PGP® Mobile 9.9

User's Guide

Version Information

PGP Mobile User's Guide. PGP Mobile Version 9.9.0. Released September 2008.

Copyright Information

Trademark Information

Licensing and Patent Information

The IDEA cryptographic cipher described in U.S. patent number 5,214,703 is licensed from Ascom Tech AG. The CAST-128 encryption algorithm, implemented from RFC 2144, is available worldwide on a royalty-free basis for commercial and non-commercial uses. PGP Corporation has secured a license to the patent rights contained in the patent application Serial Number 10/655,563 by The Regents of the University of California, entitled Block Cipher Mode of Operation for Constructing a Wide-blocksize block Cipher from a Conventional Block Cipher. Some third-party software included in PGP Universal Server is licensed under the GNU General Public License (GPL). PGP Universal Server as a whole is not licensed under the GPL. If you would like a copy of the source code for the GPL software included in PGP Universal Server, contact *PGP Support* (http://www.pgp.com/support). PGP Corporation may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents.

Acknowledgments

This product includes or may include:

• The Zip and ZLib compression code, created by Mark Adler and Jean-Loup Gailly, is used with permission from the free Info-ZIP implementation, developed by zlib (http://www.zlib.net). • Libxml2, the XML C parser and toolkit developed for the Gnome project and distributed and copyrighted under the MIT License found at http://www.opensource.org/licenses/mit-license.html. Copyright © 2007 by the Open Source Initiative. • bzip2 1.0, a freely available high-quality data compressor, is copyrighted by Julian Seward, © 1996-2005. • Application server (http://jakarta.apache.org/), web server (http://www.apache.org/), Jakarta Commons (http://jakarta.apache.org/commons/license.html) and log4j, a Java-based library used to parse HTML, developed by the Apache Software Foundation. The license is at www.apache.org/licenses/LICENSE-2.0.txt. • Castor, an open-source, data-binding framework for moving data from XML to Java programming language objects and from Java to databases, is released by the ExoLab Group under an Apache 2.0-style license, available at http://www.castor.org/license.html. • Xalan, an open-source software library from the Apache Software Foundation that implements the XSLT XML transformation language and the XPath XML query language, is released under the Apache Software License, version 1.1, available at http://xml.apache.org/xalan-j/#license1.1. • Apache Axis is an implementation of the SOAP ("Simple Object Access Protocol") used for communications between various PGP products is provided under the Apache license found at http://www.apache.org/licenses/LICENSE-2.0.txt. • mx4j, an open-source implementation of the Java Management Extensions (JMX), is released under an Apache-style license, available at http://mx4j.sourceforge.net/docs/ch01s06.html. • jpeglib version 6a is based in part on the work of the Independent JPEG Group. (http://www.ijg.org/) • libxslt the XSLT C library developed for the GNOME project and used for XML transformations is distributed under the MIT License http://www.opensource.org/licenses/mit-license.html. • PCRE version 4.5 Perl regular expression compiler, copyrighted and distributed by University of Cambridge. ©1997-2006. The license agreement is at http://www.pcre.org/license.txt. • BIND Balanced Binary Tree Library and Domain Name System (DNS) protocols developed and copyrighted by Internet Systems Consortium, Inc. (http://www.isc.org) • Free BSD implementation of daemon developed by The FreeBSD Project, © 1994-2006. • Simple Network Management Protocol Library developed and copyrighted by Carnegie Mellon University © 1989, 1991, 1992, Networks Associates Technology, Inc, © 2001- 2003, Cambridge Broadband Ltd. © 2001- 2003, Sun Microsystems, Inc., © 2003, Sparta, Inc, © 2003-2006, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. The license agreement for these is at http://net-snmp.sourceforge.net/about/license.html. • NTP version 4.2 developed by Network Time Protocol and copyrighted to various contributors. • Lightweight Directory Access Protocol developed and copyrighted by OpenLDAP Foundation. OpenLDAP is an open-source implementation of the Lightweight Directory Access Protocol (LDAP). Copyright © 1999-2003, The OpenLDAP Foundation. The license agreement is at http://www.openldap.org/software/release/license.html. Secure shell OpenSSH version 4.2.1 developed by OpenBSD project is released by the OpenBSD Project under a BSD-style license, available at http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD. • PC/SC Lite is a free implementation of PC/SC, a specification for SmartCard integration is released under the BSD license. • Postfix, an open source mail transfer agent (MTA), is released under the IBM Public License 1.0, available at http://www.opensource.org/licenses/ibmpl.php. • PostgreSQL, a free software object-relational database management system, is released under a BSD-style license, available at http://www.postgresql.org/about/licence. • PostgreSQL JDBC driver, a free Java program used to connect to a PostgreSQL database using standard, database independent Java code, (c) 1997-2005, PostgreSQL Global Development Group, is released under a BSD-style license, available at http://jdbc.postgresql.org/license.html. • PostgreSQL Regular Expression Library, a free software object-relational database management system, is released under a BSD-style license, available at http://www.postgresql.org/about/licence. • 21.vixie-cron is the Vixie version of cron, a standard UNIX daemon that runs specified programs at scheduled times. Copyright © 1993, 1994 by Paul Vixie; used by permission. • JacORB, a Java object used to facilitate communication between processes written in Java and the data layer, is open source licensed under the GNU Library General Public License (LGPL) available at http://www.jacorb.org/lgpl.html. Copyright © 2006 The JacORB Project. • TAO (The ACE ORB) is an open-source implementation of a CORBA Object Request Broker (ORB), and is used for communication between processes written in C/C++ and the data layer. Copyright (c) 1993-2006 by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University. The open source software license is available at http://www.cs.wustl.edu/~schmidt/ACE-copying.html. • libcURL, a library for downloading files via common network services, is open source software provided under a MIT/X derivate license available at http://curl.haxx.se/docs/copyright.html. Copyright (c) 1996 - 2007, Daniel Stenberg. • libuuid, a library used to generate unique identifiers, is released under a BSD-style license, available at http://thunk.org/hg/e2fsprogs/?file/fe55db3e508c/lib/uuid/COPYING. Copyright (C) 1996, 1997 Theodore Ts'o. • libpopt, a library that parses command line options, is released under the terms of the GNU Free Documentation License available at http://directory.fsf.org/libs/COPYING.DOC. Copyright © 2000-2003 Free Software Foundation, Inc. • gSOAP, a development tool for Windows clients to communicate with the Intel Corporation AMT chipset on a motherboard, is distributed under the GNU Public License, available at

