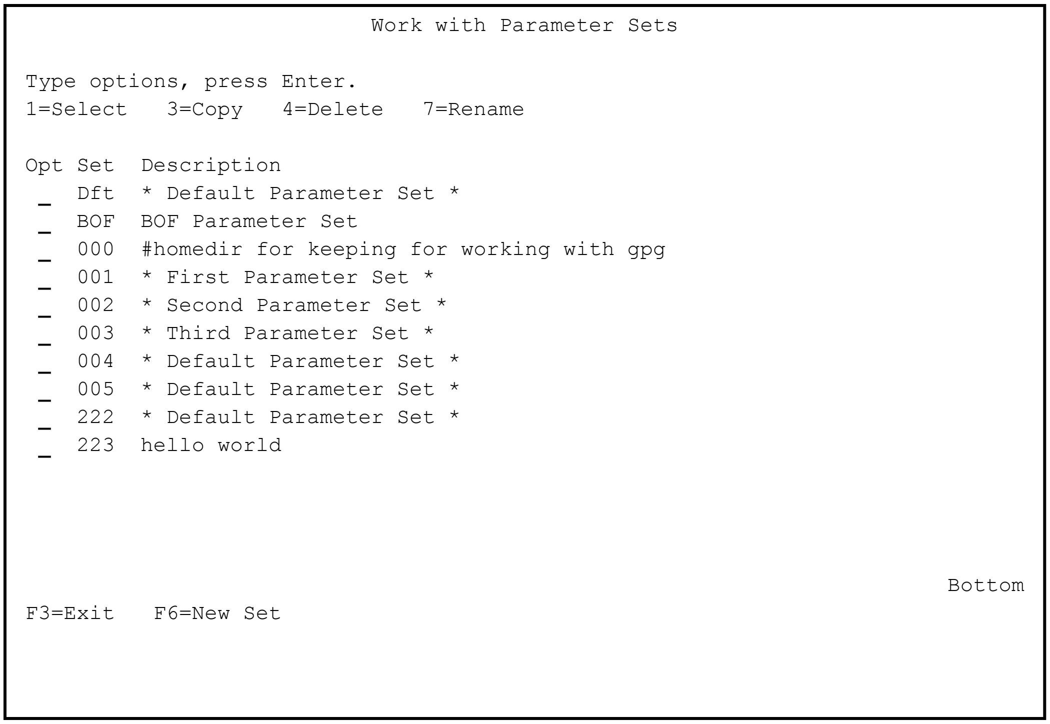
```
                          Change Current Parameter Set

 Type information, press Enter.

 Set . . . . . .  Dft    Dft = Default Parameter Set, 001-999











 F3=Exit   F4=Prompt
```

Set the **`Set`** field to a three-digit number from **`001`** though **`999`**, or leave the value as **`Dft`** to use the default value.

Work with Parameter Sets Directory

You can choose a parameter set to work on without knowing its name.

To work with parameter sets, select **11. Work with Parameter Sets Directory** in the **PGP Encryption Parameters** menu. A **Work with Parameter Sets** screen appears.



```
                           Work with Parameter Sets

Type options, press Enter.
1=Select   3=Copy   4=Delete   7=Rename

Opt Set  Description
 _  Dft  * Default Parameter Set *
 _  BOF  BOF Parameter Set
 _  000  #homedir for keeping for working with gpg
 _  001  * First Parameter Set *
 _  002  * Second Parameter Set *
 _  003  * Third Parameter Set *
 _  004  * Default Parameter Set *
 _  005  * Default Parameter Set *
 _  222  * Default Parameter Set *
 _  223  hello world




                                                                       Bottom
F3=Exit   F6=New Set
```

The body of the screen contains line for each parameter set, showing the three-character **Set** name and a free-form text **Description**.

To **copy** a parameter set, enter **3** in the **Opt** field for that line.

To **delete** a parameter set, enter **4** in the **Opt** field for that line.

To **rename** a parameter set, enter **7** in the **Opt** field for that line.

To **view or edit** a parameter set, enter **1** in the **Opt** field for that line. An editor screen appears.

To **create** a new parameter set, press the **F6** key. An editor screen appears.

Example Parameter Set

A default Parameter Set, **EncOptSetDft.sh**, is located in directory **\SMZE\**.

The default Parameter Set is shown below and is explained in the table that appears after the file.

NOTE: The capital letters that appear in red in the file do not appear in the actual file, but are references to the explanations in the table.

```
#!/bin/bash

A

##general var
#homedir for keeping for working with gpg
export DIR="/SMZE/gnupg"
export CMD="/SMZE"

B

##generate key pair
export KeyType="RSA"  #could be DSA, Elgamal or RSA
export Exp="4y"
export Length="1024"
export Usage="sign"   #could be sign or encrypt
export Preferences="AES AES256 SHA256 SHA512 ZIP Uncompressed"
export Password="openpgp"

C

#use these four parameters to create sub-key with your primary key
export IsSubKey="yes"        #"yes" for creating sub-key, otherwise - no.
 export SkeyType="RSA"       #could be DSA, Elgamal or RSA
 export SkeyLength="1024"
 export SkeyUsage="encrypt"  #could be sign or encrypt
```

D

```
##encrypt_file
export EncryptionDir=/SMZE/encrypt
export ESigner="7F116A2C"
export ESignerPass="openpgp"
export DefaultRecipient="7F116A2C"
```

E

```
##decrypt_file
export DecryptionDir=/SMZE/decrypt
export DecPass=""
```

F

```
##sign file
export Signer="7F116A2C"
export SignerPass="openpgp"
export SignedDir=/SMZE/signed
```

G

```
##sign key
export SignerKey="7F116A2C"
export SignerKeyPass="openpgp"
export SignedKeyDir=/SMZE/signed
```

H

```
##revocation
export RevokeDir=/SMZE/revocations
```

I

```
##Keyserver
export DefaultServer="hkp://pool.sks-keyservers.net"
```

J

```
##Export Dir for secret keys
export ExpSecKeys="/SMZE/exported_secret"
```

K

```
##Export Dir for public keys
export ExpPubKeys="/SMZE/exported_public"
```

L

```
##Export Dir for backup trustDB
export BackupDir="/SMZE/backupOwnerTrust"
```

M

```
##Regex var
export REALNAME=""
export EMAIL=""
export PASSWORD=""

export EXPORTSECRETKEYS=""
export EXPORTPUBLICKEYS=""
```

Reference	Description
A	Defines the libraries used in working with PGP Encryption
B	Defines the parameters used to generate a key pair: Key Type, Expiry, Length, Usage, Preference, and Password The Expiry can either be a specific date in the format dd-mm-yyyy or a number followed by a qualifier that defines days, months, or years. For example, 14d is 14 days and 1y is one year.
C	Defines the parameters used to create a sub-key from a primary key: SubKey Type, SubKey Length, and SubKey Usage
D	Defines the parameters for the encryption file: Library, Signer, Signer Password, and Default Recipient
E	Defines the parameters for the decryption file: Library and Password
F	Defines the parameters for the signature file: Signer, Library and Password
G	Defines the parameters for the signature key: SignerKey, SignerKey Password, and Library
H	Defines the Library for the revocation certificate
I	Defines the default Key Server
J	Defines the Library for exported secret keys
K	Defines the Library for exported public keys
L	Defines the Library for the backup trust database
M	Defines regular expressions