http://www.cs.fsu.edu/~engelen/soaplicense.html. • Windows Template Library (WTL) is used for developing user interface components and is distributed under the Common Public License v1.0 found at http://opensource.org/licenses/cpl1.0.php. • The Perl Kit provides several independent utilities used to automate a variety of maintenance functions and is provided under the Perl Artistic License, found at http://www.perl.com/pub/a/language/misc/Artistic.html. • rEFIt - libeg, provides a graphical interface library for EFI, including image rendering, text rendering, and alpha blending, and is distributed under the license found at http://refit.svn.sourceforge.net/viewvc/*checkout*/refit/trunk/refit/LICENSE.txt?revision=288. Copyright (c) 2006 Christoph Pfisterer. All rights reserved.

Export Information

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restricts the export and re-export of certain products and technical data.

Limitations

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement provided with the software. The information in this document is subject to change without notice. PGP Corporation does not warrant that the information meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by PGP Corporation.

Contents

1 About PGP Mobile

Built on proven encryption and key management services, PGP Mobile provides flexible encryption to meet the data protection and sharing needs of a mobile enterprise. With PGP Mobile, entire data volumes, archives, directories, or individual files can be encrypted.

Ready for the mobile enterprise, PGP Mobile can be deployed over-the-air, leveraging PGP Universal Server's trusted key management and provisioning services to reduce administrator setup time. When needed, PGP Mobile encrypted data can easily be shared with Windows users, even those without encryption software.

PGP Mobile is a PGP Encryption Platform-enabled application. The PGP Encryption Platform provides a strategic enterprise encryption framework for shared user management, policy, and provisioning, automated across multiple, integrated encryption applications. As a PGP Encryption Platform-enabled application, PGP Mobile is managed with PGP Universal Server to manage existing policies, users, keys, and configurations, expediting deployment and policy enforcement.

PGP Mobile protects your data by encrypting individual files, entire data volumes, archives, or directories. Use PGP Mobile to put any combination of files and folders into an encrypted, compressed package for easy distribution or backup. Finally, use PGP Mobile to shred (securely delete) sensitive files—so that no one can retrieve them.

In This Chapter

What's New in PGP Mobile Version 9.9

Building on PGP Corporation’s proven technology, PGP Mobile 9.9 includes numerous improvements and the following new features.

- PGP Mobile can now be installed on non-touchscreen devices.
- A new Home Screen allows quick access to the main functions of PGP Mobile.
- When viewing a key's properties, you can now also view the photo ID and signatures on the key.

- PGP Zip verification now includes a new verification panel.

Getting Assistance

For additional resources, see these sections.

Available Documentation

PGP Mobile on-device help is installed onto your touchscreen mobile device during the installation process (on-device help is not available for the non-touchscreen edition).

To view the help file on your touchscreen device, do one of the following:

- Launch PGP Mobile. To do this on your touchscreen device, select **Start > Programs**, and then select PGP Mobile. Then select **Menu > Help**.
- You can also navigate to the PGP Mobile help from your mobile device's main help. In the device's help Table of Contents, select **Help for Added Programs > PGP Mobile**.

The *PGP Mobile User's Guide* is available in an Adobe Acrobat Portable Document Format (PDF) files. You can view and print these files with Adobe Acrobat Reader, available on the *Adobe Web site* (http://www.adobe.com). The *PGP Mobile User's Guide* can be obtained from your PGP Universal Server administrator or from the PGP Corporation Knowledgebase.

Once PGP Mobile is released, additional information regarding the product is entered into the online Knowledge Base available on the *PGP Corporation Support Portal* (https://support.pgp.com).

Contacting Technical Support

- To learn about PGP support options and how to contact PGP Technical Support, please visit the *PGP Corporation Support Home Page* (http://www.pgp.com/support).
- To access the PGP Support Knowledge Base or request PGP Technical Support, please visit *PGP Support Portal Web Site* (https://support.pgp.com). **Note that you may access portions of the PGP Support Knowledge Base without a support agreement; however, you must have a valid support agreement to request Technical Support.**
- For any other contacts at PGP Corporation, please visit the *PGP Contacts Page* (http://www.pgp.com/company/contact/index.html).
- For general information about PGP Corporation, please visit the *PGP Web Site* (http://www.pgp.com).

- To access the PGP Support forums, please visit *PGP Support* (http://forum.pgp.com). These are user community support forums hosted by PGP Corporation.

2 Installing PGP Mobile

This section provides information on the system requirements and instructions for installing PGP Mobile.

Note: Your PGP Universal administrator may "push" the installation of PGP Mobile. This means that PGP Mobile will be installed on your device automatically. You are not prompted to enter any information during this type of installation.

In This Chapter

System Requirements

PGP Mobile is supported on the following operating systems and devices:

- Windows Mobile 5.0 Pocket PC
- Windows Mobile 5.0 Smartphone
- Windows Mobile 6.0 Professional
- Windows Mobile 6.0 Standard

PGP Mobile is supported on all resolutions supported by the Windows Mobile version in both portrait and landscape formats.

PGP Mobile supports external storage cards (for creating new PGP Disk volumes, creating PGP Zip files, and so on).

Installing PGP Mobile on Your Device

The following instructions describe how to install PGP Mobile on your mobile device.

To install PGP Mobile

1. The PGP Mobile installation file is a Microsoft Windows `.cab` file. The PGP Mobile configuration file is a `.dat` file. Both of these files can be transferred to your device using any of the following methods:
   - Desktop synchronization
   - Beaming (bluetooth, infrared)
   - Storage card transfer
   - Email
   - Web download
   - Mobile Device Management (MDM) push

   While it is not necessary, PGP Corporation recommends that both files be placed in the same location on your device.

   Note: Your non-touchscreen device may not include a file browser (File Explorer). If this program is not available on your device, see the following procedure for instructions on where to place the installation file on your device.
2. Once the installation and configuration files are on your device, start the installation by selecting the installation file (`.cab`).
3. When prompted, review and accept the end-user license agreement.
4. The PGP Mobile files are installed on your device. When completed, select **OK** to clear the message.
5. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
6. To enroll, enter your network login user name and password and select **OK**.
7. Once the enrollment has completed, a message is displayed informing you your key has been downloaded to your mobile device. Select **OK** to clear the message.

PGP Mobile has been installed, you have been enrolled with your PGP Universal Server, and you can now use PGP Mobile on your mobile device.

To install on devices without File Explorer

1. In ActiveSync, copy the files (`.cab` and `.dat`) to the \Windows\Start Menu folder.
2. To launch the installation file, on your mobile device select **Start**, locate the file (named `PGPMobile*.cab`), and select it. The installation program launches.
3. View and accept the license agreement and then continue to follow the previous procedure.

Upgrading from a Previous Version of PGP Mobile

To upgrade to PGP Mobile 9.9

- **From PGP Mobile 9.8:** Follow the installation process for PGP Mobile 9.9.

  PGP Mobile 9.8 is automatically uninstalled, and then PGP Mobile 9.9 is installed. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version.

Configuring PGP Mobile

PGP Mobile is managed by a PGP Universal Server. The name of the PGP Universal Server is defined in the configuration file used during installation (`PGPConfigure.dat`). Your administrator should have provided this file to you at the same time you received the installation file.

Using LDAP for Enrollment

Your network credentials are used during enrollment to your PGP Universal Server and to obtain your PGP key. During configuration, your GKM or SKM key is downloaded from the PGP Universal Server to your device.

Uninstalling PGP Mobile

When you uninstall PGP Mobile, all encrypted files and disks will remain encrypted. If you do not want these items encrypted, cancel the uninstall process and unencrypt the objects before beginning to uninstall PGP Mobile again.

To uninstall PGP Mobile on touchscreen devices

1. Select **Start > Settings** and click the **System** tab.
2. Select **Remove Programs**.
3. In the Programs in Storage Memory screen, select the PGP Mobile name and then select **Remove**.
4. When prompted to verify you want to remove PGP Mobile, select **Yes**.

To uninstall PGP Mobile on non-touchscreen devices

1. Select **Start > Settings**.
2. Select **Remove Programs**.
3. In the Remove Programs screen, select the PGP Mobile name and then select **OK**.
4. When prompted to verify you want to remove PGP Mobile, select **Yes**.

3 Using PGP Mobile

This section provides an overview of the functions you can perform with PGP Mobile. To use PGP Mobile, do one of the following:

- On a touchscreen device, select **Start > Programs > PGP Mobile**.
- On a non-touchscreen device, select **Start > PGP Mobile**.

The PGP Mobile Home Screen is displayed, providing quick access to the main features of PGP Mobile. To access additional PGP Mobile features, select the **Menu** option.

In This Chapter

Using the Home Screen

The PGP Mobile Home Screen displays options so you can quickly access the main features of PGP Mobile:

- **PGP Keys**: Select this option to view the keys list.
- **New PGP Zip**: Select this option to create a new PGP Zip archive.
- **New PGP Disk**: Select this option to create a new PGP Disk. Existing PGP Disks are displayed under this option.
- **PGP Shredder**: Select this option to securely delete a file on your device.

To access additional PGP Mobile features, select the **Menu** option.

Tip: The Home Screen provides quick shortcuts to the main functionality of PGP Mobile. All of the functions displayed in the Home Screen are also available from the PGP Mobile **Menu**. Use the **Menu** rather than the Home Screen when you want to perform more advanced functions, such as signing a file rather than encrypting a file, or unmounting a disk rather than creating a new one.

To return to the Home Screen

- From any location within PGP Mobile, select **Menu > Home Screen**.

Viewing the PGP Mobile Verification Log

Use the PGP Mobile Log to view the status of all signature operations.

To view the verification log

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. Select **Menu > PGP Zip > Verification**. The verification log is displayed.
3. To view the details of the verified item, select the item. The Verification Report screen displays information on the date the file was signed.
4. Select **Next** to display the Key Properties screen.

Clearing the Passphrase Cache

When you clear your passphrase cache, the next time you attempt to perform a PGP Mobile function, you are prompted to enter your passphrase.

To clear the passphrase cache

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. Select **Menu > Clear Passphrase Cache**.

Viewing the License Agreement

The license agreement is copied to your mobile device during the installation process.

To view the license agreement

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. Select **Menu > License Agreement**.

4 Managing PGP Keys

This section provides information on how to move keys to your device, search for others' public keys, import and delete keys, and view the properties of a key on your keyring.

In This Chapter

Viewing the Key List

The key list contains your key plus all of the public keys on the keyring on your mobile device. To view the list of keys if it is not displayed, select **Menu > Key List**.

To view the key list

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. In the main PGP Mobile screen, select **PGP Keys**. If the main screen is not displayed, select **Menu > Key List**. The list of keys on your keyring is displayed.

Viewing the Properties of a Key

The Key Type screen displays information about the key:

- Name
- Email address
- Key ID
- Type of Key
- Size
- Trust
- Validity
- Status
- Encoding
- Key Server
- Creation date
- Expiration
- Group
- Cipher
- Hash
- Compression

From this screen, you can also access the key's fingerprint, photo ID, and signatures.

To view a key's properties

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. In the main PGP Mobile screen, select **PGP Keys**. If the main screen is not displayed, select **Menu > Key List**. The list of keys on your keyring is displayed.
3. In the keys list, select the key you want to view. The Key Type screen is displayed.
4. To view additional information about the key:
   - To view the key fingerprint, select **Options > Key Fingerprint**.
   - To view the photo ID, select **Options > Key Photo ID**.
   - To view the key's signatures, select **Options > Key Signatures**.

Searching for Keys

To search for another user's public key

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. Select **Search**. The search screen is displayed.
3. Enter the name of the person whose key you are searching for and select **Search**.
4. If any results are found, they are displayed.
   - Verify that the person's name and email address is the one you want (select the key if you want to view the key's properties or fingerprint).
   - To add this person's public key to your device, select **Add**.
   - For additional options, such as to export the key, select **Options**.
5. To clear the search results so you can search again, select **Clear**.

Searching for Keys Over the Network

By default, keys are searched first on the PGP Universal Server and then in the PGP Global Directory.

Importing Keys

Keys can be imported to your device by:

- Exporting the key from PGP Desktop, copying the key to your mobile device, and then selecting the key file. The key is imported and added to your key list.
- Exporting the key, from another device, to a storage card on that device. Then insert the card into your device and select the key file. The key is imported and added to your key list.

Exporting Keys

To distribute your public key to others, export it to a file and then make this file available to the person with whom you want to communicate securely.

To export the public portion of a key

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. In the main PGP Mobile screen, select **PGP Keys**. If the main screen is not displayed, select **Menu > Key List**. The list of keys on your keyring is displayed.
3. In the keys list, select the key you want to export. The Key Type screen is displayed.
4. To export the key, select **Options > Export Key**. The PGP Key Export screen is displayed.
5. To save the key to a specific folder, select the **Folder** field and select the folder you want to use. The default location is your My Documents folder.
6. To specify the location, such as an external card on your drive, select the **Location** field and select the location where you want the file saved. Note that if you do not have an external storage card inserted in the device, the only option available is **Main Memory**.
7. Select **Save** to export the key. A message is displayed briefly that the key is being exported, and the Key Type screen is displayed again.

Deleting Keys

PGP Mobile gives you control over the keys on your device, so you can remove any user's public key.

To delete a key

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.

- On non-touchscreen devices, select **Start**, and then select PGP Mobile.

2. In the main PGP Mobile screen, select **PGP Keys**. If the main screen is not displayed, select **Menu > Key List**. The list of keys on your keyring is displayed.
3. In the keys list, select the key you want to remove. The Key Type screen is displayed.
4. To delete the key, select **Options > Delete Key**.

5 Using PGP Zip

This section provides information on how to use PGP Zip to encrypt an individual file located on your device or on an external storage card.

In This Chapter

Encrypting a File

Encrypt a single file to your key or to the public key of another user. The file can be located on your mobile device or on a storage card that is inserted in the device.

To encrypt a file

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. In the main PGP Mobile screen, select **New PGP Zip**. If the main screen is not displayed, select **Menu > PGP Zip > Encrypt**. The Encode File screen is displayed.
3. Locate and select the file you want to encrypt.
4. When prompted, select the key(s) you want to use to encrypt the file.
5. To specify additional settings, select **Options**. For more information, see *Using PGP Zip Options* (on page 20).
6. Select **Done**. The file is encrypted.

Note: If your passphrase is not cached, you are prompted to enter the passphrase for the key.

To encrypt and sign a file

1. Launch PGP Mobile as described above, and then select **Menu > PGP Zip > Encrypt & Sign**.
2. Follow the steps above to locate and select the file.
3. Do one of the following:
   - If your passphrase is cached, a message is displayed informing you the cached passphrase was used to sign the zipped file. Select **OK** to continue.
   - If your passphrase is not cached, a message is displayed asking you to enter the passphrase for the Signing Key displayed. Enter the passphrase and select **Done** to continue.

To sign a file

- Follow the steps above to encrypt and sign a file except select **Menu > PGP Zip > Sign**.

Using PGP Zip Options

When you encrypt a file, there are additional options available. Select **Options** in the Tap Keys to Add screen to display the Options menu:

- **Text Output**: Select this option if you want to email this zip archive as a binary file, and you are using an older email application. Saving the file as ASCII text increases the size of the encrypted file by about 30%.
- **Input is Text**: Select this option to create a zip archive of a text file.
- **Shred Original**: Select this option if you want to securely remove the original after the archive has been created.
- **Secure Viewer**: Select this option to create a zip archive that requires the PGP Secure Viewer, if your organization's security policies specify that requirement. If you have selected this mode, when the file is decrypted it is displayed in a PGP Secure Viewer window. Using this option protects against outdated radiation capturing attacks.
- **Self Decrypting Archive**: Select this option to create an archive that decrypts automatically when opened on a Windows computer.

- **Conventional Encryption**: Select this option to use conventional encryption using a passphrase (rather than a key) when creating the archive. You are prompted to enter and confirm the passphrase. To view keystrokes as you enter the passphrase, select **Options > Show Keystrokes**. The passphrase is required to decrypt the zip archive.

When you sign a file, there are additional options available. Select **Options** in the Signing Key screen to display the Options menu.

- **Detached Signature**: This is the default option. A separate file with a .sig file extension is created. Send this file along with the file you signed so your recipient can verify that you did, in fact, send him or her the file.
- **Text Output**: Select this option if you want to email this zip archive as a binary file, and you are using an older email application. Saving the file as ASCII text increases the size of the encrypted file by about 30%.
- **Input is Text**: Select this option to create a zip archive of a text file.

Using a Passphrase Instead of a Key

Encrypt using a passphrase:

- When you want to create a PGP Zip archive without using recipients' keys (this can be less secure than encrypting with recipients' keys, although still highly secure depending on the complexity of the passphrase you use).
- When each of your recipients has PGP Mobile installed on a mobile device or PGP Desktop (for Windows or Mac OS X) installed on their computers.
- When you do want to reveal a passphrase to file recipients.
- When you do not have a public key for each recipient (from your Keyring or a PGP Keyserver).

Tip: Encrypting with a passphrase is also referred to as *conventional encryption.*

Encrypting your PGP Zip Archive with a passphrase can be extremely secure, especially with a strong passphrase. However, encrypting to recipient keys does offer even higher security. When you encrypt to your recipients' keys, those who possess the PGP Zip Archive need both their private keys and passphrases to decrypt the file (and each recipient's private key has its own passphrase).

When encrypting with a passphrase, everyone opens the file using the same passphrase, and no private keys are required. Anyone who possesses the file, uses PGP Mobile or PGP Desktop, and knows the passphrase can decrypt the file.

Caution: Take every possible precaution to ensure that the passphrase to your PGP Zip Archive is revealed to no one but the intended recipients. If the passphrase is revealed to unauthorized persons, create a new PGP Zip Archive with a different passphrase. Note, however that you can do nothing to re-secure the original archive file and its contents.

Once your files are secured, send the resulting PGP Zip Archive file to your recipients however you choose. Your recipients then use PGP Mobile to open the PGP Zip Archive file. *Anyone who has the file and the passphrase can open the resulting PGP Zip Archive file,* and everyone sees the same items. If you need to have different recipients see different items, you must create separate PGP Zip Archive files for each.

Signing a File

For times when you do not need to encrypt a file for your recipients, you can choose the Sign option. Instead of encrypting your files and zipping them into one PGP Zip Archive, this option zips them only.

Use Sign:

- When you do not need to encrypt your files (so you do not need to reveal a passphrase to recipients).
- When you want to generate a signature file that your recipients can use to confirm the PGP Zip Archive came from you. Each file is processed individually and a separate detached sig is created for every file.
- When each of your recipients has PGP Mobile installed on a mobile device or PGP Desktop (for Windows or Mac OS X) installed on their computers.
- When you want to guarantee that you have sent the file, and you want to assure your recipient that the file has not changed during transit.

Decrypting a File

Decrypt a PGP Zip with your private key from your device.

To decrypt and verify a file

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. Select **Menu > PGP Zip > Decrypt/Verify**. The Decode File screen is displayed.

3 Locate and select the file you want to decrypt. If your passphrase is not cached, you are prompted to enter the passphrase. The file is decrypted.

Verifying Signed PGP Zip Archives

If you received a signed PGP Zip Archive, you should verify the signature so that you know who it came from—and that the archive was not tampered with before you got it.

To verify a PGP Zip Archive

1 Launch PGP Mobile. To do this:

- On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
- On non-touchscreen devices, select **Start**, and then select PGP Mobile.

2 Select **Menu > PGP Zip > Decrypt/Verify**. The Decode File screen is displayed.

3 Locate and select the file you want to verify. After the file has been verified, the verification screen is displayed.

4 To view additional information about the signed file, including the signer and date/time the file was signed, select the verified file name. The Verification Report screen is displayed.

- To view the properties of the key used to sign the file, including the key ID and verification method, select **Next**.
- To view the key fingerprint, photo ID, or signatures, select **Options**.

Creating Self-Decrypting Archives

Create a PGP Self-Decrypting Archive:

- When you want to create a PGP Zip self-decrypting archive without using recipients' keys (this can be less secure than encrypting with recipients' keys, although still highly secure).
- When your recipients do not have PGP Desktop installed on a Windows system.
- When you do want to reveal a passphrase to file recipients.
- When you do not have a public key for each recipient (from your Keyring or a PGP Keyserver).

PGP Zip SDA files are standard Windows executable (.exe) files that you an open simply by double-clicking them.

PGP Zip SDA files are slightly larger than regular PGP Zip Archives because the self-decrypting "mechanism" requires a certain amount of extra space (usually about 100 KB).

Once you have created your PGP Zip SDA, send it to your recipients however you choose. *Anyone who has the file and the passphrase can open the resulting PGP Zip Archive file,* and everyone sees the same items. If you need to have different recipients see different items, you must create separate PGP Zip Archive files for each. It is not necessary for the recipients to have PGP Desktop installed to view the contents of the PGP Zip SDA.

Caution: Take every possible precaution to ensure that the passphrase to your PGP Zip SDA is revealed to no one but the intended recipients. If the passphrase is revealed to unauthorized persons, create a new PGP Zip SDA with a different passphrase. Note, however that you can do nothing to re-secure the original archive file and its contents.

To create a self-decrypting archive

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. Select **Menu > PGP Zip > Encrypt**. The Encode File screen is displayed.
3. Locate and select the file you want to encrypt
4. When prompted to select the key(s) you want to use to encrypt the file, select **OK**. (It is not necessary to select a key since self-decrypting archives are encrypted using a passphrase.)
5. Select **Options > Self-Decrypting Archive** and then select **OK**. The passphrase screen is displayed.
6. Enter and confirm a passphrase that will be used to encrypt and decrypt the file and select **OK**. The Confirm SDA Filename screen is displayed.
7. Confirm or change the name of the self-decrypting archive and its location and select **Save**. The file is encrypted into a self-decrypting archive.

6 Using PGP Disk

This section provides information on how to create and manage secure volumes on your device or external storage card.

PGP Mobile supports all virtual disk algorithms (AES256, CAST5, and TwoFish), disk types (sparse and normal), and user types (public key or symmetric) as long as the disk is formatted using the FAT32, FAT16, or FAT12 file system. You can also create new sparse virtual disks of any size that are FAT formatted.

In This Chapter

About PGP Disks

A PGP Disk is an area of space, in memory on your device or on an external storage card, which is set aside and encrypted. PGP Disks are much like a bank vault, and are very useful for protecting sensitive files while the rest of your device is unlocked for work.

A PGP Disk looks and acts like an additional disk, although it is actually a single file that can reside in the device's memory or external storage cards. It provides storage space for your files—you can even install applications, or save files to a PGP Disk—but it can also be locked at any time without affecting other parts of your device. When you need to use the applications or files that are stored on a PGP Disk, you can unlock the disk and make the files accessible again.

PGP Disks are unlocked and locked by mounting and unmounting them from your device. PGP Mobile helps manage this operation for you.

When a PGP Disk is mounted, you can:

- Move/copy files into or out of the mounted PGP Disk.
- Save files to the mounted PGP Disk.
- Install applications within the mounted PGP Disk.

Files and applications on a PGP Disk are stored encrypted. If your device crashes while a PGP Disk is unmounted, the contents remain safely encrypted.

When a PGP Disk is unmounted, it does not appear within the File Explorer, and it is inaccessible to anyone without proper authentication.

It is important to remember that all your data remains secure in the encrypted file and is only deciphered when you mount the PGP Disk. Having the data for a volume stored in this manner makes it easy to manipulate and exchange PGP Disks with others but it also makes it easier to lose data if the file is somehow deleted. It is wise to keep a back up copy of these encrypted files so that the data can be recovered if something happens to the original.

Keeping Your Data Secure

Once you have mounted a PGP Disk, the disk appears just like any other volume or card on your device. You can access files, copy files, even work on files within that volume. Data stored in a PGP Disk is completely available until the disk is unmounted.

To ensure the security of your data, be sure to unmount the disk when you are finished working in it.

Creating a PGP Disk

Create a new PGP Disk on your device or external storage card and mount it as a secure volume. Define the size and location of the PGP Disk volume.

To create a PGP Disk

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. From the main screen, select **New PGP Disk**, or select **Menu > PGP Disk > New Disk**.
3. Enter the name you want to use for the PGP Disk, and make any changes to the location of the disk (folder, memory/storage card).
4. Select **Save**.
5. Specify the capacity and the size of the PGP Disk volume you want to create. For **Dynamic** disks, the size is the maximum size the disk can grow to (the size of the PGP Disk will grow as you add files to it, up to this maximum size). The default **Capacity** is **Dynamic** and the default **Size** is **50MB**.

6 Select the unit of measure (**KB** or **MB** or **GB**) for the size of the volume. The default setting is **MB**.

Note: The minimum size of the PGP Disk volume you can create is 100 KB; the maximum size is 25 GB..

7 Specify the encryption algorithm you want to use to protect your data:

- **AES (256 bits)**. AES (Advanced Encryption Standard) is a block cipher that can be used at 128, 192, or 256 bits. The more secure 256-bit version is used for creating PGP Disk volumes by default.
- **CAST5 (128 bits)**. CAST is a 128-bit block cipher. CAST is a strong, military-grade encryption algorithm that has a solid reputation for its ability to withstand unauthorized access.
- **Twofish (256 bits)**. Twofish is a 256-bit block cipher, symmetric algorithm. It was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the AES (Rijndael was selected).

8 Select **Next**.

9 Select the name of the user who can mount the PGP Disk and press **Enter**.

10 Select **Finish**. The PGP Disk is created. If you selected to mount the disk on creation, the disk is also mounted.

Mounting or Unmounting a PGP Disk

To use a PGP Disk, you must mount it.

To mount a PGP Disk

1 Launch PGP Mobile. To do this:

- On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
- On non-touchscreen devices, select **Start**, and then select PGP Mobile.

2 Select **Menu > PGP Disk > Mount Disk**. The PGP Disk Mount screen is displayed.

3 Locate and select the name of the PGP Disk file (*.pgd). The PGP Disk is mounted.

Tip: Quickly mount a PGP Disk from the Home Screen. Your PGP Disks are listed under the **New PGP Disk** option. To mount an unmounted PGP Disk, select the disk's name.

To unmount a PGP Disk

1 Launch PGP Mobile. To do this:

- On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
- On non-touchscreen devices, select **Start**, and then select PGP Mobile.

2 Select **Menu > PGP Disk > Unmount All Disks**. Any mounted PGP Disks are unmounted.

Using a Mounted PGP Disk

Create, copy, move, and delete files and folders on a PGP Disk just as you normally do with any other storage area on your mobile device.

Anyone else who has access to the storage area can also access the data stored there. It is not until you unmount the volume that the data is protected.

Caution: Although each PGP Disk file is encrypted and cannot be accessed by anyone without proper authorization, it can still be deleted from your mobile device. Anyone with access to your device could delete the encrypted file containing the PGP Disk. For this reason, keeping a backup copy of the encrypted file is an excellent safety measure, as is keeping your device locked when you are not using it

Compacting a PGP Disk Volume

When needed, manually compact a PGP Disk volume. Use this option if you are running low on space on your device or external storage card.

To compact a PGP Disk, you must first unmount it.

To compact a PGP Disk

1 Launch PGP Mobile. To do this:

- On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
- On non-touchscreen devices, select **Start**, and then select PGP Mobile.

2 Select **Menu > PGP Disk > Compact Disk**. The PGP Disk Compact screen is displayed.

3 Locate and select the name of the PGP Disk file (*.pgd). The PGP Disk is compacted.

Viewing the Properties of a PGP Disk

View the properties of a PGP Disk to determine the name of the PGP Disk, the location of the disk, capacity, and encryption algorithm.

To view the properties of a PGP Disk, you must first unmount it.

To view the properties of a PGP Disk

1 Launch PGP Mobile. To do this:

- On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
- On non-touchscreen devices, select **Start**, and then select PGP Mobile.

2 Select **Menu > PGP Disk > Disk Properties**. The PGP Disk Properties screen is displayed.

3 Locate and select the name of the PGP Disk file (*.pgd). The properties screen is displayed.

7 Shredding Files

If you want to completely destroy sensitive files without leaving fragments of their data behind, use the PGP Shredder utility.

The PGP Shred feature works by overwriting your data with random text. It repeats this multiple times, or *passes*. PGP Mobile is set to overwrite data with three passes. This number exceeds the media sanitization requirements specified in the Department of Defense 5220.22-M standard.

Note that PGP Shred does not delete Windows Mobile system files.

This section provides information on how to securely shred a single file.

In This Chapter

Using PGP Shred to Delete Files

When you delete a file using PGP Shred, all traces of that file are removed from your mobile device. Note that PGP Shred does not delete Windows Mobile system files.

To securely delete a file

1. Launch PGP Mobile. To do this:
   - On touchscreen devices, select **Start > Programs**, and then select PGP Mobile.
   - On non-touchscreen devices, select **Start**, and then select PGP Mobile.
2. Select **Menu > PGP Shred**. The Shred File screen is displayed.
3. Locate and select the file you want to shred.
4. In the PGP Alert screen, select **OK** to confirm you want to shred the file. The file is shredded and permanently deleted from your device.